A Symmetry Analysis of Pythagoras and Fermat's Last Theorem

All Sections, 1 to 7

R J Miller, 27 August 2004

Combined all sections, Draft D, 18 December 2004

Given the emotive nature of Fermat's Last Theorem
it is stressed this work is NOT a claim of a proof.

Abstract

An analysis of Pythagoras's Theorem and Fermat's Last Theorem is performed by the study of two conditions, termed the Residue and Quotient Condition, which have to be satisfied by any possible integer triple solution (a, b, c) to the Diophantine Equation a^n + b^n = c^n for prime, exponent n, n >= 2.

The Residue Condition filters out Candidate Pairs of integers b and c that satisfy a form of the Generalised Fermat Equation, k*a^n + b^n = c^n, for what we term the base 'a'. The Quotient Condition restricts k to unity and should such a triple (a, b, c) be found, which satisfies both the Residue and Quotient Conditions, then it would be an FLT counter-example. Of course, for exponent n >= 3, no such counter-examples exist, Wiles [1]. The Residue Condition necessitates the study of Residue Sequences: x^n (mod a^n), 0 <= x < a ^n, in the 'Standard' case; (mod b^n) in the 'Dual' case; and (mod c^n) in the 'Skew' case.

The structure of a Residue Sequence, its symmetries and the stringency of the Residue and Quotient Conditions offers insight, but not a proof, into why Pythagoras has solutions but FLT has none. The two conditions allow us to place several constraints on the form of integers a, b and c in any such FLT counter example, were they to exist.

We show that all Pythagorean triples can be generated through a symmetry in the Residue Sequences which exist by virtue of an even power exponent. For odd exponent n >= 3, this symmetry is absent and is replaced by a Skew Symmetry which we show is not sufficient to generate FLT solutions. We conclude from this that were there to be any FLT solutions for odd exponent they would have to arise through another mechanism which we term 'Unity Root Mappings'. In the Standard case, a Unity Root u, such that u^n = 1 (mod a^n), a < u < a^n, maps an integer b to integer c via the relation c = u*b (mod a^n), a < b < c. This mechanism offers the possibility of counter-examples but, in doing so, allows us to place yet more restrictions upon any such counter-example (a, b, c).

0 Introduction

0.1 Document Status

0.1.1 History

0.1.1.1 Combined, all sections 1 to 7

All sections were combined into this single volume, Issue 0 Draft D.

18/12/2004 Issue 0. Draft D

0.1.1.2 Sections 1 and 2

29/09/2003 Issue 0. Early unpublished notes
19/05/2004 Issue 0. Draft 0
27/08/2004 Issue 0. Draft A
05/11/2004 Issue 0. Draft B5
10/11/2004 Issue 0. Draft C2
11/11/2004 Issue 0. Draft C3
18/11/2004 Issue 0. Draft C4
21/11/2004 Issue 0. Draft C5

0.1.1.3 Section 3

28/11/2004 Issue 0. Draft C3

0.1.1.4 Sections 4 to 7

16/11/2004 Issue 0. Draft C3

0.1.2 Formats

Word 2000 format

This document is currently available in electronic form only as an MS Word 2000 Document.

This documents have been written using the standard ASCII character set for all equations and an equation editor has not yet been employed. This is so that a pure-text

version can easily be generated. A more standard form incorporating standard mathematical symbols, subscripts etc, will be generated at a later date prior to release.

Text format

A single text document, which is converted directly from an amalgamation of the three separate Word documents, above is also supplied.

Sections1to7_*date*.txt

HTML format

An online version will be made available, prior to external review, so that it can be made available to a wider audience.

PDF format

Once the document has been externally reviewed and corrected it is anticipated that any publishable work resulting from it will be then written with a more approriate editor such that it can be made available in Adobe Acrobat, PDF form

0.1.3 Current Status

The document is still in a pre-published form and has not yet been reviewed although it is now ready for a preliminary review prior to a full peer review and possible submission of parts for publication.

Due to its large size and diversity of topics, should extracts be published, it is likely that this document will be broken up into a summary paper and a few minor papers.

0.1.4 TBDs

All current outstanding points, missing cross references, Author references etc. are marked by the bracketed three-letter-acronym (TBD) denoting ‘To Be Defined’. In some serious cases additional text has been highlighted in yellow.

0.1.5 Originality of Content

The originality of much of the work presented cannot be guaranteed. Indeed several Theorems are trivial and well-known, for example those on Pythagoras. In these instances they are presented only for completeness. However, we are not claiming a Proof of FLT nor claiming originality of all the work. Whilst doing the work during 2003 and 2004, several aspects have been found to be prior known and published. A good example is the Modified Fermat Test (MFST), section (4.5) which is more commonly known as The ‘Strong Pseudoprime Test’, ref. Mathworld [4]). Another example is the Unity Root Polynomial ‘f(u)n’, section (3.6), which is actually a form

of ‘Cyclotomic Polynomial’, ref. Mathworld [4] with well known factor properties which are also derived. References to prior published work are welcome and will be acknowledged when verified.

0.1.6 Reviewers

Comments will be accepted by any person reading the document. Spelling and grammar corrections will also be accepted – we had to disable these word-processing features as they caused considerable problems – crashing.

The document is available electronically and electronically embedded comments are welcome. Please use some method to differentiate them, such as highlighting in red or blue, if using Word. For text only, use multiple asterisks ‘****’ or ‘@@@@’ to delineate comments. Return the document electronically, by email, to the principle author, see Contact, below.

0.1.7 Contact

Richard J Miller
richard@microscitech.com
richard@microscitech.freeserve.co.uk

0.2 Foreward

This paper is based upon earlier, unpublished work first started in September 2003. This early work established the Residue and Quotient Conditions and criteria for generating Pythagorean Triples via symmetry in the Residue Sequence. It was this initial observation on symmetry that triggered the wider study into FLT.

Absurd as it may seem to study FLT 'after the horse has bolted', i.e. several years after a proof has been published, the Wiles 1995 [1] proof is essentially an indirect proof, i.e. a proof of the Taniyama Wiles Shimuara' conjecture, and offers no simple, direct insights into the difficulty of finding any counter-example to FLT. It is the intention of this paper to try and gain some direct insight why counter-examples are non-existant for exponents n >= 3. Because Pythagoras does have solutions, we use this case extensively for a comparative study.

The paper is split into five main sections:

section 1 starts by establishing conditions and imposing constraints upon any possible solutions to the FLT equation;

section 2 then analyses the residue mechanism by which these constraints can be satisfied, splitting the exponent into even and odd cases since they have an inherently different structure in their Residue Sequences, namely symmetric (even exponent) and skew-symmetric (odd exponent);

section 3 unifies the symmetric and skew-symmetric concepts in section 2 through the study of Unity Roots;

section 4 is a collection of miscellaneous applications arising from concepts presented in sections 1, 2 and 3

section 5 summarises all the constraints upon any possible FLT counter-example, were there to be any

For some background to FLT we point you to the following two references [2] and [3]. For an elementary, under-graduate level text on Number Theory, see reference [6]. The online reference [4] is also an excellent source of information on all mathematical topics.

It is often stated that a Residue approach to work on an FLT proof is doomed to failure since there are ‘local solutions’. [Reference required TBD]. However, although the work presented in this paper is based upon a residue approach it does not start with a congruential form of the FLT equation such as

$$a^n + b^n = c^n \pmod A$$

Instead, the work starts with the exact FLT equation

$$a^n + b^n = c^n$$

and then places Residue Conditions upon possible solutions to this exact equation.

A lot of number theory deals with what the actual values of residues are, for instance, the subject of quadratic residues and, in general, n'th order residues. Our work is primarily interested in the cases where residues repeat within the [0, a^n) interval when studying residues (mod a^n). What their actual values are is of little or no relevance. Ultimately we shall see, section (3), that the only residue of real interest is +1 and, in particular, the Unity Roots u, u!= 1, where u^n = +1 (mod a^n).

The work presented in this paper is entirely based on congruential arithmetic and generally using only positive integers, never really straying into either negative numbers or complex numbers. The main reason for this is that every negative integer has a positive equivalent in modulo arithmetic, e.g. - x = A - x (mod A) and thus we can always use the positive form if so desired. Secondly, and related, any equation of the form x^n = -1 (mod A) can also be written x^n = A - 1 (mod A) for which there may/may not be solutions in integer arithmetic. If there are no integer solutions then this is not of real concern within the scope of this paper.

0.3 Conventions

The following will be assumed throughout

0.3.1 We shall be working with a triple of integer a, b and c, denoted by the ordered triple notation (a, b, c), such that it is a solution to the following Diophantine equation for integer exponent n, n >= 2.

0.3.1.1 a^n + b^n = c^n

0.3.2 The exponent n is 2 or greater and prime, excepting when n = 4.

0.3.3 The triple (a, b, c) is such that a, b and c are all positive integers and satisfy the following inequalities

0.3.3.1 a >2

0.3.3.2 b >a

0.3.3.3 c > b

The minimum value of b and c under consideration is thus 3 and 4 respectively.

0.3.4 The three integer values a, b and c are all 'co-prime in pairs'. This ensures that the solutions to equation (0.3.1.1) have no common factor, i.e. they are 'primitve'.

0.3.4.1 GCD(a,b) = 1

0.3.4.2 GCD(b,c) = 1

0.3.4.3 GCD(a,c) = 1

0.3.5 The following symbolic, mathematical conventions are employed

0.3.5.1 When referring to the modulus, invariably a^n, b^n or c^n, the base is the un-exponentiated form, i.e. a, b or c.

a - the 'Standard Base', smallest member of (a, b, c).
b - the 'Dual Base', middle value member of (a, b, c)

c – the ‘Skew Base’, largest member of (a, b, c)

When we are referring to the Standard Base a, we usually drop the 'Standard' prefix as for most terms prefixed with 'Standard' when the context is clear.

0.3.5.2 Residues, usually symbolised by 'r', are always such that r > 0. When negative, they are denoted by -r. The ‘zero residue’ (r = 0) occurs for values x = ka (integer k, base a) which is excluded since, if b or c is a multiple of a, then the triple (a, b, c) is not co-prime in pairs (0.3.4).

0.3.5.3 Quotients, usually symbolised by q and p' or p’ and q’, are always such that p > 0, q > 0, p’ > 0, q’ > 0. When negative they are denoted by -p and -q respectively.

0.3.5.4 Exponentiation takes precedence over multiplication or division. E.g. a^n/n = (a^n) / n. Often a bracket will be used for clarity.

0.3.5.5 All variables and constants are assumed positive whole numbers >= 0 unless otherwise stated.

0.3.5.6 The three ordered pairs of integers (b,c), (a,c), (a,b) are termed 'Candidate Pairs' (they each share a common 'Repeat Residue')

(b,c) - the 'Standard Candidate Pair', b^n = c^n (mod a^n)

(a,c) - the 'Dual Candidate Pair', a^n = c^n (mod b^n)

(a,b) - the 'Skew Candidate Pair', a^n = b^n (mod c^n)

When we are referring to the Standard Candidate Pair (b,c) we usually drop the 'Standard' prefix as for most terms prefixed with 'Standard' when the context is clear.

0.3.5.7 Usage of the muliplication symbol *

The multiplication symbol '*' is not always used when multiplication is implied. Such instances are

multiplying two bracketed expressions together, e.g.

(c - b)(c + b) = (c - b) * (c + b)

mulitiplication of an alphabetic symbol by a numeric constant, e.g.

2a = 2 * a

commonly used multiples, especially constant multiples of a, b or c and n, e.g.

ka = k * a

2ln = 2 * l * n

0.3.5.8 Operator Precedence

We shall assume the usual convention on operator precedence:

Exponention takes precedence over multiplication and division

Multiplication takes precence over addition and subtraction

A bracketed expression is evaluated before any of its left or right operators. Use of brackets therefore permits operator precedence to be over-ridden.

Some Examples

2a^n = 2 * (a^n)

(2a)^n = 2^n * a^n

a^n / 2 = (a^n) / 2

a^(n / 2) = (a^n)^(1 / 2)

2*(c + b)

Generally the precedence rules will be implied and brackets are only used to alter the precedence in an expression. However, to improve readability, brackets may be used in some cases although their presence may not be strictly necessary.

0.3.5.9 Usage of the term '2ln+1'

This is an extremely frequently used expression and it is defined as

2ln+1 = (2 * l * n) + 1

0.3.5.10 Non-standard symbols, notation

The readers attention is drawn to our usage of the some non-standard symbols and notation

negation symbol '!'

a != 2 denotes a not equal to 2

2 !| a denotes 2 does not divide a

nth root 'n_/'

3_/a denotes the cubic root of a

2_/(c - b) denotes the square root of (c - b)

2_/c - b = (2_/c) - b

0.4 Acronyms and Symbols

0.4.1 Acronyms

dp	Decimal Place
FLT	Fermat's Last Theorem
FST	Fermat's Little ('Small') Theorem
GCD	Greatest Common Divisor
GFLT	General FLT Equation
INT	Integer function
LDE	Linear Diophantine Equation
lhs	Left-hand side
MFLT	Modified FLT Equation
MFST	Modified FST Test
MRS	Minimal Residue Sequence
Qg	Quotient Gap
Rg	Root Gap
rhs	right hand side
TBC	To Be Confirmed
TBD	To Be Defined
wrt	with respect to

0.4.2 Symbols

For compatibility and simplicity reasons, this document is written in standard ASCII text format and can be read with a simple text editor, e.g. notepad. For this reason, certain symbols are non-standard

For compatibility and simplicity reasons, this document is written in standard ASCII text format and can be read with a simple text editor, e.g. Windows notepad. For this reason, certain symbols are non-standard

*	denotes multiplication
^	denotes exponentiation, e.g. X^2 reads X squared.
!	denotes 'not' when immediately followed by '|' or '=', otherwise it denotes factorial as per usual
n|a	denotes 'n divides a', for integers n,a
n!|a	denotes 'n does not divide a', for integers n,a
n!= a	denotes 'n is not equal to a', for integers n,a
!=	denotes 'not congruent to', e.g. X != Y (mod Z) reads X is not congruent to Y (mod Z)
~=~	denotes approximately equal
_/	denotes square root, e.g. _/x^2 = x
n_/	denotes nth root, e.g. 3_/x^3 = x
_k	when appended to an alphabetic letter, e.g. u_k, denotes the k'th element of a sequence or set

	e.g. u_k is the k'th Unity Root
|x|	absolute value of x, if x <0, |x| = -x. If x>= 0 |x| = x
[0,n-1]	closed interval of n integer values integers 0 to n- 1
[0, n)	semi-open interval of n integer values integers 0 to n- 1
(0, n]	semi-open interval of n integer values integers 1 to n
{u_i}	set of n Unity Roots, index i, 0 <= i < n - 1
(a,b,c)	an ordered triple of integers (a, b, c), 2 < a < b < c
a	Standard Base, lowest member of the triple (a, b, c).
A	generic modulus, one of {a, a^n, b, b^n, c, c^n, P}
b	Dual Base, middle member of the triple (a, b, c)
(x,y)	an ordered pair of integers (x,y), x <y
Bmax	Maximum value of b in an FLT counter-example
Cmax	Maximum value of c in an FLT counter-example
c	'Skew Base', largest member of the triple (a, b, c)
f(u)n	Unity Root Polynomial Exponent n
INT	Integer truncation. INT(x), for real x, is the largest integer value less than x
n	Exponent
p	quotient, (mod a^n)
p'	Dual quotient, (mod b^n)
P	arbitrary prime base
q	quotient
q'	Dual quotient
r	residue
u	Unity Root
u(a)	Unity Root (mod a^n)
u(b)	Dual Unity Root (mod b^n)
u_r	r'th Unity Root, u_0 = +1, u_1 > 1, 1 <= u_ < A
U	Set of n Unity Roots {u_0, u_1, .. u_(n - 1) }
U	Conjugate Set of n Unity Roots U' = -U
w	Winding number

0.5 Acknowledgements

(TBD)

1 Residues and Quotients

In this section we shall start by placing two conditions, termed the Residue and Quotient Condition, upon any possible solution triple (a, b, c) to Pythagoras and the FLT Equation. We show these two weak conditions are sufficient conditions such that, when they are both met, they can be used to generate Pythagorean triples and/or FLT counter-examples. A few example Pythagorean Triples confirm this and, indeed, by use of the analytic solution to Pythagoras, we can prove all Pythagorean triples meet both conditions. We then show that, for arbitrary exponent n, the Residue condition can be met for many 'Candidate Pairs' (b,c) where b^n = c^n (mod a^n), such that (a, b, c) is a solution to a General FLT Equation 'GFLT'. To meet the Quotient Condition we show that the difference between integers b and c, termed the 'Root Gap', of a Candidate Pair (b,c), is constrained to be less than the base if the triple (a, b, c) is to have any chance of being a FLT counter-example. Once again, in the Pythagorean case, we can prove this constraint on the Root Gap is satisified by all Pythagorean triples.

We also look at what we call the 'Dual' case, where the base is b and the modulus b^n, and we study Candidate Pairs (a,c) (mod b^n) which have to satisfy similar Dual Residue and Quotient Conditions. In combination these Standard and Dual conditions place tight constraints on any potential FLT counter-example.

Finally in this section we summarise the various constraints upon any Pythagorean Triples and FLT counter-examples solutions that have arisen, so far, in the course of the work.

Section (2) proceeds to the study of Residue Sequences, i.e. the residues x^n (mod a^n), 0 <= x < a^n and how their symmetry structure, for even exponent, can give rise to Pythagorean Triples and the consequent repurcussion for odd exponent.

1.1 The FLT and Pythagoras Equations

The work starts by placing constraints on the following Diophantine equation, referred to within this paper as the 'FLT Equation'.

1.1.1 a^n + b^n = c^n (the FLT Equation)

Although (1.1.1) applies to all exponents, n >= 2, the special case when n = 2 is termed the 'Pythagoras Equation'

1.1.2 a^2 + b^2 = c^2 (the Pythagoras Equation)

There are no integer solutions (a, b, c) to the FLT Equation (1.1.1) for integer n >2. So says Fermat's Last Theorem, finally proved by A Wiles [1].

1.2 The Residue Condition

By taking the residue of (1.1.1) (mod a^n)

1.2.1 a^n (mod a^n) + b^n (mod a^n) = c^n (mod a^n)

and using

1.2.2 a^n = 0 (mod a^n)

we obtain what is termed herein as the 'Standard Residue Condition' or more simply the 'Residue Condition'.

1.2.3 c^n = b^n (mod a^n) (the Residue Condition)

This shows that for any pair b and c of a triple (a, b, c) the residue b^n (mod a^n) is congruent to the residue c^n (mod a^n).

We term this expression (1.2.3) the Residue Condition since b^n and c^n have identical residues (mod a^n). This is a necessary but not sufficient condition upon any triple solution (a, b, c).

[Note that there is also a Dual Residue Condition (1.17.1), obtained by taking residues of (1.1.1) (mod b^n), and a Skew Residue Condition (2.5.1.18), obtained by taking residues of (1.1.1) (mod c^n)].

1.3 The Quotient Gap

The Residue Condition (1.2.3) implies that b^n and c^n can be written as follows, where we term integers p and q 'quotients', 0 <= p < q, and r is the integer residue, r >= 0, identical to both.

1.3.1 b^n = p*a^n + r

1.3.2 c^n = q*a^n + r

and we define the 'Quotient Gap' (Qg) as the positive difference of the quotients

1.3.3 Qg = q – p (the Quotient Gap)

1.4 The Quotient Condition

Substituting for b^n and c^n from (1.3.1) and (1.3.2) into (1.1.1) and cancelling the residue r implies that

1.4.1 $a^n + p*a^n = q*a^n$

Dividing throughout by a^n we obtain

1.4.2 $q - p = 1$

which, comparing with (1.3.3), becomes the 'Quotient Condition'

1.4.3 $Qg = 1$ (the Quotient Condition)

The Quotient Condition merely states that the Quotient Gap must be 1 for any Pythagorean Triple or FLT counter-example.

The Quotient Condition might just seem a restatement of the FLT equation since, by re-arrangement of (1.1.1),

1.4.4 $c^n - b^n = 1*a^n$

Nevertheless, like the Residue Condition, it is not sufficient by itself. A triplet satisfying only the Quotient Condition will not necessarily be a solution to (1.1.1). For instance, if b and c were of the form $b^n = r \pmod{a^n}$ and $c^n = s \pmod{a^n}$, where $r \neq s$ and $0 < r, s < a^n$, i.e. b and c do not meet the Residue condition, but are defined as follows,

1.4.5 $b^n = a^n + r$

1.4.6 $c^n = 2*a^n + s$

then the Quotient Gap is still unity since $q = 2$, $p = 1$. However, subtracting (1.4.5) from (1.4.6)

1.4.7 $c^n - b^n = a^n + (s - r)$

and, since $s \neq r$ by definition, the triple (a, b, c) is not a solution to (1.1.1).

1.5 Quotient & Residue Sufficiency

In essence, the Residue and Quotient Conditions split the single FLT equation into two weaker conditions. The Residue condition is a necessary condition and imposing the additional Quotient Condition upon it provides sufficiency.

We will see that the Residue Condition can be satisfied for all exponents n >= 2, whereas the Wiles Proof [1] confirms that both Residue and Quotient conditions can only be simultaneously satisfied when n = 2, i.e. the Pythagorean case.

Sufficiency Assertion

Any integer triple (a, b, c) satisfying both the Quotient and Residue condition is a solution to the FLT equation (1.1.1).

Proof

The Residue Condition (1.2.3) implies that b^n and c^n can be written, as given by (1.3.1) and (1.3.2) respectively, with quotients p and q and a common, identical residue r.

Subtracting (1.3.1) from (1.3.2) to eliminate the residue r we get

1.5.1 $c^n - b^n = q*a^n - p*a^n$

and rearranging, using (1.3.3) defining Qg, this becomes

1.5.2 $c^n = Qg*a^n + b^n$

We see from (1.5.2) that if Qg = 1 then we recover the FLT equation (1.1.1). But since Qg = 1 is simply the Quotient Condition (1.4.3) then any integer triplet (a, b, c) satisfying the Residue Condition (1.2.3) is a Pythagorean triple (n = 2) or FLT counter-example (n >2) if it also meets the Quotient Condition.

Since the two conditions are sufficient then, amongst the infinitude of triples (a, b, c) that meet the Residue Condition, any that also satisfy the Quotient condition are therefore FLT counter-examples. Since there exist solutions to the General FLT Equation (1.8) then a proof that the Quotient Condition can never be met for such GFLT solutions is equivalent to proof of FLT, i.e. the Quotient Condition becomes a restatement of FLT for GFLT.

1.6 Theorem: Pythagoras, Analytic Solution Sufficiency

If a Pythagorean Triple is given by ($u^2 - v^2$, $2uv$, $u^2 + v^2$), v > 0, integers u and v, u > v > 0, GCD(u,v) = 1, then it satisfies both the Residue and Quotient Conditions.

Proof

There are two cases to consider: 1) $u^2 - v^2 > 2uv$; 2) $u^2 - v^2 < 2uv$. The equality is not considered since it implies u = v which would imply one member of the Pythagorean triplet is zero which it is not, by definition.

By convention (0.3.3), we take a to be the smallest of the triplet (a, b, c) so that, in case 1, a = 2uv and, in case 2, a = u^2 - v^2.

Case 1: 2uv < u^2 - v^2

Let a = 2uv, b = u^2 - v^2, c = u^2 + v^2 then by squaring each term

1.6.1 a^2 = 4u^2*v^2

1.6.2 b^2 = u^4 - 2u^2*v^2 + v^4

1.6.3 c^2 = u^4 + 2u^2*v^2 + v^4

and since 4u^2*v^2 = 0 (mod a^2) by (1.6.1), taking the modulus a^2 of (1.6.2) and (1.6.3) gives

1.6.4 b^2 = u^4 + v^4 (mod a^2)

1.6.5 c^2 = u^4 + v^4 (mod a^2)

and hence equating b^2 with c^2 we see that

1.6.6 c^2 = b^2 (mod a^2)

and therefore case 1 satisfies the Residue Condition.

To prove the Quotient Condition, if we subtract (1.6.2) from (1.6.3)

1.6.7 c^2- b^2 = 4u^2*v^2

we see the difference c^2 - b^2 is identical to a^2 as given by (1.6.1). Hence case 1 satisfies the Quotient Condition.

Case 2: 2uv > u^2 - v^2, v > 0, u > v

Let a = u^2 - v^2, b = 2uv, c = u^2 + v^2,

Rearranging a = u^2 - v^2 for u^2 in terms of a and v^2

1.6.8 $u^2 = a + v^2$

and squaring b

1.6.9 $b^2 = 4u^2*v^2$

By substituting for u^2 from (1.6.8) into (1.6.9) gives

1.6.10 $b^2 = 4a*v^2 + 4v^4$

From $a = u^2 - v^2$ and $c = u^2 + v^2$ we can write c in terms of a

1.6.11 $c = a + 2v^2$

and consequently

1.6.12 $c^2 = a^2 + 4a*v^2 + 4v^4$

Taking the modulus a^2 of c^2

1.6.13 $c^2 = (4a*v^2 + 4v^4) \pmod{a^2}$

and hence equating (1.6.10) and (1.6.13) gives

1.6.14 $c^2 = b^2 \pmod{a^2}$

and we see that case 2 satisfies the Residue Condition.

To prove the Quotient Condition, if we subtract (1.6.9) from (1.6.12)

1.6.15 $c^2 - b^2 = a^2$

we see the difference $c^2 - b^2$ is identical to $1*a^2$, i.e. the Quotient Gap is 1 and hence case 2 satisfies the Quotient Condition.

1.7 Examples: Pythagorean Triples

Since Pythagorean triples are in abundance it is easy to verify the Residue and Quotients conditions with a few examples.

1.7.1 The Pythagorean triple (3,4,5)

We see that the Residue Condition is satisfied since

5^2 = 4^2 (mod 3^2) (25 = 16 mod 9)

And we have the following constructions for 4^2 and 5^2 in terms of 3^2

4^2 = 1*3^2 + 7 (16 = 1*9 + 7)

5^2 = 2*3^2 + 7 (25 = 2*9 + 7)

Showing that the quotients p = 1 and q = 2 meet the Quotient Condition.

1.7.2 The Pythagorean triple (8,15,17)

We see that the Residue Condition is satisfied since

17^2 = 15^2 (mod 8^2) (289 = 225 mod 64)

and we have the following constructions for 15^2 and 17^2 in terms of 8^2

15^2 = 3*8^2 + 33 (225 = 3*64 + 33)

17^2 = 4*8^2 + 33 (289 = 4*64 + 33)

showing that the quotients p = 3 and q = 4 meet the Quotient Condition

1.8 The General FLT Equation (GFLT)

For Qg>1 equation (1.6.2), reproduced below, is hereafter referred to as the 'General FLT Equation' and abbreviated to GFLT.

1.8.1 c^n = Qg*a^n + b^n (the General FLT Equation 'GFLT')

We will see that there are an abundance of solutions to GFLT, an infinite number in fact, all with Qg > 1. If we have a triple (a, b, c) satisfying GFLT and we make b negative, assuming odd n, we can take b^n over to the lhs and add it to c^n giving what is known as the 'Generalised Fermat Equation'.

1.8.2 b^n + c^n = Qg*a^n (the Generalised Fermat Equation)

This form is widely investigated, ref Mathworld [4], keyword 'Generalized Fermat Equation' (note the US spelling of Generalized with a ‘z’). In particular, there are only certain integral values Qg can take for a specific exponent.

Whilst we have implied the solutions of (1.8.2) have a negative value for b, this is merely because of our use of a^n in the modulus. We can obtain positive solutions by using a 'Skew' base c and taking residues of the FLT Equation (1.1.1) mod c^n. More details about this method and the Generalised Fermat Equation are provided in section (2.5.5). However, for now, we will mainly be concerned with GFLT (1.8.1).

The Quotient Gap Qg can legitimately be a perfect power of n, i.e. for some integer l, l > 1.

1.8.3 $Qg = l^n$

In which case, equation (1.8.1) becomes

1.8.4 $c^n = (la)^n + b^n$

Which shows that (a, b, c) is a triplet solution to GFLT and that (la,b,c) is actually also an FLT counter-example, n > 2. For n = 2 there do, of course, exist Pythagorean triples (a',b,c) where a' is composite, a' = la.

1.8.5 Pythagorean Example (8,15,17)

As a simple example, the Pythagorean triple (8,15,17)

1.8.5.1 $8^2 + 15^2 = 17^2$

This triple has a composite value of 8 for the base and equation (1.8.5.1) could be alternatively be written in GFLT form.

1.8.5.2 $(2^2)*4^2 + 15^2 = 17^2$

In this form the triple (4,15,17) will meet the Residue condition (mod 4^2) (a = 4 here) and will have a Quotient Gap of 2^2. This can be seen from the following construction of 15^2 and 17^2 in terms of the modulus 4^2

1.8.5.3 $15^2 = 14*4^2 + 1$

1.8.5.4 $17^2 = 18*4^2 + 1$

We see that the Residue Condition is met since 15^2 = 17^2 = 1 (mod 4^2) and that the quotients q and p are 18 and 14 respectively, hence Qg = 18 - 14 = 4 = 2^2 as in (1.8.5.2).

Alternatively, the composite b = 15 could be factored as follows

1.8.5.5 $8^2 + (3^3)*(5^2) = 17^2$

It can be viewed as a triple (8,5,15) (mod 5^2) that has Qg = 3^2 or, alternatively, as a triple (8,3,17) (mod 3^2) that has Qg = 5^2.

These example triples (4,15,17), (8,5,17) and (8,3,17) were actually reverse-engineered from a known Pythagorean triple (8,15,17) where a and/or b was composite. In fact any triple (a, b, c) where the values a or b are composite can be re-written in a GFLT form since we can just factor out the 'l', equation (1.8.4), from a or b. Furthermore, for any Pythagorean triple, since either a or b is always even but not both, one of them will always have a factor of 2 and therefore a Pythagorean triple of the form (a, 2x, c), here b = 2x, can always be written as a triple (a,x,c) such that

1.8.5.6 $a^2 + (2^2)*x^2 = c^2$

where the Quotient Gap is 2^2. Of course, this could also be viewed as a triple (a,2,c) with a Qg = x^2.

In fact, since the middle value b of a Pythagorean triple is always composite, section (1.15), there are at least two GFLT triples for every Pythagorean triple since there are always two or more factors in a composite.

1.8.6 GFLT Solutions

For arbitrary n, the GFLT equation (1.8.1) does have an infinite set of solutions. Since any residue x^n (mod a^n) repeats at $(a^n + x)^n$ (mod a^n) i.e.

1.8.6.1 $(a^n + x)^n = x^n \pmod{a^n}$

Although stated without proof, by expanding the lhs of (1.8.6.1) binomially, and taking residues (mod a^n), all terms are congruent to zero except the last term x^n]. By associating b with x and c with $a^n + x$ in (1.8.6.1) then (a, b, c) is a triple satisfying the Residue condition since

1.8.6.2 $c^n = b^n \pmod{a^n}$

As both x and a are arbitrary integers the set of triplet solutions to the GFLT equation is infinite.

Any triple given by

1.8.6.3 (a, x, a^n + x)

will satisfy GFLT.

The triples given by (1.8.6.3) are not the only solutions. There is a more select group which might offer hope, false we might add, of finding an FLT counter-example. See, for example, section (1.8.9).

Since there are so many GFLT solutions for every exponent it raises the immediate question as to why none of the solutions meets the Quotient Condition except when n = 2? Whilst it is not difficult to see that Qg >> 1 for a triple given by (1.8.6.3), it is not obvious that Qg is not a perfect power as per (1.8.3). In fact, as we shall see in the Pythagorean case, none of the solutions originate via the Repeat Residue mechanism given by (1.8.6.1). This mechanism merely makes for an easy example but is not seriously considered further except in the next example.

1.8.7 Cubic Exponent Example 1

Firstly, a relatively trivial example illustrating (1.8.6.1) and GFLT

The triple (5, 7, 132) has been constructed in accordance with (1.8.6.1) where n = 3, the base a = 5 and x = 7, hence a^n + x = 132.

Expanding 7^3 and 132^3 in terms of 5^3

1.8.7.1 7^3 = 2*5^3 + 93

1.8.7.2 132^3 = 18399*5^3 + 93

and hence 7^3 and 132^3 meet the Residue Condition (mod 5^3) since

1.8.7.3 7^3 = 132^3 = 93 (mod 5^3)

Subtracting (1.8.7.1) from (1.8.7.2) we get

1.8.7.4 132^3 - 7^3 = 18397*5^3

and re-arranging gives a GFLT form with a Quotient Gap of 18397 as follows

1.8.7.5 132^3 = 18397*5^3 + 7^3

1.8.8 Cubic Exponent Example 2

This next example, the triple (3, 4, 13), n = 3, illustrates a Repeat Residue mechanism not given by (1.8.6.1). A summary of mechanisms by which residues repeat is given in section (2.2). However, in this example, it should be noted that the exponent n = 3 divides the base a = 3 and, as a consequence, the Residue Sequence is 'Minimal', see (2.1.2.2). Basically, this means the residues repeat at a shorter interval than a^n (1.8.6.1). In fact they repeat at a^n / n. In this case, a^n = 3^3 = 27 and hence a^n / n = 9. This is why the third value of the triple c = 13 has been constructed from c = b + a^n / n = 4 + 9 = 13.

Expanding 4^3 and 13^3 in terms of 3^3

1.8.8.1 $4^3 = 2*3^3 + 10$

1.8.8.2 $13^3 = 81*3^3 + 10$

and hence 4 and 13 meet the Residue Condition (mod 3^3) since

1.8.8.3 $4^3 = 13^3 = 10 \pmod{3^3}$

Subtracting (1.8.8.1) from (1.8.8.2)

1.8.8.4 $13^3 - 4^3 = 79*3^3$

and re-arranging we get a GFLT form with a Quotient Gap of 79 as follows

1.8.8.5 $13^3 = 79*3^3 + 4^3$

1.8.9 Cubic Exponent Example 3

Lastly, a triple (7, 17, 20), n = 3, whereby the Repeat Residue mechanism is of the '2ln+1' form, see section(2.2.5). Basically, the base value a = 7 can be written as twice a multiple of the exponent n = 3, plus 1, in this case 7 = 2*3 + 1. This mechanism is of major importance in the further study of the FLT equation within this paper, essentially it is the only mechanism whereby FLT counter-examples could be (but aren't) possible. All other mechanisms, examples 1 and 2 for instance, being rejected. A summary of all mechanisms by which a residue can repeat is given in section (2.2).

Expanding 17^3 and 20^3 in terms of 7^3

1.8.9.1 17^3 = 14*7^3 + 111

1.8.9.2 20^3 = 23*7^3 + 111

and hence 17 and 20 meet the Residue Condition (mod 7^3) since

1.8.9.3 17^3 = 20^3 = 111 (mod 7^3)

Subtracting (1.8.9.1) from (1.8.9.2)

1.8.9.4 20^3 - 17^3 = 9*7^3

and re-arranging gives a GFLT form with a Quotient Gap of 9 as follows

1.8.9.5 20^3 = 9*7^3 + 17^3

1.9 Definitions: Candidate Pair and Repeat Residues

1.9.1 Definition: Candidate Pair

If b and c meet the Residue condition (1.2.3) then the pair of values is termed a 'Standard Candidate Pair' and denoted by (b,c). The prefix 'Standard' is usually removed when the modulus a^n is implied.

1.9.2 Definition: Repeat Residues

Two integers x and y are termed 'Repeat Residues' if, when raised to an integer exponent n and taking residues (mod z^k), integer z, integer exponent k, 0<k<=n, then x^n and y^n are congruent mod z^k, i.e. if

1.9.2.1 x^n = y^n (mod z^k) (integer k, 0<k<=n)

then x and y are 'Repeat Residues' mod z^n.

Specifically, in this paper, we are only interested in two particular cases where the exponent k = 1 or k = n, i.e. the modulus is z or z^n, then we have either

1.9.2.2 x^n = y^n (mod z^n) (x and y are termed Repeat Residues mod z^n)

or

1.9.2.3 x^n = y^n (mod z) (x and y are termed Repeat Residues mod z)

By definition, the values b and c of a Standard Candidate Pair (b,c) are Repeat Residues because b^n = c^n (mod a^n) by the definition (1.9.1) of a Candidate pair. Similarly, in the Dual case, the values a and c of a Dual Candidate Pair (a,c) are Repeat Residues since a^n = c^n (mod b^n), see further, (1.17).

In section (2.5.7) we shall see that residues (mod z), where z is either a, b or c of a triple (a, b, c) and the exponent n = 1, play an important part in the development of constraints upon possible FLT counter-examples.

1.10 Definition: Standard Root Gap

The Standard Root Gap, denoted by 'Rg' and more commonly referred to simply as the Root Gap, is defined as the numeric, positive difference between the values b and c of a Candidate Pair (b,c), where it is assumed c > b by convention (0.3.3.3),

1.10.1 Rg = c - b

In GFLT triplet, (1.8.6.3) above, the Root Gap is a^n. However, we will see, by Theorem (1.12), it must be much smaller than this for (a, b, c) to be an FLT counter-example. It is called a 'Root' Gap because b and c are effectively the roots of an equation

1.10.2 x^n - r = 0 (mod a^n)

and they share, by the definition of a Candidate Pair (b,c), an identical residue 'r', i.e.

1.10.3 b^n = r (mod a^n)

and

1.10.4 c^n = r (mod a^n)

For example, in the Pythagorean case, equation (1.10.2) is the Quadratic Diophantine equation

1.10.5 x^2 - r = 0 (mod a^2)

This equation can have no roots, 2 roots or a multiple of 2 roots in the interval [0, a^2). There only exist roots when r is a quadratic residue of a, i.e. if r is not a quadratic residue of a then there are no roots.

However, excepting Pythagoras, we are chiefly concerned within this paper with odd prime exponent, n >= 3 and, as regards roots to (1.10.2), there are either no roots or n roots for prime base, Lagrange's Theorem, see (2.2.5.3).

1.11 Definition: Consecutive Identical Residues

If a Candidate Pair (b,c) has a Root Gap of unity such that, by (1.10.1) Rg = 1, and therefore

1.11.1 $c - b = 1$

then the pair of values b and c are termed 'Consecutive Identical Residues', sometimes abbreviated to CIR. By the definition of a Candidate Pair the residues will be equal, hence 'identical' and, by (1.11.1), the value c is the next 'consecutive' integer after b.

Consecutive Identical Residues are an important concept when the base is prime, section (1.14).

1.12 Theorem: Root Gap Constraint

If the Root Gap for a Candidate Pair (b,c) (mod a^n) is greater than or equal to the base a then the Quotient Gap is greater than unity for all n > 1, i.e.

If

$Rg >= a$

then

$Qg > 1$

Alternatively stated, if we are to meet the Quotient Condition (1.4.3), then the Root Gap must be less than a.

If

$Qg = 1$

then

$Rg < a$

This is a necessary condition, not a sufficient condition. In general, we shall see that the Root Gap has to be a lot less than the base for a unity Quotient Gap.

Proof

By hypothesis, the Root Gap is greater than the base, i.e.

1.12.1 c - b >= a

Rearranging and raising to the n'th power we get

1.12.2 c^n >= (a + b)^n

Expanding the rhs by the binomial theorem, where nCr denotes the binomial coefficient n! / (n -r)! r!,

1.12.3 c^n >= a^n + nC1*a^(n - 1)*b

.
.
+ nCr*a^(n - r)*b^r
.
.
+ nC(n - 1)*a*b^(n - 1)
+ b^n

Now, since a < b by choice, substituting for a in place of b for all terms of order b^(n - 1) or less, this implies

1.12.4 c^n > a^n + nC1*a^(n - 1)*a

.
.
+ nCr*a^(n - r)*a^r
.
.
+ nC(n - 1)*a*a^(n - 1)
+ b^n

This inequality is now homogeneous in a^n and, using nC0 = 1, this simplifies to

1.12.5 c^n > (nC0 + nC1 + .. nCr + .. nC(n - 1))*a^n + b^n

Since the binomial coefficients nC0 to nCn sum to 2^n, then the bracketed sum above, which omits the last term nCn (= 1), sums to 2^n - 1 giving:

1.12.6 c^n > b^n + (2^n - 1)*a^n

Comparing (1.12.6) with (1.8.1) the Quotient Gap is seen to be given by

1.12.7 Qg = 2^n - 1

We see that if n >1 then

1.12.8 Qg > 1

Thus, for all n >1, if the Root Gap is greater than a, i.e. if c - b > = a then the Quotient Gap is greater than unity.

1.12.9 Remarks

Theorem (1.12) says that for any Candidate Pair (b,c) (mod a^n), to meet the Quotient Condition (1.4.3), the gap between b and c must be less than the base a. Alternatively expressed, any two integers b and c, where c > b > 3, with identical residues such that c^n = b^n (mod a^n), for n >= 2, can only be a valid Pythagorean triple or FLT counter-example if c - b < a.

Although we have given the proof in the Standard case where the base is a and the Candidate Pair is subsequently (b,c), the Theorem is equally valid in the Dual case with base b and Candidate Pair (a,c). This is because, in the Standard case, if c - b < a then it simply re-arranges to c - a < b and, in the Dual case, the Candidate Pair is (a,c) and the Base is b.

Note that Theorem (1.12) does not state that if the Root Gap is less than the base then the Quotient Gap will always be unity. It only says that the Quotient Gap will never be Unity if the Root Gap is greater than the base.

To emphasize Theorem (1.12) further.

There are no Pythagorean Triples (a, b, c), 2 < a < b < c such that c - b >= a

There are no FLT counter-examples (a, b, c), 2< a < b < c such that c - b >= a

Of course, there are no FLT counter-examples, Wiles [1]. Nevertheless, it is worth exploring how Pythagoras succeeds where others fail in the hope that it may offer some insights into FLT.

1.13 Pythagoras Root Gap < base

One can verify all Pythagorean triples (a, b, c) have a Root Gap less than the base by using the standard analytic solution.

Firstly, defining a, b and c as follows using the standard analytic solution for a Pythagorean triple

1.13.1 $a = 2uv$

1.13.2 $b = u^2 - v^2$

1.13.3 $c = u^2 + v^2$

Since

1.13.4 $b > 0$

this implies, using (1.13.2), that

1.13.5 $u^2 - v^2 > 0$

and since, by convention, a is positive then we have

1.13.6 $|u| > |v|$

Subtracting b from c using (1.13.2) for b and (1.13.3) for c we get

1.13.7 $c - b = 2v^2$

and, using inequality (1.13.6), this implies

1.13.8 $c - b < 2uv$

Substituting for a from (1.13.1) implies

1.13.9 $c - b < a$

Hence, if a is defined as the even valued member of the triple (a, b, c) as defined by (1.13.1), then the Root Gap of a Pythagorean triple is always less than the base modulus a.

To prove the case when a and b are swapped, such that b is now the even member of the triple and a is the odd member

rearranging (1.13.9) gives

1.13.10 c - a < b

If we swap a (1.13.1) with b (1.13.2) such that we now have

1.13.11 b = 2uv

1.13.12 a = u^2 - v^2

then since we have just proven (1.13.9) when using (1.13.1) for a and (1.13.2) for b, then with the definition of a and b now swapped, i.e. b now defined by (1.13.11) and a now defined by (1.13.12), then (1.13.10) is also proven. Hence the Root Gap (c - b) is always less than the modulus a for a Pythagorean Triple.

1.14 Theorem: Prime Base a, Root Gap = 1

If the base a is prime then the Root Gap for a Candidate Pair (b,c) is unity for any FLT counter-example or Pythagorean triple.

Proof

Starting with the FLT equation (1.1.1) and re-arranging for a in terms of c and b we get

1.14.1 a^n = c^n - b^n

Expanding c^n - b^n binomially and assuming n >= 2 then

1.14.2 a^n = (c- b)(c^(n - 1) + ... + b^(n - 1))

By (1.10.1) this can be expressed in terms of the Root Gap, Rg

1.14.3 a^n = Rg*(c^(n - 1) + ... + b^(n - 1))

The right hand side of (1.14.3) factors in two terms and, since the base is prime, each of these terms must be some power of a with no other factor involved. This implies Rg must be of the from a^k for some integer k, k >= 0.

1.14.4 Rg = a^k

But, by Theorem (1.12), if the Root Gap is greater than or equal to the base, then the Quotient Gap is greater than unity, i.e. if Rg >= a then Qg > 1. Conversely, if the

Quotient Gap is unity, the Root Gap must be less than a, i.e. if Qg = 1, then Rg < a. However, by (1.14.4), the only value for Rg less than a is unity since a is prime. Hence, if a is prime and the Quotient Gap is unity, then the Root Gap must also be unity and k = 0 in (1.14.4).

The consequence of this proof is that the two values b and c must be 'Consecutive Identical Residues', section (1.11). That is, if a is prime and Rg = 1 then, by (1.10.1), c = b + 1.

Note that Qg cannot be zero since 0 < a < b < c and (b,c) are a Candidate Pair (mod a^n). Hence b and c have identical residues and cannot therefore have identical quotients q, p such that Qg = q - p = 0 unless b = c which is false since b < c by convention.

Alternative Proof

This proof can also be presented without recourse to Theorem (1.12). Let us suppose the Root Gap is not unity. The next smallest value it can be is a when k = 1 in (1.14.4).

If we let k = 1, then

1.14.5 Rg = a

and therefore, by the definition of the Root Gap (1.10.1),

1.14.6 c = a + b

and substituting for Rg and c into the rhs of (1.14.3) we get, for some integer coefficients k1, k2, .. kr > 0,

1.14.7 a^n = a*(a^(n - 1) +
k1*a^(n - 2)*b^2 +
k2*a^(n - 3)*b^3 +
... +
kr*a^(n - r - 1)*b^r +
... +
+ n*b^(n - 1))

Upon multiplying through the rhs bracket by a, the first term is a^n which cancels with the lhs a^n leaving

1.14.8 0 = a * (k1*a^(n - 2)*b^2 +
k2*a^(n - 3)*b^3 +
... +
kr*a^(n - r - 1)*b^r +

... +
+ n*b^(n - 1))

This equation can only have a solution if a = 0 or the outer bracket is zero. However, since a > 0,and all terms inside the bracket are greater than zero, this equation cannot be satisified. Therefore our original assumption that Rg = a is false and we are left with the conclusion that either Rg = 1 or Rg > a. However, if we let Rg = a^k, k >1, we will arrive at the same contradiction as for (1.14.8) and so the only solution left is k = 0, i.e. Rg = 1. Therefore we conclude that if the base a is prime then the Root Gap is unity.

Both proofs were given using the expansion in (1.14.2) which assumed n >= 2. Hence the Theorem is valid for both Pythagoras and FLT. However, there is a simpler Proof for the Pythagorean case, given here for completeness.

Starting with the expansion of (1.14.2) for n = 2 we have

1.14.9 a^2 = (c + b)(c - b)

and we see that a^2 factors simply into (c+b) and (c- b)

If a is prime then, since a^2 has two factors (c + b) and (c - b), one of them must be unity since they cannot both be the same as (c + b) > (c - b) for all c > b > 0 which is true by assumption. The unity factor must therefore be the smallest factor of the two, namely (c - b) i.e.

1.14.10 c - b = 1

But the lhs of (1.14.10) is the Root Gap (1.10.1) hence, if a is prime, any triple (a, b, c) that satisfies the Pythagoras equation has a Root Gap of unity.

Remark

Unfortunately we cannot restrict our studies in this paper to prime base only, we must also consider composites. This is because, if we restricted the study to prime base only, we would need to observe not just unity Quotient Gaps but also those where the Quotient Gap is a perfect power. Conversely, by considering only composite a, we can limit ourselves to searching for unity Quotient Gaps only. This is because if there is a perfect power, Quotient Gap = l^n, (mod a^n), i.e.

1.14.11 c^n - b^n = l^n*a^n

then defining

1.14.12 a' = la

equation (1.14.11) can be re-written in unity Quotient Gap form, (mod a'^n).

1.14.13 $c^n - b^n = a'^n$

This shows there is a composite a' = la, such that (a', b, c) is an FLT counter-example. That is, any triple (a, b, c), where (b,c) is a Candidate Pair (mod a^n), and such that the Quotient Gap is a perfect square, l^n, has a 'normalised' form (la, b, c) such that the Candidate Pair (b,c) mod (la)^n has a unity Quotient Gap.

1.15 Theorem: Composite Middle Value

The middle value b of an FLT counter-example is always composite.

Theorem (1.12) proves that if the Quotient Gap for a Candidate Pair (b,c) (mod a^n) is unity, i.e. (a, b, c) is an FLT counter-example, then the Root Gap must be less than the base, i.e. if Qg = 1 then Rg < a. Theorem (1.18) then goes further to prove that if the base is prime then the Root Gap is always unity. By alternatively studying the Dual problem, i.e. the Candidate Pair (a,c) (mod b^n), we can prove that the base b is always composite.

The Dual Root Gap, Rg', for a Candidate Pair (a,c) (mod b^n), is defined as

1.15.1 $Rg' = c - a$

We can re-arrange the inequality of Theorem (1.12) on the Root Gap to give a Dual equivalent, Rg' where

1.15.2 $Rg' = c - a < b$

By rearranging the FLT equation (1.1.1) for b in terms of a and c

1.15.3 $b^n = c^n - a^n$

and expanding the rhs binomially, assuming n >= 2, then

1.15.4 $b^n = (c - a)(c^{(n - 1)} + \ldots a^{(n - 1)})$

we can get a 'Dual' equivalent expression of (1.14.3) linking Rg' and b

1.15.5 $b^n = Rg' * (c^{(n - 1)} + \ldots a^{(n - 1)})$

If we assume b is prime then we can conclude that Rg' is unity by the same argument as in Theorem (1.14). However since a < b < c and they are all integers, this implies c - a > = 2. i.e. Rg' >= 2 which contradicts the assumption that Rg' is unity if b is prime. So, we conclude that b cannot be prime and must therefore be composite.

Since the binomial expansion (1.15.4) is valid for n >= 2, this Theorem is valid for both the Pythaogorean and FLT cases.

1.16 Residue Tables

Fortunately much, if not all, of the findings in this paper can be verified experimentally (but not proven) with a computer. The key aid in the study of Repeat Residues is the generation of 'Residue Tables'. These allow a relatively quick visual inspection of finding Repeat Residues for a specific base and exponent.

A Residue Table is a 5-column table of residues r where x^n = r (mod a^n) for x = 0 to x = (a^n) - 1. Note that the quotient p is also tabulated.

A Residue Table can be interpreted as either Standard or Dual. Both tables have the same structure and are identical except for the modulus and, as a consequence, the number of entries. A Standard Table has a modulus a^n, the Dual Table has modulus b^n. However, whether a Residue table is Standard or Dual is actually just a matter of interpretation. For example, if one generates a table of residues (mod 3^2) and identifies elements b = 4, c = 5 as having identical residues (mod 3^2) (as they do) then, since the base a = 3 is less than the middle value of the triple b = 4, this table could be interpreted as a Standard Residue table with respect to the Pythagorean triple (3,4,5). Alternatively, if one was examining a Residue Table (mod 4^2) and identifies that elements b = 3, c = 5 as having identical residues (mod 4^2), then since the base b = 4 is the middle value of the triple (3,4,5), the table can be regarded as a Dual table with respect to the Pythagorean triple (3,4,5).

1.16.1 Standard and Dual Residue Tables

The columns in a Standard (and Dual) Residue Table are as follows:

Column 1:	x	(0 <= x < a^n)
Column 2:	x^n	
Column 3:	residue r	r = x^n (mod a^n)
Column 4:	residue r	r = x^n (mod a)
Column 5:	quotient q	x^n = p*a^n + r

Strictly speaking, we have used the residue r and quotient p as used for a base a. In the dual case, we should write residue r' and quotient p' for the dual equivalent residue table for base b. However, this is not done and please keep in mind that all residues r, r' and quotients p, p' (and often a and a') are all essentially one and the same meaning, just different context.

An example Residue Table is shown below for the case a = 5, n = 2

```
      Residue Table a = 5, n = 2
   x        x^n    residue  residue quotient
```

		(mod a^n)	mod a	
0	0	0	0	0
1	1	1	1	0
2	4	4	4	0
3	9	9	4	0
4	16	16	1	0
5	25	0	0	1
6	36	11	1	1
7	49	24	4	1
8	64	14	4	2
9	81	6	1	3
10	100	0	0	4
11	121	21	1	4
12	144	19	4	5
13	169	19	4	6
14	196	21	1	7
15	225	0	0	9
16	256	6	1	10
17	289	14	4	11
18	324	24	4	12
19	361	11	1	14
20	400	0	0	16
21	441	16	1	17
22	484	9	4	19
23	529	4	4	21
24	576	1	1	23
25	625	0	0	25

Notes

The residue (mod a), column 4, is also shown in addition to the residue (mod a^n), column 3, since it is useful in the study of residues (mod a^n). For example, if there are two values x and y such that they are congruent (mod a^n), i.e. y^n = x^n (mod a^n), then they are also congruent (mod a), i.e. y^n = x^n (mod a). For large a, the identification of x,y with identical residues (Repeat Residues) (mod a^n) can be visually identified quicker by first checking those with identical residues (mod a). If x and y are such that they do not share an identical residue (mod a), then they will not have an identical residue (mod a^n). For small a, very approximately a = 100, this is not particularly necessary but it can be useful when a is very large.

As a specific example of Repeat Residues, one can see in the table above that x = 12, when squared, has the same residue (19) as for x = 13 when squared, i.e. 12^2 = 19 (mod 5^2) and 13^2 = 19 (mod 5^2). The pair (12,13) thus form a Candidate Pair. Inspection of the quotients reveals that for x = 12, p = 5 (12^2 = 5*5^2 + 19) and for y= 13, q = 6 (13^2 = 6*25 + 19) and thus q - p = 1 and therefore meets the Quotient Condition. Since the Candidate Pair (12,13) meets both the Residue and Quotient Conditions we can conclude from the Sufficiency Theorem (1.5) that (5,12,13) is a Pythagorean triple. From this we can see that by studying Residue tables, (mod a^n), we can identify Pythagorean Triples of the form (a, b, c) where (b,c) is a Candidate Pair which meets the Residue Condition, by definition, and simultaneously satisfies the Quotient Condition.

The x = 25 (5^2) residue is shown primarily for completeness: 25 = 5^2 = 0 (mod 5^2), and confirms that, for reasons of computational checking, the x = 25 entry is

identical to that for x = 0. Of course, for any integer i, (a^n + i)^n = i^n (mod a^n) so that the entire set of residues for 0 <= x < a^n repeat, in the same sequence, for a^n <= x <2a^n, 2a^n <= x < 3a^n etc. which is why we need only tabulate the first a^n entries, 0 <= x < a^n.

1.17 Dual Residue Condition

So far, most of the focus has been on residues (mod a^n) where a is the smallest of an integer triple (a, b, c). However, the FLT equation (1.1.1) is interchangeable in a or b. Whilst keeping with the convention, a < b < c, we can effectively double up the Quotient and Residue Conditions, (1.2.3) and (1.4.3) respectively and obtain Dual equivalents.

The Dual equivalent of the Residue Condition (1.2.3) is

1.17.1 c^n = a^n (mod b^n) (the 'Dual Residue Condition')

This shows that for any pair (a,c) of a triple (a, b, c), the residue a^n (mod b^n) is equal to the residue c^n (mod b^n).

The reciprocal nature of the Residue Conditions (1.2.3) and (1.17.1) are quite restrictive. Individually they are easily satisfied for either base a or b and all exponents and lead to a GFLT equation, section (1.8). Taken together, they are much more restrictive but, nevertheless, give rise to a more general Diophantine equation which we have tentatively named the Modified FLT equation 'MFLT'

1.17.2 c^n = a^n + b^n + k*a^n*b^n

This does have solutions and is briefly discussed in section (**Error! Reference source not found.**), albeit it is the subject of a separate paper ref. [5].

1.17.3 Duality of Candidate Pairs (b,c) and (a,c)

If (a, b, c) is an FLT counter-example then both (b,c) (mod a^n) and (a,c) (mod b^n) are Candidate Pairs.

This statement is really just a formalisation of the Standard Residue Condition (1.2.3) and the Dual Residue Condition (1.17.1).

If (a, b, c) is an FLT counter-example then, by taking residues (mod a^n) of the FLT equation (1.1.1), we obtain the Residue Condition (1.2.3). Since this shows that b^n is congruent to c^n (mod a^n) they therefore have equal residues and, by definition, (b,c) (mod a^n) is thus termed a Candidate Pair. However, equally, we can take residues, (mod b^n), of the FLT equation (1.1.1) and obtain (1.17.1). Since this shows that a^n is congruent to c^n (mod b^n), they therefore have equal residues and, by

definition, (a,c) (mod b^n) is termed a Dual Candidate Pair. Hence both (b,c) (mod a^n) and (a,c) (mod b^n) are Candidate Pairs; the Candidate Pair (a,c) (mod b^n) is the Dual equivalent of (b,c) (mod a^n).

1.18 Dual Quotient Condition

By analogy with (1.3.1) and (1.3.2) the Dual Residue Condition implies that a^n and c^n can be written as follows (the primed values denote Dual):

1.18.1 $a^n = p'*b^n + r'$

1.18.2 $c^n = q'*b^n + r'$

where p' and q' are 'quotients' and 'r' is the residue identical to both.

However, before continuing to derive the Dual Quotient Condition, since a < b by convention, we see that p' in (1.18.1) is zero when we keep with the convention that r' is zero or positive. Note that a zero residue is of no interest since it implies a and b, or b and c, contain a common factor, i.e. they are not co-prime.

Thus, with p' defined as zero,

1.18.3 $p' = 0$

then (1.18.1) shows that

1.18.4 $r' = a^n$

and therefore and (1.18.2) can be re-written

1.18.5 $c^n = q'*b^n + a^n$

Substituting for c^n from (1.18.5) into the FLT equation (1.1.1) and cancelling the residue r' (= a^n) we get

1.18.6 $b^n = q'*b^n$

and dividing throughout by b^n we obtain a Dual Quotient Condition

1.18.7 q' = 1 (the Dual Quotient Condition)

Whereas in the Standard Quotient Condition we have two quotients p, q each greater than unity, but with the condition q - p = 1, for this Dual Quotient Condition we must have p' identically zero and q' identically unity. So, if we study a Dual Table, we need only look for values c where the quotient q' is unity. At the point x = b then q' = 1 since x^n = 1*b^n and at the point x = 2b then q' = 2^n since x^n = 2^n*b. Therefore somewhere in between x = b and x = 2b the quotient q' becomes greater than unity and we can end our search for a value x = c, such that c^n = a^n (mod b^n).

1.19 Bmax

The Quotient Condition places an upper limit on the value of b in a Candidate Pair (b,c) (mod a^n).

1.19.1 Theorem

Given a Candidate Pair (b,c) (mod a^n) there exists a value Bmax, in general non-integral and an element of the Reals such that, for b >= Bmax, the Quotient Condition can never be met.

This is equivalent to the following statement upon any FLT counter example:

If (a, b, c) is an FLT counter-example, odd exponent n >= 3, 1 < a < b < c, then the middle value b is always less than a value Bmax where Bmax is defined via the relation:

$$n*Bmax^{(n - 1)} = 2*a^n$$

Proof

For a given value of b, Candidate Pair (b,c), to minimise the Quotient Gap, we need to minimise the Root Gap. This is almost self-evident since, for any given triple (a, b, c), if Rg = k such that c - b = k by (1.10.1), then c^n - b^n = (b + k)^n - b^n = Qg*a^n, by (1.8.1), and therefore Qg is minimised if k = 1. The value of k cannot be zero since this would imply b = c which is not a valid Candidate Pair (it would mean a = 0).

Thus, if the minimum Root Gap is unity then, by (1.10.1), the values b and c are consecutive

1.19.1.1 c = b + 1

In which case b and c are termed 'Consecutive Identical Residues', (1.11). The Candidate Pair is thus (b, b + 1) and, by (1.8.1), the Quotient Gap is given by

1.19.1.2 Qg*a^n = (b + 1)^n - b^n

Since we wish to disregard all Candidate Pairs for which the Quotient Gap is greater than unity, we wish to find a maximum value b, denoted by Bmax, such that for all b > Bmax the Quotient Gap satisifies the following condition

1.19.1.3 Qg >= 2

A binomial expansion of the rhs of (1.19.1.2), gives us the following inequality such that for all n >= 2,

1.19.1.4 (b + 1)^n - b^n > n*b^(n - 1)

If we choose a value b = Bmax whereby Bmax is defined via the relation

1.19.1.5 n*Bmax^(n - 1) = 2*a^n

where the lhs of (1.19.1.5) purposefully matches the rhs of (1.19.1.4) when b = Bmax, then inequality (1.19.1.4) implies

1.19.1.6 (Bmax + 1)^n - Bmax^n > n*Bmax^(n - 1) = 2*a^n

and this implies the Quotient Gap at b = Bmax, by (1.19.1.2), satisifies the inequality

1.19.1.7 Qg*a^n > n*Bmax^(n - 1) = 2*a^n

i.e. if b = Bmax, then Qg > 2 since the a^n factor cancels in (1.19.1.7).

The Bmax value in (1.19.1.5) is generally non-integral and real-valued. For example, if a = 7, n = 3, then Bmax is 15.12 to 2dp. We can actually round this down to the nearest integer since rounding up, as we shall show below, can only give an even larger Quotient Gap. However, doing this means that we must consider values of b <= Bmax instead of b < Bmax. We will assume throughout that Bmax is not rounded to an integer and, generally, remains real-valued and non-integral.

It remains to show that if b >= Bmax then Qg >= 2 always holds true.

To do this, we have to show that if (b, b + 1) is a Candidate Pair with Quotient Gap Qg and (b + k, b + k + 1), integer k, k > 0, is another Candidate Pair with Quotient Gap Qg' then the integral Quotient Gap Qg' is greater than or equal to Qg, i.e. the Quotient Gap either remains the same or increases as b increases, but never decreases.

Note that for both Candidate Pairs we have only chosen a Root Gap of unity in each case. Since we have reasoned (but not rigorously proven) that the minimum Quotient

Gap occurs for a minimimum Root Gap of unity then more general Candidate Pairs with non-unity Root Gaps need not be considered.

With the Quotient Gap Qg for Candidate Pair (b, b + 1) given by

1.19.1.8 $(b + 1)^n - b^n = Qg*a^n$

and the Quotient Gap Qg' for Candidate Pair (b + k, b + k + 1) given by

1.19.1.9 $(b + k + 1)^n - (b + k)^n = Qg'*a^n$

then we have to show that, for all $k > 0$,

1.19.1.10 $Qg' >= Qg$

which, by multiplication by a^n and re-arranging, is equivalent to showing that

1.19.1.11 $Qg'*a^n - Qg*a^n >= 0$

Without going into the algebra, it can be shown, by the binomial expansion of $(b + k)^n$ and $(b + k + 1)^n$ that for all $b >= 1$, $k >= 1$, $n >= 1$, the following inequality holds true

1.19.1.12 $(b + k + 1)^n - (b + k)^n >= (b + 1)^n - b^n$

then, by comparison with (1.19.1.8) and (1.19.1.9), this implies (1.19.1.10) is true for all $b >= 1$, $k >= 1$, $n >= 1$,

With $1 < a < b < c$ by convention (0.3.3), $b = 3$ is actually the smallest middle value under consideration. Similarly, $n = 2$ is the smallest exponent. The value of k is arbitrary but, for the smallest possible Root Gap, as prior stated, $k = 1$.

Thus we have shown that $Qg >= 2$ for all $b >= Bmax$ where Bmax is defined by (1.19.1.5), rounded down to the nearest integer.

1.19.2 Notes

What about the other value c in a Candidate Pair (b,c)? Since b must actually be less than Bmax the maximum value for c is b + 1 when the Root Gap is minimal, i.e. $Rg = 1$. In terms of Bmax, this value of c is INT(Bmax)+1 where the 'INT' function denotes truncation to the nearest integer, see (0.4.2). What we actually have are the two conditions:

1.19.2.1 b < Bmax

1.19.2.2 c <= INT(Bmax)+1

Which might then beg the question, why not call (1.19.2.2) Cmax and use that instead since c > b by convention? Firstly, equation (1.19.1.2) was written in terms of b not c hence it would not seem right to then call it Cmax. Secondly, C'max is used for the Dual equivalent condition, see (1.20).

Lastly, for the two smallest exponents under consideration, for Pythagoras (n = 2) we get for Bmax

1.19.2.3 Bmax = a^2

and for the smallest, odd FLT exponent, n = 3, we get

1.19.2.4 Bmax = _/(2*a^3 / 3) (where '_/' denotes the square root)

1.19.3 Example

1.19.3.1 n = 3, a = 7

Using (1.19.2.4) for the n = 3, a = 7 case, we get for Bmax

1.19.3.2 Bmax = 15.2 to 1dp.

If we look at the Residue Table for n = 3, a = 7, of which the entries 7 <= x <= 21 are reproduced below, we see that the quotient values (last column) from x = INT(Bmax) (= 15) onwards are 9, 11, 14, 17, 19, 23, 27 with corresponding Quotient Gaps increasing from 2 (= 11 - 9) to 4 (= 27 - 23) and therefore always greater than or equal to 2. Notice that the Quotient Gap for x < Bmax jumps by 2 (Qg = 5 - 3) for x = 11 and x = 12. However, this is a spurious jump and the Quotient Gap between x = 14 and x = 15 is back to unity with quotients 8 and 9 respectively. Around Bmax, these spurious jumps tend to occur and are due to truncation in integer arithmetic. If we worked in real valued quotients the Quotient Gap would increase monotonically.

Residue Table a = 7, n = 3

x	x^n	residue (mod a^n)	residue mod a	quotient
7	343	0	0	1
8	512	169	1	1
9	729	43	1	2

10	1000	314	6	2
11	1331	302	1	3
12	1728	13	6	5
13	2197	139	6	6
14	2744	0	0	8
15	3375	288	1	9
16	4096	323	1	11
17	4913	111	6	14
18	5832	1	1	17
19	6859	342	6	19
20	8000	111	6	23
21	9261	0	0	27

Given that INT(Bmax) = 15 for n = 3 and a = 7 and, coupled with the knowledge that b must be composite by Theorem (1.15) and also have one or more factors of the form 2ln+1, see section(2.2.5), this does not leave much room for a possible value of b. The smallest value of 2ln+1 is 7 (hence a = 7), and since b cannot equal a, which is prime anyhow, the next smallest composite it can be is 14. But this is a multiple of the base a and so has a zero residue. We cannot go any higher than INT(Bmax) = 15 so we conclude that there is no Candidate Pair for n = 3, a = 7 and, consequently, no FLT counter-example. Of course, this just rules out a = 7, it doesn't dismiss the entire n = 3, cubic exponent case.

1.19.4 Theorem: Bmax < a^n / 2

The value Bmax is always less than a^n / 2 for n >= 3, a >= 2.

Proof

Assume this is true then

1.19.4.1 Bmax < a^n / 2

Raising to the (n - 1)'th power and multiplying by n, so as to make the lhs identical to (1.19.1.5), we get

1.19.4.2 n*Bmax^(n - 1) < n*(a^n / 2)^(n - 1)

And substituting for n*Bmax^(n - 1) from (1.19.1.5) implies

1.19.4.3 2*a^n < n*(a^n / 2)^(n - 1)

Dividing throughout by a^n we obtain the inequality

1.19.4.4 2 < n*(a / 2)^(n - 2)

For n = 2, we see that this leads to a contradiction 2 < 2, so it doesn't hold for n = 2. In fact Bmax = a^2 for n = 2, see (1.19.2.3).

For n = 3, we see that 2 < 3*a / 2 which is true for a >= 2. Since a = 2 is the minimum value of the base a throughout this paper, Bmax is always less than a^3 / 2 for n = 3. [Note that by the '2ln+1' constraint put on the base a, see (2.2.5), a = 7 is actually the minimum practical value of a].

In general, for any exponent, n >= 3, the following inequality is always satisified for all a > 0

1.19.4.5 $(a / 2)^{(n - 2)} >= a / 2$

Multiplying throughout by n we get

1.19.4.6 $n*(a / 2)^{(n - 2)} >= 3*a / 2$

and if we impose the constraint on a that

1.19.4.7 $a >= 2$

which is satisified by convention (0.3.3.1) then the rhs of (1.19.4.6) is such that

1.19.4.8 $3*a / 2 >= 2$

and so combining (1.19.4.5) and (1.19.4.8) we get the inequality

1.19.4.9 $n * (a / 2)^{(n - 2)} > 2$

which shows that for all n >= 3 and a >= 2, inequality (1.19.4.4) is met and so Bmax < a^2 / 2

Almost needless to say, this a^n / 2 value is a poor upper bound for Bmax. It could be made much tighter. However, it is not required herein.

1.19.5 Theorem: Bmax > a for n >= 2

The value Bmax is always greater than a for n >= 2 and a of the form 2ln+1.

Proof

Rearranging (1.19.1.5)

1.19.5.1 Bmax^(n - 1) = 2*a^(n - 1)*a / n

Taking the (n - 1)'th root of both sides [the symbols '(n - 1)_/' denote the (n - 1)'th root] we get

1.19.5.2 Bmax = a*((n - 1)_/(2a / n))

Therefore, by (1.19.5.2), if the (n - 1)'th root of (2a / n) is greater than unity, then Bmax will be greater than the base a. If a is of the following form

1.19.5.3 a = 2ln + 1

then this is easily seen since

1.19.5.4 2a / n = 4l + (2 / n)

and for all n > 2, if l >= 1, then

1.19.5.5 4l + (2 / n) > 1

so that for all n > 2, if l >= 1, (1.19.5.2) becomes

1.19.5.6 Bmax > a

Combining this result with Theorem (1.19.4), we get a range for Bmax, a = 2ln+1, n > 2, l >= 1 as

1.19.5.7 a < Bmax < a^n / 2

1.20 C'max

Just as there is an upper limit 'Bmax', section (1.19), on the value b in a Candidate Pair (b,c) (mod a^n), so too is there an upper limit on the value c in the Dual Candidate Pair (a,c) (mod b^n).

1.20.1 Theorem: C'max

Given a Dual Candidate Pair (a,c) (mod b^n), there exists a value C'max, such that for c > C'max, the Quotient Condition can never be met.

The proof is actually much simpler than that for the Standard case of Bmax as given in Theorem (1.19.1).

Proof

In the dual case it is not the Quotient Gap that has to be unity but simply the absolute quotient value q' (1.18.7) which has to be unity. This is because the smaller quotient p' (1.18.3) is always zero. Thus to achieve a Dual Quotient Gap of unity we simply set a limit on q' as

1.20.2 $q' < 2$

Inserting this limit into (1.18.5) we get the inequality

1.20.3 $c^n < 2*b^n + a^n$

Now since a < b and n >= 2, by convention, then

1.20.4 $a^n < b^n$

and so inequality (1.20.2) is equivalent to

1.20.5 $c^n < 3*b^n$

Defining C'max as

1.20.6 $C'max^n = 3*b^n$

then inequality (1.20.5) becomes

1.20.7 $c^n < C'max^n$

So that for all c < C'max we have an absolute quotient q' such that q' < 2 and the Dual Quotient Condition is satisfied.

1.20.8 Notes

By (1.34.4) we see that C'max is always less than the n'th root of 3 multiplied by b. As a rule of thumb, without accurately computing the value of C'max, a good limit, for the two smallest, odd, prime exponents, n = 3 and n = 5 is

1.20.9 n = 3, C'max < (3 / 2)*b

1.20.10 n = 5, C'max < (5 / 4)*b

[Note that although it appears C'max < (n / (n - 1))*b, this is not so for prime n >= 7. Neither is a more lenient C'max < ((n+1) / n)*b]. For large n they are reasonable approximations BUT for an upper bound such that C'max is always below, use C'max < (5 / 4)*b, i.e. the n = 5 result].

This means that in the cubic exponent case (1.20.9), when examining a Dual Residue table for Repeat Residues (a,c), we need never look any further than b < c < 3b / 2. Contrast this with a Standard Residue Table (mod a^n) where we have to search for Repeat Residues up to Bmax which, by (1.19.5.2), can be many times larger than the base a, when a is itself large. However, as good as this may seem, it is actually illusory in that the absolute value of c is the same in both dual and Standard cases. This is because the derivation of Bmax, Theorem (1.19.1), also puts a restriction on the value of c in the Candidate Pair (b,c) (mod a^n), see (1.19.2.2). This c value is the same 'c' as in the Dual Candidate Pair (a,c) (mod b^n). Hence the value of c is subject to both the C'max restriction (1.20.6) and the Bmax restriction (1.19.1.5). If b is its largest possible value, b = INT(Bmax), then c can only be equal to INT(Bmax) + 1 if the triple (a,b,c) is to be an FLT counter-example.

1.21 Summary of Conditions

A summary of all the conditions and constraints, developed so far, on a triplet (a, b, c) were it to be a an FLT counter-example.

1.21.1 The Standard Residue Condition (1.2.3), Candidate Pair (b,c)

b^n = c^n (mod a^n)

1.21.2 The Standard Quotient Condition (1.4.3)

If (b^n = p*a^n + r) and (c^n = q*a^n + r) then q - p = 1

1.21.3 The Dual Residue Condition (1.17.1), Candidate Pair (a,c)

a^n = c^n (mod b^n)

1.21.4 The Dual Quotient Condition (1.18.7)

If (c^n = q'*b^n + a^n) then q' = 1

1.21.5 The Root Gap Constraint, Theorem (1.12)

c - b < a

1.21.6 The Root Gap (1.10.1) is unity if the base is prime, Theorem (1.14)

c - b = 1

1.21.7 The Standard Root Gap (1.10.1) divides the Standard Base

Although not explicitly prior stated, from the factorisation of the FLT equation (1.14.2) we can deduce that the Standard Root Gap (c - b) divides the Standard Base a, i.e.

(c – b) | a

1.21.8 The Dual Root Gap (1.15.1) divides the Dual base b

As for (1.21.7), we can similarly deduce, by factorisation of the term c^n - a^n (= b^n), that the Dual Root Gap (c - a) divides the Dual Base b, i.e.

(c – a) | b

1.21.9 The Dual base b is always composite, Theorem (1.15)

1.21.10 The Dual Root Gap Rg' (1.15.1) is always greater than unity

By convention (0.3.3), a < b < c, so that

(c – a) >= 2

1.21.11 There is a value Bmax such that, for all b >= Bmax, the Quotient Gap Qg of a Standard Candidate Pair (b,c) mod a^n is always greater than unity, Theorem (1.19.1)

For all b >= Bmax, Qg > 1

1.21.12 There is a value C'max such that, for all c >= C'max, the Dual Quotient Gap Qg' of a Dual Candidate Pair (a,c) mod b^n is always greater than unity, Theorem (1.20.1)

For all c >= Cmax, Qg' > 1

2 Mechanisms for Repeat Residues

The first section of this paper started with the FLT equation (1.1.1) placing two conditions, the Residue and Quotient Condition, upon any possible solution triple (a, b, c) for exponents n >= 2. These conditions were proven to be met with respect to Pythagorean triples (1.6) and we expanded upon the conditions to impose some tighter constraints upon any potential FLT counter-example.

We showed that key to meeting the Residue Condition were Candidate Pairs (b,c) and (a,c) where c^n = b^n (mod a^n) and c^n = a^n (mod b^n) respectively. Theorem (1.12) constrained these Candidate Pairs and lead us to the study of Residue Sequences, i.e. the residues x^n (mod a^n), 0 <= x < a^n, which is where we start the work in this section. We are particularly concerned with how residues repeat within a narrow range of the base, a in the Standard case, b in the Dual case, and therefore generate Candidate Pairs which may also meet, or come close to meeting, the Quotient Condition.

We will see that even-exponent Residue Sequences possess the necessary symmetry such that integers b and c of a Candidate Pair (b,c) are almost back-to-back, i.e. consecutive. Using this symmetry for Pythagoras we proceed to derive the analytic solution for Pythagorean triples. We also then look at the quartic case (n = 4) which also possesses even exponent symmetry but, of course, no FLT counter-examples.

Since Residue Sequences for odd exponent lack the symmetry of even exponents, we can then no longer rely upon such symmetry to guarantee us an abundance of Candidate Pairs which have any chance of meeting the Root Gap Constraint, Theorem (1.12), and, consequently, the Quotient Condition. We shall see that odd exponent Residue Sequences do have a general Skew-symmetry but it is shown this cannot produce FLT counter-examples. Instead, we investigate another known ‘2ln+1’ mechanism whereby residues can repeat, Candidate Pairs can form, and some may even satisfy the Root Gap constraint. All these investigations yield yet more constraints which are summarised at the end of the section.

Finally, whilst even and odd exponents are treated separately, it is mentioned, in advance, that the two can be unified under a single scheme we term ‘Unity Root Mappings'. The subject of Unity Roots and their Mappings is discussed fully in section (3).

2.1 Introduction

Before starting, please keep in mind that whilst much of the work throughout this paper uses the Standard base a, it could equally be the Dual base b or, as we shall see later, the Skew base c.

The simplest form of repetition of residues, equation (1.8.6.1) repeated below, was introduced to obtain quick solutions to the General FLT Equation (1.8).

2.1.1 (a^n + x)^n = x^n (mod a^n)

This shows that a residue x always repeats at (a^n + x) (mod a^n) for all a and n. Theorem (1.12) shows that such repetitions, where the Root Gap is greater than the base, can never satisfy the Quotient Condition (1.4.3).

Since there do exist solutions to the Pythagoras Equation there must be Repeat Residues, at least for n = 2 with a Root Gap less than the base, and so mechanism (2.1.1) cannot be that responsible for generating Pythagorean triples.

We consider alternative mechanisms which can produce repetition of residues within the [0, a^n) interval and, in some cases, within an interval less than the base for all n, and for some specific forms of the base, thereby meeting the Root Gap Constraint (1.12).

2.1.2 Definitions

Before continuing, the following definitions are used throughout this paper.

2.1.2.1 Residue Sequence

A Residue Sequence, as defined herein, is a sequence of residues r_i, index i, modulus a^n, given by

2.1.2.1.1 r_i = i^n (mod a^n)

for integer i in the range

2.1.2.1.2 0 <= i < a^n if n !| a

or

2.1.2.1.3 0 <= i < a^(n - 1) if n | a

The term ‘Sequence’ is used in preference to ‘Set’ because its members may not not all be unique and the ordering is important.

2.1.2.2 Minimal Residue Sequence

A Residue Sequence is termed a ‘Minimal Residue Sequence’ if the exponent divides the base as given by (2.1.2.1.3).

Such a Residue Sequence is prefixed 'Minimal' because it is the smallest sequence of residues that repeats in its entirety, and in the same order, n times within the interval [0, a^n).

Thus, for any value x, the equivalent of (2.1.1) is

2.1.2.2.1 (a^(n - 1) + x)^n = x^n (mod a^n)

Because the exponent divides the base, unless the base is identically equally to the exponent, i.e. a = n, then the base is composite.

Because this natural repetition of all residues in a sequence is at a Root Gap a^(n - 1), rather than a^n, the Quotient Gap of a Candidate Pair (b,c), where b = x, c = a^(n - 1) + x, will be smaller than if the Root Gap were a^n, as in (2.1.1). Nevertheless, this is still not adequate to meet the Root Gap Constraint. Note that a Root Gap of a^(n - 1) would give Rg = a, if the exponent n were to equal to 2, for n >= 3 this gives Rg >= a^2.

2.1.2.2.2 Example

The simplest, non trivial FLT case is the cubic exponent with base a = 3, modulus 3^3. Here the exponent is equal to the base and so the size of the Minimal Residue Sequence is 3^3 / 3 = 3^2, i.e. 9. So the Minimal Residue Sequence comprises residues r_i, 0 <=i < 9.

2.1.2.3 Maximal Residue Sequence

A Residue Sequence is termed a ‘Maximal Residue Sequence’ if the exponent n does not divide the base, as given by (2.1.2.1.2).

If the base a is prime then all non zero residues are unique and a Maximal Residue Sequence is of size a^n. It is termed Maximal since, by (2.1.1), it is the largest possible Residue Sequence, (mod a^n), that doesn’t repeat in its entirety.

2.2 Overview of Repeat Residue Mechanisms

2.2.1 Introduction

There are four possible mechanisms such that a residue r for a value b, as given by

2.2.1.1 b^n = r (mod a^n)

can repeat at a point c, within an interval [0, a^n), whereby

2.2.1.2 c^n = r (mod a^n)

When we talk of 'Repeat residues', the zero residue, r = 0, is ignored. Any integer multiple k of the base a is such that (ka)^n = 0 (mod a^n) as can be seen in the examples in section 13. We could, for example, pick a Candidate Pair (b,c) whereby b = ka, c = (k + s)a, integral s, s > 0, which would have the common residue 0. However since the modulus is a^n, the common factor of a would cancel, i.e. the triple (a, b, c) would be co-prime in pairs which is discounted by convention (0.3.4).

2.2.2 The exponent n divides the base

When the exponent divides the base, i.e.

2.2.2.1 n | a

then the Residue Sequence obtained is a Minimal Residue Sequence (2.1.2.2), and residues naturally repeat at a reduced interval of a^(n - 1), rather than a^n, such that for a value x,

2.2.2.2 (a^(n - 1) + x)^n = x^n (mod a^n)

Because this natural repetition of all residues in a sequence is at a Root Gap a^(n - 1), the Quotient Gap of a Candidate Pair (b,c), where b = x and c = a^(n - 1) + x in (2.2.2.2), will be smaller than if the Root Gap were a^n, as in (2.1.1). Nevertheless, this is still not adequate to meet the Root Gap Constraint, Theorem (1.12). Note that a Root Gap of a^(n - 1) would give Rg = a if the exponent n were to be equal to 2. For n >= 3 this gives Rg >= a^2.

By the arguments in the above paragraph, this mechanism for Repeat Residues is insuffcient, by itself, to produce FLT counter examples. However, if the base a (or b in the Dual case) were to be composite, such that not only does n | a but a has a factor of the 2ln+1 form (section (2.2.5)), then the base could yield possible Candidate Pairs.

With the form of the base a expressed by (2.2.5.10), we see that the factor ‘x’ would have to be such that n | x. For FLT, the smallest case under consideration is the cubic exponent and the smallest value of (2ln+1) would therfore be 7 (where l = 1, n = 3). So the smallest possible composite value for a, with a Minimal Residue Sequence, would be a = 21.

2.2.3 The base is composite

Because of reasons expressed at the end of Theorem (1.14), a composite base has to be a consideration. Nevertheless we shall show that, whilst it can give Repeat Residues within a Maximal Residue Sequence, these occur for the factors of the base and do not therefore satisfy co-primality in pairs, convention (0.3.4).

We shall assume none of the factors is of the '2ln+1' form. If they are the arguments still apply but we also have to consider the '2ln+1' mechanism for Repeat Residues given in (2.2.5) which concludes that such composite bases can not then be eliminated.

Stated without proof.

Let us define the base a as comprising two factors k and m, i.e.

2.2.3.1 a = k*m

where each factor can either be prime or composite and neither is of the 2ln+1 form. Furthermore we will assume the exponent n does not divide the base a, i.e.

2.2.3.2 n !| a

Then, if b is a multiple s, integer s, s>0, of the factor k, i.e.

2.2.3.3 b = s*k

and c is defined as follows for integer t, t>0,

2.2.3.4 c = s*k + t*k*m^n

we assert that c is a Repeat Residue of b and (b,c) is a Candidate Pair, i.e.

2.2.3.5 c^n = b^n (mod a^n)

Of course, we can interchange factors k and m to get a similar result for multiples of the factor m.

This assertion is not too difficult to see since, if we re-write c as follows with the factor k,

2.2.3.6 c = k*(s + t*m^n)

and raise c to the power n, binomially expanding the rhs bracket and take residues of the rhs (mod a^n) (= mod k^n*m^n) we would get

2.2.3.7 c^n = k^n*s^n mod (km)^n

i.e.

2.2.3.8 $c^n = (k*s)^n = b^n \bmod (km)^n = b^n \pmod{a^n}$

The smallest interval of repetition (of the Residue), i.e. the Root Gap (c - b) is now, for t = 1 in (2.2.3.4),

2.2.3.9 $Rg = k*m^n$

We can see this Root Gap is considerably less than the maximum a^n, hence we get Repeat Residues within the Maximal Residue Sequence. Before discussing further, we have to look at the case where the exponent divides the base, in which case we can reduce the Root Gap even further.

Using the same equations as above, except now the exponent n divides the base a by dividing the factor m, i.e.

2.2.3.10 $n \mid m$

and with c now defined as

2.2.3.11 $c = s*k + t*k*(m^n) / n$

then

2.2.3.12 $c^n = b^n \pmod{a^n}$

i.e. c is a Repeat Residue of b and (b,c) is a Candidate Pair

We see that, if the exponent divides the factor m, then the smallest interval of repetition of the Residue, i.e. the Root Gap, is now, for t = 1 in (2.2.3.11), given by

2.2.3.13 $Rg = k*m^{(n - 1)}$

We can see this Root Gap is considerably less than the maximum a^n. Nevertheless, before this seems like a good mechanism to try and get a small Root Gap and with it, a consequently small Quotient Gap, we should note that we have already exceeded our constraint of 'co-primality in pairs' (0.3.4) since GCD(b, c) = s. Therefore this repetition of residues will not give us true primitive FLT counter-examples.

If this wasn't enough to eliminate this case, we can see from (2.2.3.13), that even the reduced Root Gap (2.2.3.13) cannot be less than or equal to the base a (a = k*m) unless the exponent n = 2. Even then the Root Gap is only equal to a and not less than a, so the Root Gap Constraint, Theorem (1.12), cannot be met.

The conclusion is that, whilst we still consider composites, we are only interested in b and c values such that GCD(b, a) = GCD(c, a) = 1.

2.2.4 The exponent is even

Since an even exponent, barring the Pythagorean case, is always composite, we would generally dismiss even exponents for FLT, convention (0.3.2). However, the quartic case (n = 4) is considered primarily since the symmetry arguments we use in the Pythagorean case equally apply to any even exponent. Of course, the quartic case was proven by Fermat himself, actually prior to the cubic proof, Euler, 1753.

An even power exponent guarantees, by the symmetry of the Residue Sequence it produces, that a residue will repeat at least once within the [0, a^n] interval. Furthermore, and key to Pythagoras, this repetition can occur for back-to-back values (actually roots, see (1.10.2) and Consecutive Residues (1.11)) i.e. those values around the symmetry point. These residues have a Root Gap of unity giving them a good chance of having a unity Quotient Gap. For odd, prime base a there is one such symmetry point at (a^2 - 1) / 2 and so there is always at least one Candidate Pair. For even base there are additional symmetry points at a^2 / 4 and 3*a^2 / 4 and subsequently more Candidate Pairs – something not guaranteed for odd exponent.

Concluding, an even exponent is a very import criteria for repetition of residues and its symmetry aspects and consequences are fully detailed in section (2.4).

2.2.5 The base is of the 2ln+1 form

Because an odd exponent does not give a symmetric Residue Sequence as obtained with an even exponent, Repeat Residues do not come guaranteed for odd exponents. It would be nice if that were the end of the story since we could then conclude, using Theorem (1.12), that FLT was true. Of course this is not so. For certain base a, modulus a^n, Repeat Residues do occur within the interval [0, a^n) and, indeed, within an interval of much smaller size, i.e. within the base a. This is because there can be multiple, unique roots to the following congruential equation

2.2.5.1 $x^n = r \pmod{a^n}$

The key point is that if there is a root x = b and another root x = c then they share the same residue and hence (b,c) form a Candidate Pair (this has been prior mentioned in section (1.10)). Note that not all bases have multiple roots. For most bases we only get a single root and consequently no chance of a Candidate Pair either. However, for some bases, which we will now discuss further, multiple roots means Candidate Pairs.

Equation (2.2.5.1) is a special form of the general polynomial congruence, (mod P)

2.2.5.2 r_n*x^n + r_n_1*x^(n - 1) + … r_1*x + r_0 = 0 (mod P)

An inportant theorem on integer solutions to this polynomial congruence is that due to Lagrange.

2.2.5.3 **Lagranges Theorem on Congruences**

Lagrange's Theorem of Congruences states that:

a polynmial congruence (2.2.5.2), degree n, (mod P), where n and P are prime, cannot have more than n solutions and, if the modulus P is of the form

2.2.5.3.1 P = k*n + 1

then there are exactly n solutions.

In the case of our Unity Root equation (2.2.5.1) there is always one root for odd, prime exponent which is the trivial root +1. For the only prime, even exponent, n = 2, there are always two roots for prime modulus and these are +1 and –1.

If we consider odd exponent, n>=3, then, for integer m, m >0, n is of the form

2.2.5.4 n = 2m + 1

so that the base modulus P (2.2.5.3.1) is of the form

2.2.5.5 P = 2k*m + k + 1

If k is odd this would make P even but, since P is prime, then k must be even and hence, for some integer l, l > 0, k is of the form

2.2.5.6 k = 2l

Substituting for k in (2.2.5.3.1) we arrive at the form for the modulus P as

2.2.5.7 P = 2ln + 1

Hence, if we are to get multiple roots and therefore Candidate Pairs, for odd, prime exponent n, n >= 3, prime modulus P, we require P to be of the '2ln+1' form given by (2.2.5.7). A more intuitive approach to the derivation of this form is given in Section (2.5.7).

That said, in this paper we are interested in modulus a^n (or modulus b^n, c^n in the Dual and Skew cases) where the base a, b or c may also be composite. Indeed, by Theorem (1.15), the Dual base b is always composite. Fortunately, the extension to composite base can be constructed from the work on prime base and some further discussion is given in section (2.5.14). However, we state here, without proof, that for odd, prime exponent Repeat Residues will occur within the (0, a^n] interval if the base is prime of the '2ln+1' form or composite with one or more prime factors of the '2ln+1' form. Furthermore, unlike any of the other Repeat Residue mechanisms for odd exponent, (see (2.2.2) and (2.2.3)), this mechanism is the only one with the potential to generate Repeat Residues with a Root Gap of less than the base, see Theorem (1.12), i.e. it is the only mechanism that can generate possible FLT counter-examples.

We finish this section by introducing two new constraints on the form of the Standard base a and Dual base b as concluded from the discussions.

For integers x and k

2.2.5.8 $x >= 1$

2.2.5.9 $k >= 1$

The value a is either prime ($x = 1$) or composite ($x > 1$) with one or more factors of the form ($2kn + 1$), i.e.

2.2.5.10 $a = x*(2kn + 1)$

For integers y and l satisfying the following inequalities,

2.2.5.11 $y >= 2$

2.2.5.12 $l >= 1$

then, by Dual considerations, we can also constrain b such that it is always composite ($y > 1$, see also Theorem 1.15) with one or more prime factors of the form 2ln+1, i.e. b is of the form

2.2.5.13 $b = y*(2ln + 1)$

2.3 Key Mechanisms

Summarising section (2.2), there are only two cases which give rise to Repeat Residues such that the Root Gap is less than the base, these are

2.3.1 The exponent n is even, arbitrary base

2.3.2 The exponent n is odd and the base is either prime of the form 2ln+1 or composite with one or more prime factors of the form 2ln+1. This applies to both the Standard and Dual base, a and b respectively.

2.4 Even Exponent

2.4.1 Introduction

Even power exponents n = 2m, where m is integral, m > 0, produce a symmetric sequence of residues since for any x and m we have

2.4.1.1 x^(2m) = (a^(2m) - x)^(2m) mod a^(2m)

and so the residue at x is identical to that at a^(2m) - x, i.e. there is a symmetry about the mid-point a^(2m) / 2.

In particular, for the Pythagorean case, where m = 1, (2.4.1.1) becomes

2.4.1.2 x^2 = (a^2 - x)^2 (mod a^2)

For odd a, the Residue Sequence is Maximal (2.1.2.3), i.e. length a^2, and has a half integral mid-point at

2.4.1.3 x = a^2 / 2

Two integers b and c, either side +/-y / 2 (integer y, y > 0) of the midpoint a^2 / 2, and given by

2.4.1.4 b = (a^2 - y) / 2

and

2.4.1.5 c = (a^2 + y) / 2

form a Candidate Pair (b,c) since

2.4.1.6 c^2 = b^2 (mod a^2)

Because the Residue Sequence is symmetric, all points +/-y / 2 about the mid-point also have the same residue. This gives rise to many such Candidate Pairs with a Root Gap, Rg = y, and therefore, by Theorem (1.12), to have any chance of satisfying the Quotient Condition we must have y < a.

2.4.2 Examples, n = 2, odd base a

2.4.2.1 a = 3, n = 2

See the Residue table in section (7.1.1).

The Residue Sequence mid-point is (3^2) / 2 = 4.5, the integers either side are b = 4 and c = 5 and their squares are congruent (mod 3^2), i.e. 4^2 = 5^2 (mod 3^2).

Furthermore, the Residue table shows that 4^2 = 1*3^2 + 7 and 5^2 = 2*3^2 + 7 and hence the quotients, p and q, equations (1.3.1) and (1.3.2), are 1 and 2 respectively, giving a Quotient Gap of 1. Therefore, the Candidate Pair (4, 5) satisfies the Quotient Condition and the triple (3,4,5) is a Pythagorean triple.

Since a is prime we see the Root Gap, Rg = 5 - 4, is unity, confirming Theorem (1.14)

2.4.2.2 a = 5, n = 2

See the Residue table in section (7.1.3).

The Residue Sequence mid-point is (5^2) / 2 = 12.5, the integers either side are b = 12 and c = 13 and their squares are congruent (mod 5^2), i.e. 12^2 = 13^2 (mod 5^2).

Furthermore, the Residue table shows that 12^2 = 5*5^2 + 19 and 12^2 = 6*5^2 + 19, and hence the quotients, p and q, equations (1.3.1) and (1.3.2), are 5 and 6 respectively, giving a Quotient Gap 1. Therefore the Candidate Pair (12,13) also satisfies the Quotient Condition and the triple (5,12,13) is a Pythagorean triple.

Since a is prime (a = 5) we see the Root Gap, Rg = 13 - 12, is unity confirming Theorem (1.14).

For even a the Residue Sequence is Minimal, i.e. length a^2 / 2. This is because the exponent, n = 2, divides the base. The entire Minimal Residue Sequence is also symmetric about its mid-point which is thus at a^2 / 4. It should also be noted that the Maximal Residue Sequence, of length a^2, is always itself symmetric about its mid-

point a^2 / 2. If we concentrate on the Maximal Sequence first, for even n, the mid-point is integral and the two central values, either side of this mid-point, denoted by b and c, are b = (a^2 - 1) / 2 and c = (a^2 + 1) / 2.

2.4.3 Examples, n = 2, even base a

2.4.3.1 a = 4, n = 2

See the Residue table in section (7.1.2).

The Maximal Residue Sequence mid-point is (4^2)/ 2 = 8, the integers either side are b = 7 and c = 9 and their squares are congruent (mod 4^2), i.e. 7^2 = 9^2 (mod 4^2). The Residue table shows that 7^2 = 3*4^2 +1 and 9^2 = 5*4^2 +1 and hence the quotients, p and q, equations (1.3.1) and (1.3.2), are 3 and 5 respectively, giving a Quotient Gap of 2. Since the Root Gap is not unity, the Candidate Pair (7,9) does not satisfy the Quotient Condition and therefore the triple (4,7,9) is not a Pythagorean triple.

In this same example the Minimal Residue Sequence mid-point is (4^2) / 4 = 4 and the integers either side are b = 3 and c = 5 and their squares are congruent (mod 4^2), i.e. 3^2 = 5^2 (mod 4^2). This case is, of course, the Pythagorean triple (3,4,5) that was considered in the Example (0). In that case, however, the base (a = 3) was odd. In this case, we are considering the even base (a = 4) and so we are actually looking at the Pythagorean triple (3,4,5) in a Dual aspect, whereby the Residue Table base is the middle value of the triplet (= 4) rather than the more usual Standard case whereby the base is the lowest member of the triple (= 3).

Looking at the Dual Residue table, (mod 4^2), we see the quotient p' for b = 3 is 0, i.e. 3^2 = 0*4^2 + 3^2, as expected by equation (1.18.3). Similarly, since 5^2 = 1*4^2 + 3^2, the quotient q' is 1. Therefore the Quotient Gap in this Dual case is still unity since q' - p' = 1, q' = 1, p'= 0 and, as expected, the triplet (3,4,5) is a Pythagorean triple.

This latter, even base example confirms all the Standard and Dual conditions summarised in section (1.21).

2.4.4 Pythagorean Triples - An Analytic Solution via Symmetry

Using the Symmetry present in the Residue Tables, (mod a^2), we can derive the analytic equation from which to generate all Pythagorean Triples.

For even base a, modulus a^2, we have a symmetry point a^2 / 4 which is an exact integer. Either side of this mid-point +/- y, y integral, y > 0, we have identical residues and, consequently, Candidate Pairs (b,c) where b and c are

2.4.4.1 b = a^2 / 4 – y

2.4.4.2 c = a^2 / 4 + y

It can be verified that b^2 is congruent to c^2 (mod a^2), i.e. (b,c) are indeed a Candidate Pair, since

2.4.4.3 b^2 = a^2 / 4 - 2(a^2 / 4)y + y^2

2.4.4.4 c^2 = a^2 / 4 + 2(a^2 / 4)y + y^2

Defining r' as

2.4.4.5 r' = (a^2 / 4 + y^2) (mod a^2)

and taking the residues of (2.4.4.3) and (2.4.4.4) (mod a^2), we get

2.4.4.6 b^2 = r’ - (a^2 / 2)y (mod a^2)

2.4.4.7 c^2 = r’ + (a^2 / 2)y (mod a^2)

and since, for any integer y,

2.4.4.8 (a^2 / 2)y = - (a^2 / 2)y (mod a^2)

then we see that (2.4.4.6) and (2.4.4.7) are identical, i.e.

2.4.4.9 b^2 = c^2 (mod a^2)

Therefore, for all integer values of y, the values b and c, as defined by (2.4.4.1) and (2.4.4.2) respectively, form a Candidate Pair (b,c).

Subtracting (2.4.4.6) from (2.4.4.7) gives

2.4.4.10 c^2 - b^2 = y * a^2

We see that the Quotient Gap is given by y and will not meet the Quotient Condition except when y = 1. Therefore, although (b,c) is a Candidate Pair (mod a^2), it would seem that it is only a genuine solution, i.e. a Pythagorean triple, if y = 1. However, by defining y as a perfect square

2.4.4.11 $y = k^2$

and then transforming a to composite a' defined by

2.4.4.12 $a' = ka$

Then (2.4.4.10) becomes

2.4.4.13 $c^2 - b^2 = a'^2$

and we see that (2.4.4.13) has a unity Quotient Gap (mod a'^2) and (a',b,c) is a Pythagorean Triple.

The values of b and c, as given in(2.4.4.1) and (2.4.4.2), now become, using (2.4.4.11) for y but keeping with a and not a',

2.4.4.14 $b = a^2 / 4 - k^2$

2.4.4.15 $c = a^2 / 4 + k^2$

Lastly, the Pythagorean Triple (a',b,c) was generated assuming an even base a. Re-defining a in terms of integer l, $l > 0$, where l is odd or even

2.4.4.16 $a = 2l$

Substituting for a from (2.4.4.16) into (2.4.4.12), (2.4.4.14) and (2.4.4.15) then a', b and c become

2.4.4.17 $a' = 2kl$

2.4.4.18 $b = l^2 - k^2$

2.4.4.19 $c = l^2 + k^2$

And so we finally obtain the standard analytic solution to the Pythagoras Equation given by equations (2.4.4.17), (2.4.4.18) and (2.4.4.19), where k and l are integers, $l > k > 0$, with no odd or even restrictions.

Remarks

a' is no longer necessarily the smallest member of the triple (a',b,c). This is a labelling issue, we could choose to interchange a', b and c so that c > b > a' and then rename a' = a. For example, with l = 3, k = 12, equations (2.4.4.17) to (2.4.4.19) give a' = 12, b = 5 and c = 13. We see a' is composite and now greater than b. We could arbitrarily re-assign a = 5, b = 12 and c = 13.

That the association of y to a perfect square, k^2, was made in (2.4.4.11) shows that not every pair, equidistant by y about the symmetry point (a^2 / 4), can be a Pythagorean triple. Indeed, only when y is a perfect square is this so. Thus, Candidate Pairs appear +/-1, +/-4, +/-9, ... +/-k^2, about the symmetry point and the Pythagorean triples are (ka, b, c). Following from this, the Quotient Gap (mod a^2) is only unity if k is unity and this gives us only one solution about the symmetry point a^2 / 4. Of course, there are many solutions for composite a' = ka, k >1.

For example, if a = 8, the symmetry point is 8^2 / 4 = 16. The two values either side, k = +/-1, are b = 15, c = 17 and, indeed, (8, 15, 17) is a Pythagorean Triple (mod 8^2). On the other hand, if we let k = +/- 2^2, then the two values, b and c, either side of the symmetry point are 12 and 20. Studying the Residue Table (Section 7.1.x TBD), we see that the residues are identical since 12^2 = 20^2 = 16 (mod 8^2), as would be expected for a Candidate Pair (12, 20), but that the quotients are 2 and 6 respectively, giving a Quotient Gap of k^2 = 4, also as expected. Thus, the Candidate Pair (12, 20) is not part of a Pythagorean Triple (mod 8^2) but it is (mod a'^2) where a' is the composite k*a = 2*8 = 16.

Studying the residue table (mod 16^2) (not supplied in this paper), we observe that the pair (12, 20) have identical residues mod 16^2 (12^2 = 16^2 = 144 mod 16^2) and that the Quotient Gap is unity so that we have the non-primitive Pythagorean triple (12, 16, 20). It is termed non-primitive because each element has a common factor of 4, i.e. it does not satisfy co-primality in pairs. However, dividing a, b and c by this factor gives the primitive triple (3, 4, 5) where a, b and c are now co-prime in pairs.

We know equations (2.4.4.17) to (2.4.4.19) will give us all Pythagorean Triples, see for instance ref. [6], subject ‘Diophantine Equations’. However, the derivation above started by assuming an even base when we could have used an odd base instead. The derivation using an odd base is done in the section (2.4.6). However, on the even-base derivation alone, and without recourse to other proofs, could we have been guaranteed sufficiency that these three equations will give us all Pythagorean Triples including the odd ones? The answer is yes because the derivation was made for all even numbers, not just a subset. Suppose (x,y,z) is a Pythagorean triple where x or y is odd, then there is a corresponding, improper solution (2x,2y,2z) with a common factor of 2. Whilst it is a non-primitive solution, it remains valid and both 2x and 2y are now even. This solution will always appear for some choice of l and k since the equations are valid for all even numbers - either l or k are both odd or both even. Therefore, for certain non-primitive even solutions, we can divide throughout by two and obtain all the odd solutions.

Because every residue table (mod a^2), where a is odd or even, has at least one Pythagorean Triple and since the set of even numbers is infinite then so too is the set of Pythagorean triples. This conclusion is reached without any analytic solution.

2.4.5 More on Symmetry

For odd a there is only the symmetry point at the half integer value a^2 / 2. For even a there are actually three symmetry points, one at the mid-point a^2 / 2, another at a^2 / 4 and the third at 3*a^2 / 4. This latter point at 3*a^2 / 4 is the mirror image point of the symmetry point at a^2 / 4.

The symmetry point a^2 / 2 for odd a is half-integral. If it were divided again, it would give a quarter fraction. In such a case the smallest integer not larger than it would be 1 / 4 below the mid-point, and the smallest integer not less than the mid-point would be 3 / 4 above from the mid-point. These two points would not technically be symmetric about a^2 / 4 for odd a. Consequently, we do not see the symmetry point a^2 / 4 in the residue tables for odd a that we see for even a.

One might think that for an even value of the base modulus such as a = 2^s, integer s, s>2, there might be an even smaller symmetry point at, say, a^2 / 2^s. In fact there are symmetry points but only for even x (x^2 (mod a^2), x> 0), consequently, they are termed 'partial symmetry points'. About these partial points one can find Candidate Pairs which manifest themselves as non-primitive solutions. These pairs do not appear to be symmetric about the usual symmetry point about which the entire Residue Sequence is symmetric. By studying another residue table to a different and smaller base, e.g. a' = a / 2^t, t > 0, the same Candidate Pair can be found at the more familiar, symmetric location, i.e. either side of a symmetry point a^2 / 4.

For example, in the a = 16 table (not supplied), there is a partial symmetry point at 16^2 / 2^4 = 16. If one looks at the points b = 16 - 4 and c = 16 + 4 one can see that they have equal residues and that their Quotient Gap is unity. This is therefore a non-primitive Pythagorean triple (12,16,20) which is actually just the infamous (3,4,5) triple. The (3,4,5) triple can be identified in the Residue table for a = 4 - the proper symmetry point being a^2 / 4 = 4 and the corresponding Candidate Pair lying either side of the standard a^2 / 4 symmetry point at b = 3, c = 5.

2.4.6 Odd Sequence Pythagorean Triples

We shall show in this section that we can also obtain the standard analytic solution for Pythagorean triples by analysis of an odd base a.

By symmetry about the mid-point, for any value x, we have

2.4.6.1 $(a^2 - x)^2 = x^2 \pmod{a^2}$

Expanding the lhs and cancelling x^2 from both sides

2.4.6.2 $a^2*a^2 - 2a^2*x = 0 \pmod{a^2}$

For some integer k this implies

2.4.6.3 $a^2*(a^2 - 2x) = k*a^2$

let $a^2 / 2 > x$ then $k > 0$. By cancelling the a^2 term in (2.4.6.3) we get for k

2.4.6.4 $a^2 - 2x = k$

For a Pythagorean triple, if we let $k = 1$ and solve for x then

2.4.6.5 $x = (a^2 - 1) / 2$

This implies a is odd for $k = 1$ so that $a^2 - 1$ on the rhs is even and x is integral. If we subtract both sides from a^2, we get

2.4.6.6 $a^2 - x = (a^2 + 1) / 2$

And, identifying b with x in (2.4.6.5) and c with a^2-x in (2.4.6.6), then we have a Pythagorean triple for odd a where

2.4.6.7 $b = (a^2 - 1) / 2$

2.4.6.8 $c = (a^2 + 1) / 2$

These two points (b,c) lie either side of the midpoint $a^2 / 2$ of the Residue Sequence $x^2 \pmod{a^2}$, $0 <= x < a$.

The smallest, non-trivial, odd value for a is 3 and substituting for a in (2.4.6.7) and (2.4.6.8) gives $b = 4$, $c = 5$, i.e. (a, b, c) is the (3,4,5) triple. The next smallest odd a is 5 which, using the same equations, gives the Pythagorean triple (5,12,13), $a = 7$ gives (7,24,25), $a = 9$ gives (9,40,41), etc.

For the more general solution, odd a, if we let $k = l^2$, instead of 1, in equation (2.4.6.4) above and solve for x

2.4.6.9 $x = (a^2 - l^2) / 2$

and subtracting both sides from a^2, we get

2.4.6.10 $a^2 - x = (a^2 + l^2) / 2$

Defining a' = la and identifying b with x in (2.4.6.9) and c with $a^2 - x$ in (2.4.6.10), then we have a Pythagorean triple (a',b,c) for odd a where

2.4.6.11 $a' = la$

2.4.6.12 $b = (a^2 - l^2) / 2$

2.4.6.13 $c = (a^2 + 1^2) / 2$

These two points (b,c) lie $+/-l^2$ about the midpoint $a^2 / 2$ of the Residue Sequence $x^2 \pmod{a^2}$, $0 <= x < a$.

In the first derivation of b and c, equations (2.4.6.7) and (2.4.6.8) respectively, the value of l, as in (2.4.6.12), was set to 1 and so the base a had to be odd to ensure $a^2 - 1$ was even, divisible by 2, and therefore give integral values for b and c. We do not have this restriction now since we can make l odd or even. If l is odd then a must be odd. Alternatively, we can have even l and even a. However, odd a, even l is not possible and neither is even a, odd l otherwise b and c are non-integral.

If we let both a and l be even then, for integers u,v > 0,

2.4.6.14 $a = 2u$

2.4.6.15 $l = 2v$

and, substituting for a and l in equations (2.4.6.11) to (2.4.6.13), we get

2.4.6.16 $a' = 4uv$

2.4.6.17 $b = 2(u^2 - v^2)$

2.4.6.18 $c = 2(u^2 + v^2)$

We now see this is gives non-primitive triple (a',b,c) because 2 is a common factor of a',b and c. Dividing throughout by 2 we finally get the familiar equations

2.4.6.19 a' = 2uv

2.4.6.20 b = (u^2 - v^2)

2.4.6.21 c = (u^2 + v^2)

which are identical in form to those obtained from the even series. We can thus get all the Pythagorean triples for both even and odd base starting either with an even base and deriving an even series or starting with an odd base and deriving an odd series, both of which can be transformed to a standard form common to both. All done by assuming symmetry about a point a^2 / 4 for even base a, and about a point a^2 / 2 for odd base a.

2.4.7 Symmetry a = 2, n = 2

The a = 2 case actually has a trivial solution (0,2,2), i.e. 2^2 = 2^2 + 0^2. One can see from the Residue Table below, that the symmetry point a^2 / 4 = 1 2^2 / 4 = 1 does exist. However, this means that the points immediately either side are b = 0 and c = 2. The zero value for b is essentially trivial and we are left with a = 2, b = 0, c = 2, which is trivially a^2 = c^2. Fortunately, this case presents no contradiction or exception to any of the conclusions or derivations.

Residue Table a = 2, n = 2

x	x^n	residue (mod a^n)	residue mod a	quotient
0	0	0	0	0
1	1	1	1	0
2	4	0	0	1
3	9	1	1	2
4	16	0	0	4

Because of its triviality, the a = 2 case is not considered and we are start with the lowest non-trivial, primitive Pythagorean triple which is (3,4,5) with a base a = 3.

2.4.8 Even Power Exponent, n = 4

Although even exponent, n >2, is of no real concern to this paper (see below for an explanation), it is worth just looking at an example, a = 4, n = 4 to see the same even exponent Symmetry in the Residue Sequence as was present in the Pythagorean case. If, for no other reason, studying n = 4 might offer an insight into why this symmetry alone cannot produce solutions for every even exponent.

The general reason not to consider even power exponents is that they are, of course, composite and therefore unnecessary for any work on FLT excepting the case of

n = 4. The n = 4 case does require a proof, which Fermat himself supplied. This is because, since there are solutions (a, b, c) to the Pythagoras equation, some of these solutions may be of the form (s^2, t^2, u^2) and would therefore also be solutions to the n = 4 case. With a =s^2, b =t^2, c =u^2 and a^2 + b^2 = c^2 this would also imply s^4 + t^4 = u^4, i.e. (s,t,u) is a triple solution to the FLT equation for the quartic exponent.

Other exponent powers of the form 2^l, integer l, l >= 3, would be a composite exponent of 2^2 and, since Fermat proved there were no solutions for the quartic case, there is no need to prove FLT for higher powers of 2 and, indeed, any even exponent n >= 4.

2.4.9 Example a = 4, n = 4

Since, in this example, the exponent n divides the base a, i.e. n | a, we know that the Residue Sequence is Minimal (2.1.2.2) with a size 4^4 / 4 = 64. Since this Minimal Sequence is also symmetric about its mid-point, by virtue that n is even, this gives us a symmetry point of 32, i.e., for integer y, y > 0, residues for b = 32 - y and c = 32 + y are identical, mirror images of each other,. A look at the Residue table for this case, shown below, confirms this.

Residue Table a = 4, n = 4

x	x^n	residue (mod a^n)	residue mod a	quotient
0	0	0	0	0
1	1	1	1	0
2	16	16	0	0
3	81	81	1	0
4	256	0	0	1
5	625	113	1	2
6	1296	16	0	5
7	2401	97	1	9
8	4096	0	0	16
9	6561	161	1	25
10	10000	16	0	39
11	14641	49	1	57
12	20736	0	0	81
13	28561	145	1	111
14	38416	16	0	150
15	50625	193	1	197
16	65536	0	0	256
17	83521	65	1	326
18	104976	16	0	410
19	130321	17	1	509
20	160000	0	0	625
21	194481	177	1	759
22	234256	16	0	915
23	279841	33	1	1093
24	331776	0	0	1296
25	390625	225	1	1525
26	456976	16	0	1785
27	531441	241	1	2075
28	614656	0	0	2401

29	707281	209	1	2762	
30	810000	16	0	3164	
31	923521	129	1	3607	
32	1048576	0	0	4096	<--- symmetry point x=32
33	1185921	129	1	4632	
34	1336336	16	0	5220	
35	1500625	209	1	5861	
36	1679616	0	0	6561	
37	1874161	241	1	7320	
38	2085136	16	0	8145	
39	2313441	225	1	9036	
40	2560000	0	0	10000	
41	2825761	33	1	11038	
42	3111696	16	0	12155	
43	3418801	177	1	13354	
44	3748096	0	0	14641	
45	4100625	17	1	16018	
46	4477456	16	0	17490	
47	4879681	65	1	19061	
48	5308416	0	0	20736	
49	5764801	193	1	22518	
50	6250000	16	0	24414	
51	6765201	145	1	26426	
52	7311616	0	0	28561	
53	7890481	49	1	30822	
54	8503056	16	0	33215	
55	9150625	161	1	35744	
56	9834496	0	0	38416	
57	10556001	97	1	41234	
58	11316496	16	0	44205	
59	12117361	113	1	47333	
60	12960000	0	0	50625	
61	13845841	81	1	54085	
62	14776336	16	0	57720	
63	15752961	1	1	61535	
64	16777216	0	0	65536	

If one looks at the Quotients it can be seen that the Quotient Gap already exceeds unity for values of x as small as x = 6, which has a quotient of 5. The x = 5 value has a quotient of 2 hence, if b = 5 and c = 6 had identical residues, which they don't, then they wouldn't meet the Quotient Condition and could not be an FLT counter-example.

Computation of Bmax, equation (1.19.1.5) with n = 4 and a = 4, gives, upon rounding down to the nearest integer, Bmax = 5. This confirms our findings in the Residue Table above and therefore, for all values x > 5, we can rule out any FLT counter-examples for triples of the form (4, b, c), c > b > 4, i.e. the a = 4, n = 4 case has no solutions. Nevertheless, since there are many Candidate Pairs, there are many GFLT solutions.

For example, about the symmetry point x = 32, the values b = 31 and c = 33 have an identical residues of 129

2.4.9.1 33^4 = 31^4 = 129 (mod 4^4)

and the quotients are 3607 and 4632 respectively since

2.4.9.2 31^4 = 3607*4^4 + 129

2.4.9.3 33^4 = 4632*4^4 + 129

subtracting 31^4 from 33^4 and re-arranging gives a GFLT solution

2.4.9.4 33^4 = 1025*4^4 + 31^4

In fact, we can get a smallest possible Quotient Gap of 5 for a = 4 since, by examining the Residue Table, we see that the residue of 16 at x = 2 repeats at x = 6, i.e. (2,6) form a Candidate Pair (mod 4^4).

2.4.9.5 6^4 = 2^4 = 16 (mod 4^4)

and the quotients are 0 and 5 respectively since

2.4.9.6 2^4 = 0*4^4 + 16

2.4.9.7 6^4 = 5*4^4 + 16

subtracting 2^4 from 6^4 and re-arranging gives a GFLT solution

2.4.9.8 6^4 = 5*4^4 + 2^4

By dividing throughout by the common factor 2^4 we get the relation

2.4.9.9 3^4 = 5*2^4 + 1

which could have been identified from the Residue Table (mod 2^4), i.e. base a = 2, and identifying (1,3) as a Candidate Pair mod 2^4.

In the above example for base a = 4, b = 2, c = 6, we noted that all three values a,b and c have a common factor 2 and are not co-prime in pairs. Algorithmically speaking, it is a waste of time to look at residue values of x that have a common factor with the base a. It is more straightforward to look at all x co-prime to a. If a is even then we need only look at odd x. We see that the residues x^4 (mod 4^4) are unique for odd x, 0 <= x <32, i.e. x below the symmetry point. Whilst it might be thought that this is always the case for x co-prime to the base, this is not always true for the case where the base is odd and of the ln+1 form (section (2.5.8)). For example, if n = 4, a = 5, whilst the symmetry rules remain for odd base, i.e. the Residue Sequence is

only symmetric about the point a^4 / 2, the ln+1 mechanism guarantees four roots, whereas symmetry for an odd base only gives two. We therefore conclude that somewhere there are two other non-symmetric repetitions of the same residue.

The smallest example of this occurs when a = 5, n = 4 and, hence, a = 4l + 1, l = 1. For the Candidate Pair (38,41) where we see that

38^4 = 3336*5^4 + 136

and

41^4 = 4521*5^4 + 136

therefore

41^4 = 38^4 + 1185*5^4.

Neither 38 nor 41 lie either side of the only symmetry point 5^4 / 2 and thus they are the two, non-symmetric roots of four possible roots. The other two points are easily obtained by symmetry about the centre point 5^4 / 2. The point symmetric to 38 is 587 and the point symmetric to 41 is 584. In all, therefore, we have four roots 38, 41, 584 and 587 all such that, when raised to the fourth power, they are congruent (mod 5^4) with resiude 136.

Notice that in the Residue Table the Quotient Gap also rapidly increases with x and any chance of a Unity Gap is also hopeless for all x>2. That leaves only x = 0 and x = 1 which do not have identical residues. x = 0 is not allowed anyhow since it gives the zero residue and, therefore, the a = 2, n = 4 case has no FLT counter-examples. This is perhaps not surprising but it is a nice, simple dismissal of the a = 2, n = 4 case.

The growth of the Quotient Gap with increasing exponent should be tempered with some caution. The rapid growth is seen above because the base is small relative to the exponent. It is possible to choose a value for the base, sufficiently large, that the growth in the Quotient Gap is effectively tamed.

2.4.10 An Analytic Solution for n = 4?

Although trying to find an analytic solution for the quartic exponent is doomed to failure, using the same technique as in (2.4.4) for the Pythagoras Equation, we can at least see the consequences of such an attempt.

For even base a, divisible by 4, i.e. a = 4l, integer l, l > 0, we have a Minimal Residue Sequence symmetry point (a^4) / 4 which is an exact integer. Either side of this mid-point +/-y, y integral, y > 0, we have identical residues and, consequently, Candidate Pairs (b,c) (mod a^4).

2.4.10.1 b = (a^4) / 4 – y

2.4.10.2 c = (a^4) / 4 + y

Raising b and c to the fourth power and subtracting c^4 - b^4 gives

2.4.10.3 c^4 - b^4 = y*(a^4)*(a^8/64 + y^2)

This is much like the Pythagoras expression, equation (2.4.4.10) and, by comparison, we see that the Quotient Gap Qg is given by

2.4.10.4 Qg = y*(a^8/64 + y^2)

We see that Qg is similar to the Quotient Gap for Pythagoras (Qg = y) but with an extra factor (a^8/64 + y^2). In the Pythagorean case the Quotient Gap was controlled solely by y so we could choose to make it unity. In this case we would have an instant Pythagorean triple. Alternatively, we could make y a perfect square, as in (2.4.4.11), and obtain a solution for a modified base a', see equation (2.4.4.12). Either way, we obtained Pythagorean triples.

The extra factor (a^8/64 + y^2) on the rhs of (2.4.10.4) rules out any hope of making the Quotient Gap unity. Even with y = 1, the smallest possible value of the factor is (a^8/64 + 1) and Qg = (a^8/64 + 1). If there were to be any analytic solution, we must set the factor to a perfect quartic, i.e.

2.4.10.5 k^4 = y*(a^8/64 + y^2)

However, we have seen several times that if, for some base a, we obtain a Candidate Pair with a Quotient Gap that is a perfect power, namely a quartic, say l^4 when n = 4, then there is always a composite base, a' = la, such that the same Candidate Pair has a Quotient Gap of unity when using this new base, modulo (la)^4.

Nevertheless, in moving to a new, composite base a' we have also moved the symmetry point from a^4 / 4 to a'^4 / 4 and we no longer have global symmetry of the Residue Sequence (mod a'^4) about the original symmetry point a^4, instead it is now about a'^4 / 4. This also occurs in the Pythagorean case. Remember that a is an even base, hence symmetry at a^4 / 4. If it were odd, the symmetry would be about a^4 / 2.

So, in the quartic case, we have the potential for a Candidate Pair with a Unity Quotient Gap if we move to a composite base. However, we then lose the original symmetry point. Alternatively, if we keep with symmetry, as above, we still have Candidate Pairs but we now have to consider the possibility that they have a non-unity Quotient Gap which is a perfect power. This was also the case for Pythagoras.

In summary, it would be nice if we could dismiss n = 4 instantly since, for arbitrary base, the Quotient Gap of points about the symmetry points will never be unity. We are stifled from this conclusion since the Quotient Gap can quite legitimately be a perfect power.

Further study of this case, even exponent, n >= 4 remains open.

2.4.11 Summary Even Power Exponent

We have seen that the symmetry in the Residue Sequences for an even exponent generates numerous Candidate Pairs (b,c) (mod a^n), whereby b and c are mirror image points about the symmetry point: a^n / 2 for odd a; (a^n) / 4 for even a.

In the Pythagorean case, for every base except a = 2, there is at least one Candidate Pair (b,c), where b = (a^2 - 1) / 2 and c = (a^2 + 1) / 2 for odd a, and b = a^2 / 4 - 1 and c = a^2 / 4 + 1 for even a, such that the Candidate Pair (b,c) also meets the Quotient Condition and therefore (a, b, c) is a Pythagorean triple.

For all higher, even power exponents, n = 4 and beyond, we know there are no solutions (Fermat himself proved n = 4, the remainder indirectly proven by Wiles [1]) but, since the symmetry in Residue Sequences exists for all even power exponents, there still exists numerous Candidate Pairs (b,c) centred around a symmetry point, albeit we can be sure that none of them meets the Quotient Condition. In fact, at least intuitively, by studying residue tables for n = 4 we can see that the Quotients for such Candidate Pairs (those about symmetry points) grow rapidly and a Quotient Gap of unity is impossible. Nevertheless, this is not to say the Quotient Gap cannot be a perfect power. With FLT proven this is obviously never the case although that has not been proven here.

2.5 Odd Exponent

2.5.1 Skew-Symmetry

For odd power exponents, the point symmetry seen for even exponents is replaced by a skew-symmetry.

A Skew-Symmetric sequence of residues is such that any point x, integer x, 0 <= x <= (a^n) / 2, i.e. x is less than or equal to the mid-point of the Residue Sequence, satisfies the relation

2.5.1.1 (a^n - x)^n = -(x^n) (mod a^n)

That is the residues x^n (mod a^n), for x values in the lower half of the Residue Sequence, are the negative of those in the upper half. In effect, the residues in the upper half are 'conjugate' to those in the lower half and vice versa.

2.5.1.2 Definition: Conjugate

The value (a^n - x) is termed 'conjugate' to the value x when it satisfies (2.5.1.1). Conversely x is also conjugate to (a^n - x).

Because the residues in one half of the Residue Sequence are conjugate to those in the other half they cannot be identical, unlike even exponent residues, except when they are zero - which is discounted by convention. Note that for even base the mid-point, a^n / 2, is a single point and is effectively identical to itself.

If the residues in the lower half are unique then they are unique in the upper half and the entire Residue Sequence is unique. It would seem, therefore, that we cannot obtain a single Candidate Pair that will meet the Residue Condition, i.e. if the residues are all unique in the lower half then there are no Candidate Pairs (no identical/Repeat Residues) and, in one clean sweep, we could prove FLT for odd n! Of course, the assumption of unique residues in one half of a Residue Sequence is fallacious. A Residue Sequence with a unique set of residues is quite common but, for certain base (the '2ln+1' form), Repeat Residues do exist for odd exponent and odd base which can also meet the stringent Root Gap Constraint given by Theorem (1.12), namely that the Root Gap must be less than the base. However, before discussing this, we shall show that skew-symmetry can offer some alternate views on FLT and has links to the complex plane.

If we denote the value b with x in (2.5.1.1) and c as its mirror image about the centre-point, i.e. c = a^n - b, then (2.6.1.1) becomes

2.5.1.3 $b^n = -c^n \pmod{a^n}$

We see that this is of the same form as the original Residue Condition (1.2.3) but with a negative sign, i.e. the residues are not identical but conjugate to each other.

2.5.1.4 Definition: Skew Candidate Pair

A pair (b,c) that satisfy the congruence (2.5.1.3) is termed a 'Skew Candidate Pair'. Rearranging (2.6.1.3)

2.5.1.5 $b^n + c^n = 0 \pmod{a^n}$

which implies, for integer k,

2.5.1.6 $b^n + c^n = k*a^n$ (the Generalised Fermat Equation, section (1.8.2))

If k were to equal unity we would have an FLT counter-example (a, b, c). However, by convention, a < b and a < c and we will see that k >= 2, as follows.

By expanding b^n and c^n in the quotient, remainder form

2.5.1.7 b^n = p*a^n - r

2.5.1.8 c^n = q*a^n + r

and adding b^n and c^n we get

2.5.1.9 b^n + c^n = (q + p)*a^n

Comparing (2.5.1.9) with (2.5.1.6) we see that k is given by

2.5.1.10 k = q + p

By analogy with (1.3.3), which defines a Quotient Gap as the difference of q and p, we define a Quotient Sum, 'Qs' as follows

2.5.1.11 Qs = q + p 'Quotient Sum, Qs'

The value k in (2.5.1.10) is thus synonymous with the Quotient Sum

2.5.1.12 Qs = k

If we assume a < b, a < c, which can be made by initial choice of x such that x > a, (b = x^n, c = a^n - x in (2.6.1.1)), then the quotients q and p in (2.5.1.7) and (2.5.1.8) are such that

2.5.1.13 q >= 1, p >= 1

and therefore the Quotient Sum satisfies the inequality

2.5.1.14 Qs >= 2

That is, the Quotient Sum is always greater than or equal to 2. Alternatively stated, the coefficient k in the Generalised Fermat Equation is always greater than or equal to two.

Because of this, the triple (a, b, c) is clearly not an FLT counter-example. However, k could be a perfect power in a similar fashion to (1.8.3)

2.5.1.15 k = l^n

We would then have a triple (b, c, la) which would be an FLT counter-example, i.e.

2.5.1.16 b^n + c^n = (la)^n

However, we now see that la > b and la >c and we get a new skew-symmetry in the residues similar to (2.5.1.3) as follows

2.5.1.17 b^n = - c^n mod (la)^n

If we re-label c with a and la with c, we get the 'Skew Residue Condition'

2.5.1.18 b^n = -a^n (mod c^n) (the Skew Residue Condition)

And we see that we can achieve the same result by taking residues (mod c^n) of the original FLT equation (1.1.1). This Skew Residue Condition completes a trio of Residue Conditions, the other two being (1.2.3), (1.17.1) for the moduli a^n and b^n respectively.

Reverting to (2.5.1.14), this Quotient Sum Condition shows that a general skew-symmetry (mod a^n) cannot generate FLT counter-examples. Nevertheless we see that from (2.5.1.18) a Candidate Pair (a,b) (mod c^n) does satisfy a skew-symmetry condition. We have to conclude from this that Skew Candidate Pair (a,b) (mod c^n), must be produced via a different mechanism to that of skew-symmetry about a mid-point, as given by (2.5.1.1). Indeed, since both a and b are less than c, when taking residues a^n (mod c) and b^n (mod c), the residues must be skew-symmetric, i.e. satisfy (2.5.1.18), within the interval c. This is effectively a Root Gap condition, analogous to that for a standard Candidate Pair (b,c) (mod a^n), see (1.10). Since this is not possible via a general skew symmetry of the form (2.5.1.1), the only mechanism that can do this is when c is also of the 2ln+1 form. This is quite a big conclusion, because we now require all three values a, b and c to be of the 2ln+1 form or have prime factors of this form. That is, not only must a and b be of 2ln+1 form, but now c too.

2.5.2 Conclusion

From the result in the last section on the form of c we conclude that, for integer m, arbitrary integer factor z, z >= 1, c can take the form

2.5.2.1 c = z(2mn + 1)

where the integers m and z are such that a, b and c remain co-prime, according to convention (0.3.4), and have the following ranges

2.5.2.2 m > 0, n > 0

2.5.3 Summary

Skew-symmetry offers us an alternative view-point. It shows we could possibly arrive at an FLT counter-example by studying skew-symmetric Residue Sequences, if we keep in mind that the modulus is c^n, as opposed to studying symmetric Residue Sequences, (mod a^n) or (mod b^n).We have also seen that there is always a Skew Residue Condition (2.5.1.18) equivalent of the Standard (1.2.3) and Dual Residue Conditions (1.17.1).

That said, general skew-symmetry about a mid-point, as given by (2.5.1.1), can only provide a pointer to a triple (b,c,la) with the largest element 'la', composite, as in (2.5.1.16). This triple will then have to satisfy the Residue and Quotient Conditions for residues c^n (mod b^n) and (la)^n (mod b^n). We are back to having to be able to find Repeat Residues by a non-symmetric mechanism, namely, when the base a is prime of the form 2ln+1 or composite with one or more prime factors of the 2ln+1 form.

It is worth looking back at both odd and even exponents since (2.5.1.18) shows us that a skew-symmetry exists for both odd and even exponent if we take residues (mod c^n) of the FLT equation (1.1.1). For odd exponent the minus sign in (2.5.1.18) can be absorbed into 'a' as follows

2.5.3.1 b^n = (-a)^n (mod c^n) (odd exponent n)

For even exponent we would have to put in a complex 'i' to achieve the same effect, as follows

2.5.3.2 b^n = (ia)^n (mod c^n) (even exponent n)

In fact we could harmonise both (2.5.3.1) and (2.5.3.2) by using an 'nth root of unity u defined by

2.5.3.3 u^n = - 1 (odd or even exponent n)

such that

2.5.3.4 b^n = (ua)^n (mod c^n) (odd or even exponent n)

It is of interest that the leap to usage of the complex plane and, in particular, the n'th roots of unity, seems almost unavoidable when studying FLT. What is symmetric for

even exponent in the integers is skew-symmetric in the complex domain. Conversely, what is skew-symmetric for odd exponent in the integers, is skew-symmetric in the complex domain.

The full depth of these observations is not discussed further in this paper as an aim of this paper, when studying the FLT equation, is to work in integers and integer constraints imposed by studying residues. Section (3) examines Unity Roots 'u', where u^n = 1 (mod a^n), which are modulo arithmetic equivalents of the complex roots of unity. In fact there is an isomorphism between Unity Roots and the complex n'th roots of unity.

2.5.4 Theorem: Summation of a Candidate Pair (b,c)

For odd exponent, if c and b are such that, for integer l, l > 0

2.5.4.1 $c + b = l*a^n$

then

2.5.4.2 $c^n + b^n = 0 \pmod{a^n}$

This theorem gives us a very simple method to construct Skew Candidate Pairs (b,c) by simply choosing any two numbers b and c that satisfy (2.5.4.1). Note that this is not the only method but it is a simple method valid for all odd exponents and arbitrary base a. Another method uses the Repeat Residue properties for base a of the 2ln+1 form.

Proof

Re-arranging (2.5.4.1) for c in terms of b

2.5.4.3 $c = l*a^n - b$

Raising both sides to the n'th power and taking residues (mod a^n) we find that

2.5.4.4 $c^n = (- b)^n \pmod{a^n}$

For odd exponent we can take the minus sign outside of the rhs bracket

2.5.4.5 $(- b)^n = -(b^n)$

which gives

2.5.4.6 c^n = -(b^n) (mod a^n)

And adding b^n to both sides we get

2.5.4.7 c^n + b^n = 0 (mod a^n)

Hence, for some integer l, l > 0 we get

2.5.4.8 c^n + b^n = l*a^n

and so the Theorem is proven.

2.5.5 Generalised Fermat Equation

The Generalised Fermat Equation, mentioned in (1.8.2) and (2.5.1.6) and reproduced below, is a much-studied equation in Number Theory.

2.5.5.1 b^n + c^n = k*a^n (the Generalised Fermat Equation)

For odd n, the skew-symmetry of residues b and c, (mod a^n), as given by (2.5.1.3), gives rise to an infinity of solutions.

If b is an arbitrary integer, 0< b < a ^n, and c is defined as its 'conjugate'

2.5.5.2 c = a^n - b

then clearly

2.5.5.3 c^n = - b^n (mod a^n)

and consequently, for some integer k, k > 0, also termed ‘Qs’, the Quotient Sum in (2.5.1.11), we can write

2.5.5.4 c^n + b^n = k*a^n

We showed in equation (2.5.1.14) that k (=Qs) was greater than or equal to 2. Obviously, if it were 1, we would have an FLT counter-example.

The study of the possible values for k is outside the scope of this paper but a few values for n = 3 and n = 5 are given below. The values of k for which there are possible solutions can be found at Mathworld, ref [4], keyword 'Generalized Fermat Equation' (note the US spelling of Generalized with a ‘z’).

For n = 3, the first few published values are

k ={2, 6, 7, 9, 12, 13, 15, 16, 17, 19, 20, 22, 26,
28, 30, 31, 33, 34, 35, 37, 42, 43, 48, 49, 50...}

For n = 5, the first few published values are

k ={2, 31, 33, 64, 211, 242, 244, 275, 486, 781, 942...}

Since Skew Candidate Pairs (b,c), constructed according to (2.5.4.1), are in abundance, we can see that there must be many different values of the Quotient Sum k. If a is odd, prime, and not of the 2ln+1 form, there are in fact (a^n - 1) / 2 unique pairs (b,c). So, for 0 < b < (a^n - 1) / 2, it is probable that there are also (a^n - 1) / 2 unique values for k. Of course, we needn't restrict ourselves to 0 < b < a ^n and we can construct a pair for any arbitrary value of b.

A general pair (b',c') is constructed for 0 < b < (a^n - 1) / 2, integer l, m >= 0, as follows. Let b' and c' be defined as

2.5.5.5 $b' = l*a^n + b$

2.5.5.6 $c' = m*a^n - b$

then we see that

2.5.5.7 $c'^n = - b'n \pmod{a^n}$

and therefore, for some integer k

2.5.5.8 $b'^n + c'n = k*a^n$

i.e. the pair (b',c') is a Skew Candidate Pair with a Quotient Sum k.

2.5.5.9 Example

To see how k varies, take a simple example

Let

a = 7, n = 3, l = 0, m = 1

then, by varying b from 1 to the mid-point at 171 (= (7^3 - 1) / 2), i.e. 0 < b < 172, we get the following for b', c' and k

b = 1, b' = 1, c' = 342, k = 116623
b = 2, b' = 2, c' = 341, k = 115603
b = 3, b' = 3, c' = 340, k = 114589

b = 169, b' = 169, c' = 174, k = 29431
b = 170, b' = 170, c' = 173, k = 29419
b = 171, b' = 171, c' = 172, k = 29413

The k value decreases monotonically from a high at b = 1 to a minimum at the mid-point b = 171. We could see this by some algebraic manipulation of the differences ((b + 1)^3 - b) / a^3). That aside, it is noticed that k is relatively large, especially when looking at the published values for k which start at k =2. This is, of course, the lowest possible value k could be without there existing an FLT counter-example. This implies that our mechanism, shown above, to construct Skew Candidate Pairs is not that which leads to such low values for k. As mentioned, in section (2.2), there are several mechanisms for Repeat Residues. Whilst the '2ln+1' form of the base is strictly necessary to generate FLT counter-examples, where k = 1, other mechanisms, such as the exponent dividing the base, can provide smaller values of k than those listed above. Ultimately, however, it has to be the '2ln+1' mechanism that is responsible for producing the smallest k values.

When the exponent divides the base a, i.e. n | a, we obtain a Minimal Residue Sequence of size n times smaller than a^n, i.e. a^n / n or a^n - 1, see section (2.2.2). By definition, consecutive Minimal Residue Sequences repeat n times within the full 0 <= x < a ^n interval. Hence, Repeat Residues and skew-symmetric residues repeat at a much smaller interval. For instance, we can construct much more closely spaced and smaller absolute values of b' and c' since a^n in (2.5.5.5) and (2.5.5.6) is replaced by a^(n - 1).

To get some smaller k values, let l = 0 and m = 1 then, if n | a,

2.5.5.10 b' = b

2.5.5.11 c' = a^(n - 1) - b

To see how k varies in this case, take a simple example

2.5.5.12 Example a = 6, n = 3

This example shows how a smaller value for k can be obtained when the exponent n divides the base a.

let

a = 6, n = 3, l = 0, m = 1

then the Minimal Residue Sequence size is 6^3 / 3 = 72. The midway point is 36 and so, repeating example (2.5.5.9), for a few values of b we get

b = 1, b' = 1, c' = 71, k = 1657
b = 2, b' = 2, c' = 70, k = 1588
b = 3, b' = 3, c' = 69, k = 1521

b = 33, b' = 33, c' = 39, k = 441
b = 34, b' = 34, c' = 38, k = 436
b = 35, b' = 35, c' = 37, k = 433
b = 36, b' = 36, c' = 36, k = 452

We see that k is indeed a lot smaller if n | a.

However, we can get even smaller values for k by ensuring that, within the Minimum Residue Sequence, there are also Repeat Residues. This we can do by making the base composite of form a =n*m where the other factor m is both prime and of the 2ln+1 form. For n = 3, the smallest such base is a = 3*7 since 3 | 21 and 7 is of the 2ln+1 form where l = 1.

Using a computer, the following Skew Candidate Pairs have been extracted. Each Skew Candidate Pair, in the (b,c) notation, has been tabulated below with the k value in the second column.

(b,c)	k
[17,37]	6
[28,35]	7 *
[54,57]	37
[56,70]	56 *
[91,98]	183 *

* These Skew Candidate Pairs have a common factor of 7. This tells us, by Theorem (TBD) that, in fact, the a = 3, n = 3 case has the following Candidate Pairs, each with the same Quotient Gap.

(b,c)	k
[13,14]	183
[4,5]	7
[8,10]	56

We see that the k value has been considerably reduced to more within the range of published values. This was, of course, a one-off example and we might be able to identify other published values for other examples of the base.

The first value, k = 6, is actually the second smallest published value for the exponent n = 3. The lowest published value is 2. It would be nice to obtain a Skew Candidate Pair that gives this k value - something we are working on.

Lastly, in the same study, a Candidate Pair (51, 60) was identified that satisfies the GFLT equation (1.9.1) and the Quotient Gap is 9, i.e.

60^3 = 51^3 (mod 21^3)

60^3 = 51^3 + 9*21^3

It is actually of no coincidence that the pair [51, 60] = 3*[17, 20] since [17, 20] is a Candidate Pair for the prime factor 7 and Theorem (TBD) proves that if (b,c) is a Candidate Pair (mod s^n) then, for integers s and t, so too is the pair (t*b, t*c) (mod (s*t)^n).

2.5.6 Theorem: Standard and Skew Candidate Pair Duality

For every Candidate Pair (b,c), (mod a^n), odd exponent n, that satisfies the GFLT equation (1.8.1), there is an equivalent Skew Candidate Pair (b',c), where b' is the conjugate of b (mod a^n), such that (a, b', c) satisfies the Generalised Fermat Equation (2.5.5.1).

Proof

Since (b,c) are a Candidate Pair then, by definition

2.5.6.1 c^n = b^n (mod a^n)

hence,

2.5.6.2 c^n - b^n = 0 (mod a^n)

For odd exponent, this can be re-written

2.5.6.3 c^n + (- b)^n = 0 (mod a^n)

Defining b' as the conjugate of b

2.5.6.4 b' = a^n + - b

then

2.5.6.5 b' = - b (mod a^n)

and raising both sides to the n'th power gives

2.5.6.6 b'^n = (- b)^n (mod a^n)

Substituting for (- b)^n from (2.5.6.6) into (2.5.6.3) we get

2.5.6.7 c^n + b'^n = 0 (mod a^n)

and therefore, for some integer k, k > 0,

2.5.6.8 c^n + b'^n = k*a^n

Taking residues (mod a^n) of (2.5.6.8) gives

2.5.6.9 c^n = -(b'^n) (mod a^n)

and we see that (b',c) form a Skew Candidate Pair and that, by (2.5.6.8), the triple (a, b', c) is therefore a solution to the Generalised Fermat Equation (2.5.5.1).

Notes

This Theorem establishes a correspondence between our GFLT Equation (1.8.1) and the Generalised Fermat Equation (2.5.5.1) i.e. a solution to one provides a solution to the other and any result arising from one can be applied to the other.

It is easier to work with Candidate Pairs (b,c), rather than their skew-symmetric counterparts (b',c), because identifying b' entails matching a residue c^n (mod a^n), with a conjugate counter-part b', defined by (2.5.6.4). Whereas finding a Candidate Pair (b,c) involves simply finding two matching residues without any negation of sign, (b to -b in (2.5.6.4)), and then addition of a^n as in a^n + -b - also in(2.5.6.4)).

2.5.6.10 Example

n = 3, a = 7

Let b = 20, c = 17 where, by design, (17, 20) is a Candidate Pair (mod 7^3) and therefore satisfies the following congruence relation

20^3 = 17^3 (mod 7^3)

By (2.6.8.4) we get a value for b' of 326 since

b' = 7^3 - 17 = 326

Thus, by Theorem (2.5.6), the Skew Candidate Pair (b',c) = (326,20) satisfies the congruence relation (2.6.8.9)

20^3 = -326^3 (mod 7^3)

and the triple (7, 326, 20) satisfies the Generalised Fermat Equation (2.5.5.1) where the integer k is 101032

20^3 + 326^3 = 101032*7^3

This completes our discussion on skew-symmetric matters and we revert back to the 2ln+1 form and a more intuitive discussion on where hence it originates.

2.5.7 Why 2ln+1?

A rigorous proof of the 2ln+1 form comes via Lagrange's Theorem, see section (2.2.5) for a brief background to it. Also see Davenport [6] for a more formal explanation.

As a start we will consider prime bases and discuss composite bases later since the theory for composites is essentially that of its prime factors.

That the base is prime and of the form 2ln+1, integer l, l > 0, can be thought of as a divisibility condition on the base a, i.e. (2ln + 1) | a, that guarantees repetition of non - zero residues x^n (mod a^n) within an interval 0 <= x < a^n. More importantly, some residues may repeat within a much smaller interval less than the base value a. The latter, smaller interval of size a allows for the possibility that any Repeat Residues may meet the Quotient Condition (1.4.3) by virtue of Theorem (1.12).

For prime a, the number 'm' of unique, non-zero residues 'r', (mod a), as defined by the following equation, for integer x, 0 <= x < a,

2.5.7.1 x^n = r (mod a)

and subject to the condition

2.5.7.2 n | (a - 1)

is given by

2.5.7.3 m = (a - 1) / n

Since for every root x, residue r, there is always a conjugate root (a - x), residue -r, the condition (2.6.9.3) has to be tightened to

2.5.7.4 2n | (a - 1)

That is, for some integer l, l > 0, the base a must be of the form

2.5.7.5 a = 2ln + 1

If n does not divide (a - 1) there are 'a' unique residues for prime a, i.e. if n !| (a - 1), then m = a.

In other words, the '2l' of '2ln+1' is the number of unique, non-zero residues, x^n (mod a), prime a, 0 < x < a. The residues can be paired off since, for each unique residue r, there is a conjugate -r and hence the factor of 2 in '2l'. Each unique, non-zero residue occurs n times and the +1 accounts for the single zero residue r = 0 at x = 0. Lastly, (a - 1) must be divisible by 2n and hence a = 2ln+1 for integer l, l > 0.

2.5.7.6 Example

If a = 7, n = 3, then m = 2 and there are two (= (7 - 1) / 3) unique, non-zero residues (actually +1 and –1 where –1 = 6 (mod 7)). The zero residue, x = 0, is the third and only other residue.

2.5.7.7 Example

If a = 13, n = 3, then m = 4 (= (13 - 1) / 3) and, including zero, there are five unique residues (0, +1, - 1, +8, -8).

2.5.7.8 Example

If a = 5, n = 3 then since 6 !| (5 - 1), m = 5 and, including zero, there are five unique residues (0, +1, +2, +3, +4).

2.5.7.9 Example

If a = 11, n = 5 then since 5 | (11 - 1), m = 2 and, including zero, there are the minimum three unique residues (0, +1, - 1 where -1 = 10 (mod 11)).

2.5.8 Odd and Even Exponent Comparison

The '2ln+1' condition applies to odd exponents and, for even exponents, the condition is a slightly more relaxed 'ln+1' form. So far we haven't discussed this ln+1 form since, in this paper, we really wanted to show that a symmetry argument and not Lagrange's Theorem is, in the case of the even exponent, n = 2, the responsible mechanism for generating Pythagorean triples. Furthermore, this symmetry argument leads to the standard analytic solution for such Pythagorean triples. On the other hand, for odd exponent, the symmetry is replaced by skew-symmetry which can only give us solutions to the Generalised Fermat Equation (section (1.8.2)) but not FLT counter-examples.

That there are exactly n solutions for a prime base P is not of particular significance in the arguments herein. The only matter of real importance is that there is always more than one root. This is so for even power exponents since they always possess at least two roots by virtue of symmetry in the Residue Sequence. Two solutions is enough to generate Repeat Residues, i.e. a Candidate Pairs. This would also be true for any even exponent n >= 4. So whether there are more than two solutions is of little consequence to the symmetry arguments presented. Nevertheless, four or more roots would only increase the likelihood of more Repeat Residues. Counteracting this bonus is the problem that as the exponent grows the Quotient Gap also grows rapidly for Candidate Pairs centred upon these symmetry points. Albeit, this hasn't been rigorously proven and this is slightly deviating from the point.

For odd exponent we don't have the point symmetry in the Residue Sequence and we do need another mechanism to Repeat Residues within a constrained range, that of the base, Theorem (1.12). This other mechanism is possible through the requirement that the base is of the '2ln+1' form.

To generate solutions, in the Pythagorean case, the ln+1 form is n = 2l+1 since n = 2. That is, any prime, odd base will suffice to give exactly two solutions and hence Repeat Residues. Since we know that in all Pythagorean Triples (a, b, c) one member of the pair a and b is odd this confirms the ln+1 requirement. For example, with the prime base a = 3, we know that (3, 4, 5) is a Pythagorean triple and we know $4^2 = 5^2 \pmod{3^2}$ i.e. (4, 5) are two solutions which could arise as a consequence of the two Unity Roots. This might seem to confirm the ln+1 mechanism as providing Repeat Residues.

[Note that in all our work the modulus (the n'th power of the base) is usually a^n, i.e. it is never actually prime but composite with a single factor 'a' when a is prime. However, this does not change the arguments on the number of roots for prime base. The base can be of the form ln+1 or be composite with one or more factors of the ln+1 form. For n = 2, this would only mean the base has one or more odd factors].

However, by duality arguments in section (1.17.1), we could get a similar result for the Pythagorean triple (3, 4, 5) using the base b = 4 since $3^2 = 5^2 \pmod{4^2}$. But now the base is not of the ln+1 form and neither is its factor 2 of that form. Therefore we have Repeat Residues (4, 5) that do not arise by the ln+1 argument but, rather, by the symmetry of an even power exponent. The same applies to the Pythagorean triple (8, 15, 17) with base a = 8 and, in fact, it applies to any triple with the base a of the form a = 2^k, k >= 2 does not adhere to the ln+1 form. Contrast this with a general odd exponent, whereby ALL members of the triple (a, b, c) must be of the 2ln+1 form. We are forced to conclude that the 'ln+1' form, arising from Lagrange's Theorem, is not wholly responsible for Pythagorean triples.

If we study the n = 4 case, the smallest base of the ln+1 form is 5. The residue table for n = 4, a = 5 confirm there are four Unity Root solutions (see (7.2.2)) and we can find all other Repeat Residues in sets of four. Hence, any pair out of the four repeats could be a potential Candidate Pair. Nevertheless, Fermat himself proved that there are no solutions for the n = 4 case and we therefore know that we won't find any candidate Pairs that meet the Quotient Condition. It is slightly sad that solutions stop at n = 2! It would be nice if they stopped at n = 4 since we might be able to confirm

symmetry arguments for any solutions. On the other hand, if there were solutions, it is unlikely that FLT would have remained unproven for such a long time.

In concluding, the ln+1 form, that produces n roots and therefore more than one Repeat Residue for n >= 2, is valid for odd and even exponents. But, at least for n = 2, it would not seem able to explain ALL Pythagorean triples. In particular those where the base is of the form 2^s, s > 1 and hence have no odd factors of the 2l+1 form. On the other hand, all Pythagorean solutions can be explained by symmetry in a Residue Sequence arising from an even power exponent.

We thus conclude tht it is a symmetry in the residue sequence that generates Pythagorean Triples and that Lagrange's Theorem is not the responsible mechanism for all solutions.

2.5.9 Repeat residues (mod a)

To re-cap, by Theorem (1.12), it is a necessity that for any FLT counter example (a, b, c) the residues for a Candidate Pair (b,c) repeat within an interval, termed the 'Root Gap', section (1.10), of size less than the base a, i.e. 0 < Rg < a. Dual arguments also apply for the Candidate Pair (a,c) (mod b^n). For even exponent this is an easy requirement since the residues are symmetric about a mid-point. In particular, those immediately either side of the mid-point are essentially back-to-back with a Root Gap of 1 for odd base a and 2 for even base a. Such Candidate Pairs are numerous for Pythagoras and such pairs also meet the Quotient Condition, hence there are numerous Pythagorean Triples. For even exponent n >2, i.e. n = 4 etc, the symmetry is still present and there are also numerous Candidate Pairs. Nevertheless, such pairs no longer meet the Quotient Condition since the exponent causes the quotients to grow rapidly. On the other hand, such a large Quotient Gap could still be a perfect square.

For odd n, there is no longer an automatic supply of Repeat Residues since the symmetry is no longer present. Nevertheless, there is the ‘2ln+1’ mechanism to give Repeat Residues (mod a) and, consequently, also the possibility they may repeat (mod a^n) within the Root Gap interval 0 < Rg < a. Thus, also providing a Candidate Pair (b,c) that satisfies the Quotient Condition and which might, ultimately, be an FLT counter-example.

If a residue repeats (mod a^n) it always repeats (mod a^(n - 1)), (mod a^(n -2)) etc down to (mod a), i.e. if (b,c) is a Candidate Pair then b and c also have identical residues (mod a^(n - 1)), (mod a^(n -2)) etc. all the way down to (mod a).

This is easily seen since, given that b and c are a Candidate Pair (b,c), where

2.5.9.1 $b^n = r \pmod{a^n}$

and

2.5.9.2 $c^n = r \pmod{a^n}$

then, expressed in the quotient, remainder form b^n, and c^n are

2.5.9.3 $b^n = p*a^n + r$

2.5.9.4 $c^n = q*a^n + r$

and, by rearranging the quotients, we see that

2.5.9.5 $b^n = (p*a)*a^{(n - 1)} + r$

2.5.9.6 $c^n = (q*a)*a^{(n - 1)} + r$

and so

2.5.9.7 $b^n = r \bmod a^{(n - 1)}$

2.5.9.8 $c^n = r \bmod a^{(n - 1)}$

Thus, b and c are congruent (mod $a^{(n - 1)}$), i.e.

2.5.9.9 $b^n = c^n \bmod a^{(n - 1)}$

and therefore form a Candidate Pair mod $a^{(n - 1)}$.

We can continue in this way down to n = 1, i.e. (mod a), such that

2.5.9.10 $b^n = c^n \pmod{a}$

and hence b and c also form a Candidate Pair (mod a).

All Candidate Pairs (b,c) (mod a^n) are therefore also Repeat Residues (mod a). The converse is rarely true, i.e. most Repeat Residues (mod a) are not Candidate Pairs (mod a^n). Nevertheless, if a residue does not repeat (mod a) it will not repeat (mod a^n). Thus, we do need repetition of residues (mod a) as a starting point to find residues (mod a^n). Alternatively stated, if the residues x^n (mod a) are all unique, which they are if condition (2.5.7.4) is false, i.e. (a - 1) is not divisible by 2n, then there will be no Repeat Residues x^n (mod a^n) within an interval of size a. Consequently, there will be no Candidate Pairs (b,c) (mod a^n) such that the Root

Gap is less than a and, by Theorem (1.12), the Quotient Condition will never be met for any Candidate Pair (mod a^n).

We now look in more detail at the repetition of residues (mod a), where a is prime.

Considering the residues r for values of x, 0 <= x < a, given by the following

2.5.9.11 x^n = r (mod a)

Firstly, for any n, odd or even, and any base, composite or prime, there is always a zero and unity residue since, for x = 0 and x = 1,

2.5.9.12 0^n = 0 (mod a)

2.5.9.13 1^n = 1 (mod a)

Additionally, for odd n, there is always a negative Unity Root since

2.5.9.14 -1^n = - 1 (mod a)

Thus, for odd n, n >= 3, the minimum number of unique residues (mod a) is 3 and they are - 1, 0 and +1.

The zero residue occurs only once and is its own conjugate, i.e. -0 = +0. On the other hand, for each occurrence of residue +1, there is a corresponding 'conjugate' residue - 1 since if

2.5.9.15 x^n = 1 (mod a)

then

2.5.9.16 (a - 1)^n = -1 (mod a)

The values of x which have a unity residue +1 are given by solving the following Diophantine equation

2.5.9.17 x^n = 1 (mod a)

Obviously x = 1 is always a solution as in (2.5.9.13). If (2.5.9.17) were an algebraic polynomial x^n = 1 it would, by the Fundamental Theorem (ref TBD) have n roots. For such a polynomial, these Unity Roots are termed the nth roots of unity. For odd n, n - 1 of these n roots are complex and one is real, namely x = 1.

In the case of the Diophantine polynomial (2.5.9.17), where we want unique integer solutions, there are not always n of them for arbitrary a. If, however, there is a Unity Root other than x = 1, then there will be n of them. In other words, there is either one or n Unity Roots for certain values of a. Similarly, if there is a negative Unity Root other than x =- 1 then there will be n of them. For prime a there will also be a single solitary zero root (mod a) and so we have thus accounted for 2n+1 residues. Since there can at most be 'a' residues (mod a), unique or otherwise, the 2n+1 residues must fit into this set. As a minimum then, a must be of size 2n+1 for odd n.

Thus, for any odd, prime base of the form 2n+1 there will always be 2n values of x which have a residue of +1 or -1 and a single zero root. This leaves no room for any other residues and the only n'th order residues (mod a) are {0, +1, -1}.

The smallest odd exponent under consideration is n = 3 and, if a = 7, hence 2n+1= 7, we will only get the residues 0, +1 and -1 and no others. Looking at the first seven entries in the Residue table for a = 7, n = 3 (fourth column in the table below) confirms this. Note that -1 = 6 (mod 7) hence the appearance of 6 and not -1 in column 4.

Residue Table a = 7, n = 3

x	x^n	residue (mod a^n)	residue mod a	quotient
0	0	0	0	0
1	1	1	1	0
2	8	8	1	0
3	27	27	6	0
4	64	64	1	0
5	125	125	6	0
6	216	216	6	0

Notes

Although the residues (mod a) repeat within the interval 0 <= x < a, the residues (mod a^n) do not repeat. In fact, residues x^n (mod a), prime a, 0 <= x < a will not repeat since x^n < a^n. This applies to all a, prime or composite, arbitrary exponent n. Hence there are never Repeat Residues (mod a^n) in any interval where k*a^n <= x < (k*a^n) + a, integer k, k >= 0, i.e. they are all unique. One consequently would not look for Candidate Pairs (b,c) within this particular interval. Furthermore, the minimum gap between repetition of a residue (mod a) is therefore a. In such a case, by Theorem (1.12), any Repeat Residues (mod a) cannot meet the Quotient Condition and, hence, a unique Residue Sequence (mod a) is of no consequence re possible FLT counter-examples.

The case a = 7, n = 3 is one of an infinite set of cases where there are only three unique residues 0, +1 and -1. a = 7 is the smallest possible prime value. If a = 3 or 5, the Residue Sequence is unique - for a = 3 it is {0, 1, 2} and, for a = 5, the sequence is {0, 1, 3, 2, 4}. This is also the case for any prime that is not of the 2ln+1 form. In the case a = 7 the integer 'l' in (2.5.7.5) is 1. We can see from (2.5.7.5) that for any case where a = 2n + 1, i.e. l = 1, there will only be three unique residues (mod a). The fact

that, for any x, prime base a, 0 < x < a, it's residue x^n (mod a) will be either +1 or -1 can form the basis of a primality test 'MFST' which we have detailed in section (4.5). MFST is an abbreviation of 'Modified Fermat's Small (Little) Theorem'. However, it is basically the more commonly known 'Strong Pesudo-Prime Test'.

To quickly recap, if a is prime and of the 2n+1 form then there are guaranteed n Unity Roots such that x^n = 1 (mod a) and also n conjugate Unity Roots such that x^n = - 1 (mod a). Additionally, there is the single zero root x = 0. The entire set of residues x^n (mod a), 0 <= x < a, is {0, +1, -1}. Since there are multiple roots for each non-zero residue, each residue effectively repeats (mod a) and, from the discussion following (2.5.9.10), this may mean that there are some Repeat Residues (mod a^n) which might meet the Quotient Condition and hence would be FLT counter-examples.

So far we have restricted ourselves to the residues 0, +1 and - 1. If a is of the 2ln + 1 form where l >1, then there will be other residues r, equation (2.5.9.11) where |r|>1, which also repeat. For instance, if a = 13, n = 3, then l = 2 and, of the 13 possible residues, one will be zero, three will be +1, three will be minus –1. This leaves six possible non-zero, non-unity residues remaining. In fact, there are only two other unique residues for a = 13, n = 3 since they too will repeat three times each and thus account for the remaining six. These two residues are 5 and 8 and the residue 8 is actually conjugate to 5 (mod 13) and vice versa, i.e. -5 = +8 (mod 13). The entire residue set is thus {0, +1, -1, +5, -5}. Note that in the language of n'th order residues, +1, +5, -1 and -5 are cubic residues of 13. For even exponent, n = 2, this is the much-studied subject of 'Quadratic Residues', see ref [6] for more details on the subject.

The first 13 entries x^n (mod a), 0 <= x <13, are shown in the residue table below, fourth column. Note that 12 = -1 (mod 13) hence the residue value 12 is shown instead of -1.

Residue Table a = 13, n = 3

x	x^n	residue (mod a^n)	residue mod a	quotient
0	0	0	0	0
1	1	1	1	0
2	8	8	8	0
3	27	27	1	0
4	64	64	12	0
5	125	125	8	0
6	216	216	8	0
7	343	343	5	0
8	512	512	5	0
9	729	729	1	0
10	1000	1000	12	0
11	1331	1331	5	0
12	1728	1728	12	0
13	2197	0	0	1

The key point here is not the specific value of the extra, unique residues 5 and 8 but that they also repeat n times where n = 3. In other words, we have yet more Repeat Residues (mod a) in addition to the +1 and - 1 residues that might also repeat (mod a^n). A glance at the table above shows that not only do they repeat but, for example

in the case of r = 8, we see that the repeats occur for consecutive values of x = 5 and x = 6. This gives a unity Root Gap and, should this repetition also occur (mod 13^3), then we would have a Candidate Pair (5,6) with a Root Gap of unity that would have a good (ish) chance of meeting the Quotient Condition. Of course, as shown above, x = 5 and x = 6 are NOT such that 5^3 = 6^3 (mod 13^3) so (5, 6) is not a Candidate Pair (mod 13^3). However, since all residues x^n (mod a) repeat at (x + k*a)^n (mod a), we know that the residue for x = 5 will repeat at 5 + k*13, similarly the residue at x = 6 will repeat at 6 + k*13 and maybe, therefore, there exists some integer k such that (5 + k*13)^3 = (6 + k*13)^3 (mod 13^3) in which case the pair (5 + k*13, 6 + k*13) is a Candidate Pair (mod 13^3). In a dream-world of FLT counter-examples, such a pair might meet the Quotient Condition!

That the other unique, non-zero residues (mod a) also repeat n times when a is prime is basically because, for certain residues r, there are n integer roots to the equation (2.5.9.11). Since each root has a conjugate there are n roots for r and always n roots for -r, each residue pair r and -r consumes 2n roots. If we started with the basic residue set {0,+1,- 1}, prime a, a = 2n+1 and then added another root for residue r, the residue set would then be {0, +1, -1, +r, -r} and we would have to accommodate another 2n values of x, hence a grows from 2n + 1 to a = (2n + 1) + 2n, i.e. a = (2*2n) + 1. Any value of a between 2n + 1 and 4n + 1 would not be able to fit enough integer roots. We can therefore see that if we keep incrementing the base by 2n and, ensuring it remains prime, it will always be of the 2ln+1 form and will provide multiple (copious) Repeat Residues.

2.5.10 Repeat residues (mod a^n)

The previous section (2.5.9) discussed Repeat Residues (mod a). However, that is a stepping stone to what is really required namely, Repeat Residues (mod a^n).

The transition from residues (mod a) to (mod a^n) is actually very simple. This is because we have not actually changed the degree of the Diophantine equation, only the modulus from a to a^n. If we can handle all values of a then amongst them would be those where a was a perfect nth power, e.g. a = k^n.

The condition that the base is prime, of the form 2ln+1, remains for now as regards derivation of some equations. A discussion on composites is deferred to Sections (2.5.14) and (3.9.2). Nevertheless we shall assume the results can be extended to composites and will often refer to the base as either prime of the 2ln+1 form, or composite of 2ln+1 form.

To meet the Root Gap Constraint (1.12) we require, by necessity, that residues repeat within an interval of size a and this can only occur if the residues repeat (mod a). For repetition of residues, therefore, the value of the base remains constrained to prime of the form 2ln+1 or composite with one or more prime factors of form 2ln+1.

Considering the residues x^n (mod a^n), 0 <= x < a^n.

2.5.10.1 x^n = r (mod a^n)

As for section (2.5.9), we know that for odd n, and any base, composite or prime, the 0, +1 and -1 residues are always present.

2.5.10.2 0^n = 0 (mod a^n)

2.5.10.3 1^n = 1 (mod a^n)

2.5.10.4 -1^n = -1 (mod a^n)

Since the modulus a^n is effectively composite, with the single factor a repeated n times, we now have multiple zero residues at integer multiples of k (mod a^n), i.e. for integer k, k >= 0, (k*a)^n = 0 (mod a^n). Since zero residues now occur at intervals of a throughout the entire range 0 <= x < a^n, the number of zero residues 'Nz' is now given by

2.5.10.5 Nz = a^n / a

and we have a^(n - 1) of them

2.5.10.6 Nz = a^(n - 1)

This leaves the number of available non-zero residues 'Nnz' as

2.5.10.7 Nnz = a^n - Nz

Substituting for Nz from (2.5.10.6) into (2.5.10.7) gives

2.5.10.8 Nnz = a^(n-1) * (a - 1)

and substituting for a from (2.5.7.5) into (2.5.10.8) gives

2.5.10.9 Nnz = a^(n-1) * 2ln

The number of non-zero residues is consequently a multiple of 2n which is a requirement for repeat residues (mod a^n).

As for (mod a), there can be n Unity Roots, (mod a^n), given by solving the following Diophantine equation

2.5.10.10 $x^n = +1 \pmod{a^n}$

and, for each occurrence of the residue +1 at root x, there is a corresponding 'conjugate' residue '-1' (mod a^n) at root (a^n - x), hence there are also n conjugate roots

2.5.10.11 $x^n = -1 \pmod{a^n}$

Similarly, and more generally, if there is a root x such that

2.5.10.12 $x^n = +r \pmod{a}$

then there are n of them and there will also be n conjugate roots (a^n - x) where

2.5.10.13 $(a^n - x)^n = -r \pmod{a^n}$

Exactly as for the (mod a) case, we see that a root and its conjugate occupy 2n values. Since we make no distinction on the non-zero residue r, (2.5.10.12), all pairs of roots x, -x for residues r, -r respectively, will occupy some multiple of 2n and thus we require the number of non-zero residues to be a multiple of 2n. Indeed equation (2.5.10.9) shows us this is the case if the base is of the form 2ln+1.

[Note that 2ln+1 could actually be composite here. However, referring right back to Lagrange's Theorem and in particular, equation (2.2.5.7), the base used in that derivation is assumed prime. We require the primality condition for the case (mod a) and we will keep with it for this (mod a^n) discussion. In fact, the base can be composite of 2ln+1 form but only if it also has one or more factors of 2ln+1 form. If it is composite of 2ln+1 form but has no factors of this form then it will not produce the desired repetition of residues and we therefore reject those cases since they will not produce repeat residues with an interval of the base, see the previous section (2.5.9). For example, if n=3 then a=25 is composite of 2ln+1 form but has a repeat factor of 5 which is clearly not of 2ln+1 form. We would therefore reject this case since all the residues x^3 mod 5, 0 <= x < 5 will not repeat.]

Returning to the main discussion, we see that, for every non-zero residue r which is an nth order residue (mod a^n), there will be n roots if the base is prime of the form 2ln+1 or composite with at least one prime factor of the form 2ln+1.

Conversely, if the base is not of the desired form then each residue r is unique and occurs once only if the base is prime. Alternatively, if the base is composite, with no factors of the form 2ln+1 and/or it is not divisible by the exponent n, Repeat Residues can occur but not within the Root Gap requirement, and these cases have been prior rejected, see section (2.2). For composites, with a prime factor of the form 2ln+1, we are only interested in values of x which are co-prime to the base for the reason of 'co-primality in pairs' (0.3.4).

Notes

The 'Unity Root' equation (2.5.10.10) is of key importance in the further development of this work, primarily on unifying all the mechanisms for repetition of residues for both odd and even exponent. This subject is discussed extensively in section (3).

2.5.10.14 Exponent n = 3, base a = 5

The base a = 5 is the smallest value for a such that it is neither composite nor is it divisble by the exponent. Since it is not of the form 2ln+1 then, from what has been said prior in this section, all its non-zero residues x^n (mod a^n) should be unique in the 0 <= x < 5^3 interval. The residue table, section (7.1.4), confirms this. For each x, where x is not a multiple of 5, there is a unique, non-zero residue r.

2.5.10.15 Exponent n = 3, base a = 7

This is the smallest case for both the base and odd exponent, which permits Repeat Residues within the constraints of the Quotient Condition. The Residue Table is given in section (7.1.5).

The first and, as we shall see later, most important residue is r = 1 for which the Unity Roots are found by inspection to be 1, 18 and 324. That 324 = 18^2 is actually no surprise since Unity Roots are cyclic. This is fully discussed in Section (3).

If we look at the residue r = 8 as an example of a non-unity residue, we see this residue repeats three times at x = 2, x = 36 and and x = 305. Indeed, those residues that do repeat repeat three times, as expected, since the exponent n = 3. This can be verified by picking a value for x at random, except where x is a multiple of 7 and therefore has a zero residue, and checking the repetition of its residue (mod a^n) occurs three times, including its first occurence at x.

Since a = 7, n = 3 has Repeat Residues, do any residues repeat within an interval of size a? The answer is yes - the smallest x for which this occurs is x = 17, r = 111 which repeats again at x = 20 and x = 306. Therefore, assigning b = 17 and c = 20, the pair (17, 20) is a Candidate Pair (mod 7^3) with a Root Gap, Rg = 3 (= 20 - 17). Not surprisingly, the Quotient Gap is not unity but 9 (= 23 - 14) since the quotients are p = 14 and q = 23 for b = 17 and c = 20 respectively, see column 5. Because the pair (17, 20) do have identical residues they are a solution to the GFLT equation, see Example (1.8.8).

Actually, the Candidate Pair (17, 20) (mod 7^3) could be rejected immediately, without recourse to checking the Quotient Condition, for three separate reasons a) to c) outlined as follows:

a) Theorem (1.15) asserts that the middle value 'b' of the triple (a, b, c) is always composite. Here the middle value of the triple (7, 17, 20) is 17 which is prime so we can reject it immediately. Note that even if b were composite, the Dual Residue Condition (1.17.1) implies that the middle value must have one or more prime factors of the form 2ln+1.

b) By the Dual Residue Condition (1.17.1), the pair (7, 20) (mod 17^3) is not a Dual Candidate Pair since 7^3 != 20^3 (mod 17^3).

c) By Theorem (1.14) since a is prime, the Root Gap must be unity but, since the Root Gap here is 3 (= 20 - 17), we can reject (17, 20).

Including the Quotient Condition, and reasons a) to c) above, we have four reasons to reject (17, 20) as a potential FLT counter-example. Even without any reference to other published FLT work, that Candidate Pairs such as (17, 20), with a Root Gap less than the base, appear nowhere near in abundance to those for even exponent would hopefully make one appreciate the scarcity of any potential FLT counter-examples.

For each Candidate Pair there is always a conjugate Candidate Pair since every x, has a conjugate a^n - x. Thus the Candidate Pair conjugate to (17, 20) is (323, 326) which shares the residue r = 232.

By Theorem (1.14) we could reject this pair (323, 326) immediately since it has the same, non-Unity Root Gap as (17, 20) and will not therefore meet the Quotient Condition.

The residue r = 232 (above) is conjugate to the residue r = 111, common to (17, 20). However, as x becomes much larger than the base, here x = 323, the quotients are growing rapidly for each increment in x. The quotient p for b = 323 is 98245 and the quotient q for c = 326 is 101008 and so the Quotient Gap is 2763 - nowhere near unity. This emphasizes that even for the smallest of exponents any Candidate Pair must be found near the start of the table.

However, all is not quite lost yet. With a = 7, n = 3. The pair (17, 20) is not the only Candidate Pair with a Root Gap less than the base. In fact, there is always at least two 'Consecutive Identical Residues', see sections (1.11) and (4.2).

The residue r = 309 at x = 120, repeats at x = 121. Thus (120, 121) is a Candidate Pair with a Root Gap of unity. So too is the Conjugate pair (222, 223) whereby 222 = 7^3 - 121 and 223 = 7^3 - 120. However, it is evident that even at x = 120, the Quotient Gap is 127 (= 5164 - 5037). Furthermore, b = 120 is far geater than Bmax which is 18.5, to 1 dp, for a base a = 7, see Example (1.19.3).

This simple example highlights the numerous tests that can be applied to any Candidate Pair. Firstly one has to identify a Candidate Pair (b,c). The Root Gap has to be unity for prime base, i.e. the pair (b,c) must be consecutive (c = b + 1); by the Dual Residue Condition, the pair (a,c) must also be a Candidate Pair (mod b^n). Furthermore, both a and b must be of the 2ln+1 form and b must also be composite. By the Skew Residue Condition, the pair (a,b) must be a Skew Candidate Pair and c must also be of the 2ln+1 form.

We can put an upper bound 'Bmax' (1.19) on the value b, above which the Quotient Gap between consecutive x, i.e. x and x + 1, is always two or greater, i.e. any Candidate Pair cannot meet the Quotient Condition. Hence, if b >= Bmax, the Candidate Pair can be rejected. Similarly, for the Dual Residue table, we can put an upper bound on the value of c (C'max, section (1.20)) for the Candidate Pair (a,c) (mod b^n) such that the absolute value of the quotient, q' is always two or greater.

This concludes our discussion on the repetition of residues (mod a^n) and we now make a quick digression into Conjugate Candidate Pairs. Section (2.5.14) returns to a

short discussion on composite base and Section (2.5.15), following it, discusses the Dual base b. [Note that we shall re-order the sections in a later issue of this work.]

2.5.11 Theorem: Conjugate Candidate Pairs

If (b,c) is a Candidate Pair (mod a^n), then the Conjugate Pair (a^n - c, a^n - b) is also a Candidate Pair (mod a^n).

Proof

By the arithmetic of congruences, the Conjugate Candidate Pair satisifies the following relation

2.5.11.1 $(a^n - b)^n = - b^n \pmod{a^n}$

2.5.11.2 $(a^n - c)^n = - c^n \pmod{a^n}$

But since (b, c) are, by definition, a Candidate Pair then

2.5.11.3 $b^n = c^n \pmod{a^n}$

And so equations (2.5.11.1) and (2.5.11.2) imply that

2.5.11.4 $(a^n - b)^n = (a^n - c)^n \pmod{a^n}$

Hence $(a^n - b)^n$ and $(a^n - c)^n$ are congruent (mod a^n) and are therefore a Candidate Pair (mod a^n).

2.5.12 Theorem: Conjugate Pair Root Gap

The Candidate Pair (b,c) (mod a^n), odd exponent n, has the same Root Gap as the Conjugate Candidate Pair (a^n - c, a^n - b).

Proof

Since b < c by definition then

2.5.12.1 $a^n - c < a^n - b$

and since, by Theorem (2.5.11), a^n - c and a^n - b are a Conjugate Candidate Pair then the Root Gap is, by analogy with (1.10.1), given by

2.5.12.2 Rg = (a^n - b) - (a^n - c)

which reduces to

2.5.12.3 Rg = c - b.

But, by (1.10.1), the Root Gap of the Candidate Pair (b,c) is also (c - b) and hence the Root Gap of a Candidate Pair is the same as that of the Conjugate Pair.

2.5.13 Theorem: Conjugate Pair Bmax

If (b,c) (mod a^n) is a Candidate Pair, odd exponent n, such that b < Bmax, then the Conjugate Candidate Pair (b',c') (mod a^n), where b' = a^n - b and c' = a^n - c, cannot meet the Quotient Condition.

Proof

If b < a^n / 2 then the conjugate value, b' = a^n - b, is such that b' >= a^n / 2. But for all n >=3, if

2.5.13.1 b < Bmax

and, using (1.19.1.5),

2.5.13.2 Bmax < (a^n) / 2

then (2.5.13.1) implies

2.5.13.3 b < (a^n) / 2

The conjugate value b' is defined as

2.5.13.4 b' = (a^n) - b

Using inequality (2.5.13.3) this implies

2.5.13.5 b' > a^n / 2

and, using (2.5.13.2), we have

2.5.13.6 b' > Bmax

Hence if b < Bmax then the conjugate value b' is such that b' > Bmax and therefore, by Theorem (1.19.1), any Conjugate Candidate Pair (b',c') has a Quotient Gap greater than unity.

The practical side of this result is that we need not investigate a Conjugate Candidate Pair (b',c') (mod a^n) if we have rejected the Candidate Pair (b,c) (mod a^n) where b < Bmax. This can be extended for b >= Bmax. Defining the Quotient Gap of the pair (b,c) as Qg, and that of the conjugate pair (b',c') as Qg' then, if b' > c', by the same arguments in the proof of Theorem (1.19.1), Qg' > Qg.

2.5.14 Composite Base

The Remark at the end of Section (1.14) states that we have to consider composite base if we wish to restrict ourselves to unity Quotient Gaps. This is a shame but, if we were to restrict ourselves exclusively to prime a, we would have to widen our investigations to accommodate Quotient Gaps that are a perfect power.

That said, the transition from prime base to composite is minimal. Instead of the base being prime, of form 2ln+1, the only requirement for composite base is that it has one or more prime factors of the form 2ln+1.

Examining a residue table for prime base a, a of the 2ln+1 form, will show each and every residue repeats n times. If we look at a simple composite 2a, then the residue table mod (2a)^n will still have all the original residues (mod a^n), albeit multiplied by 2^n. For example x^n (mod a^n) maps to (2x)^n (mod (2a)^n). Although the residue value changes from r to (2^n)*r, any Repeat Residue y^n (mod a^n), such that x^n = y^n (mod a^n) will still be a Repeat Residue (mod (2a)^n) such that (2x)^n = (2y)^n (mod (2a)^n). In essence, a Candidate Pair (mod a^n) is also a Candidate Pair (mod (2a)^n). That said, even in this simple composite example, Candidate Pairs such as (2x, 2y) (mod (2a)^n) have a common factor '2' giving the triple (2x, 2y, 2a) a common factor of 2, i.e. co-primality in pairs is lost. We would then be better off reverting to studying the residues (mod a^n) where a is the original prime factor. We could, of course, study the prime factor 2^n too. It would be nice to dismiss all composites so easily. However, what we really have to consider, for a composite like 2a are those values of x that are co-prime to 2a, i.e. GCD(x, 2a) = 1. Such co-prime x do have Repeat Residues too when the composite base has a factor of the form 2ln+1. In brief, we needn't have prior stressed primality of the base, merely co-primality between all three member a, b or c, regardless of which one is the base.

However, returning to composites, although no proof is supplied here we can at least reason as per section (2.5.7) why Repeat Residues still occur for x, co-prime to the composite base. Reverting to the simple example of the composite 2a, where a is prime of the form 2ln+1. From what has been said in the prior paragraph, half of the sequence of residues x^n (mod (2a)^n), 0 <= x <2a, (all the even values x) are basically the same as in the (mod a^n) case but multiplied by a factor 2^2. Consequently, if two even values (b,c) repeat (mod a^n), they repeat (mod (2a)^n).

We are not interested in these values because they contain a common factor of 2 shared with the base and therefore any potential FLT counter-example triple (b, c, 2a) is not co-prime in pairs - we may as well revert to studying residues (mod a^n).

The even half of the residue sequence is of size 2ln+1 and so too, not surprisingly, is the odd half x since if a = 2ln+1, then 2a = 2*(2ln + 1) and 0 <= x < 2a. For odd x (not divisible by prime a either), there is a residue r such that x^n = r (mod (2a)^n). This is an nth order Diophantine equation and, for x co-prime to the base, has n solutions. Similarly, there will be a conjugate residue -r with n conjugate solutions -x, where (-x)^n = -r (mod (2a)^n). For each residue r and -r, there are n values for x and n values for -x and we can see that by identical arguments to those used in (2.6.9), we can accommodate, without gaps, an integral number of them in the 2ln+1, odd half of the Residue Sequence, allowing for the zeros, (mod a^n). If the odd half, and therefore also the even half, were not of the 2ln+1 form then there might be n roots for some residues and only say 2 or 3 roots for others. This would leave a rather asymmetric pattern and beg the question, why favour some residues and not others? In fact, it is a case of all or nothing. For an arbitrary value r there are either n solutions x, such that x^n = r (mod (2a)^n), or there are none when r is not an n'th order residue of the modulus. Obviously, not every integer value 0 <= r <2a can have a solution since there simply wouldn't be enough space if any one residue repeated more than once. The only other acceptable scheme occurs if a is NOT of the 2ln+1 form. In which case every x has a unique residue r and vice versa, excepting the zero residues occurring for any x^n divisible by (2a)^n.

2.5.15 Dual Case (mod b^n)

So far most discussion has been on Repeat Residues (mod a) or (mod a^n). However, the same arguments apply equally in the Dual case of Repeat Residues (mod b) or (mod b^n).

Thereom (1.15) asserts that the middle value 'b' of a triple (a, b, c) is always composite and, since the modulus of a Dual Residue Table is b^n, this implies the modulus is consequently composite. From discussions in (2.5.7) and (2.5.14), if there are to be any Repeat Residues a and c such that the Dual Candidate Pair (a,c) (mod b^n) can meet the Quotient Condition, the base b must have a prime factor of 2ln+1 form. However, since a is either prime of the form 2ln+1 or is composite with a prime factor of the form 2ln+1, the 2ln+1 factor cannot be the same for both a and b otherwise they would not be co-prime.

Section (1.20) discusses the upper limit C'max on the value of c in a Dual Candidate Pair (a,c). Notably that this limit, relative to the base b, is much less than that for a standard table where the base is a. This is because in a Dual Residue Table one need not look for a value of c beyond C'max. In a standard Residue table, (mod a^n), the value of Bmax, which is an upper limit on the middle value b, is many times greater than the base a, see Theorem (1.19.1). Nevertheless, the value of c is the same in each Candidate Pair (a,c) and (b,c) and so the absolute search range for Repeat Residues is the same in both Standard and Dual residue tables.

2.6 Summary of Conditions

This section is a summary of all the conditions and constraints developed in this section and placed upon a triplet (a, b, c) were it to be an FLT counter-example.

For integers x and k

2.6.1 $x >= 1$

2.6.2 $k >= 1$

the value a is either prime ($x = 1$) or composite ($x > 1$) with one or more factors of the form $(2kn + 1)$, i.e.

2.6.3 $a = x(2kn + 1)$

For integers y and l

2.6.4 $y >= 2$

2.6.5 $l >= 1$

the value b always composite with one or more prime factors of the form $2ln+1$, i.e.

2.6.6 $b = y(2ln + 1)$

For integers z and m

2.6.7 $z >= 1$

2.6.8 $m >= 1$

the value c is either prime ($z = 1$) or composite ($z > 1$) with one or more factors of the form $(2mn+1)$, i.e.

2.6.9 $c = z(2mn + 1)$

The Skew Residue Condition (2.5.1.18), Candidate Pair (a,b) (mod c^n)

2.6.10 b^n = -a^n (mod c^n)

3 Unity Roots

Sections (1) and (2) focussed on the study of Residue Sequences x^n (mod a^n), 0 <= x < a^n, in the pursuit of Candidate Pairs (b,c) where b^n = c^n (mod a^n) or Dual Candidate Pairs (a,c) where a^n = c^n (mod b^n), which could possible meet the Root Gap constraint (c - b < a) imposed by Theorem (1.12). Of principal study in the previous section was how residues repeat within a sequence. For even exponents the repetition was attributed to symmetry and, for odd exponents, the repetition was attributed to the '2ln + 1' mechanism. Perhaps unsurprisingly, by Lagrange's Theorem (2.2.5.3), both mechanisms are shown in this section to be unified by the concept of Unity Roots u, where u^n = 1 (mod a^n) or (mod b^n). In particular, Candidate Pairs can be generated through a mapping mechanism c = u*b (mod a^n).

The pursuit of Unity Roots (mod a^n) also leads to Unity Roots (mod a) and the study of the Unity Root Polynomial, exponent n, denoted by 'f(u)n', which is a cyclotomic polynomial with many of its own interesting properties. These properties are explored in this section as a digression from the main theme of this Paper. In particular, the factor properties of f(u)n and applications in such areas as Mersenne Numbers.

Although analytically unsolved, we present an algorithm to obtain Unity Roots (mod a^n), given the roots (mod a). We also detail how to obtain Unity Roots for composites given those of its prime factors.

Of key note in this paper is the observation that the even exponent symmetry, which we used to generate Pythagorean triples in section (2.4.4), can be viewed as a negative Unity Root mapping and therefore a 'flip' about the symmetry point.

Lastly, as for all previous sections, we summarise all the latest constraints upon any potential FLT counter-examples that have arisen in this section.

3.1 Definition: Unity Root

A Unity Root is defined as an integer u, u > 0, such that for all a > 0, n > 0

3.1.1 u^n = 1 (mod a^n)

Obviously u = 1 is a Unity Root for all a and n and is termed the 'trivial root'. Normally we are more interested in the non-trivial roots, u > 1.

3.2 Introduction

As mentioned prior in section (2.6), but without any explanation, Unity Roots are fundamental to the repetition of all residues.

Section (2) split the analysis of the FLT equation (1.1.1) into two distinct cases whereby the exponent was either odd or even. For the even case this was primarily Pythagoras. The Pythagorean case makes a good example since it does have solutions, i.e. Pythagorean Triples, in which to test the Residue and Quotient Conditions and advance the work further. Nevertheless, Repeat Residues in both the two cases, even and odd exponents (2.4) and (2.5), can be unified under one scheme, namely 'Unity Root Mappings'.

3.2.1 For odd prime exponent n, prime base a, modulus a^n, the set U of Unity Roots may comprise either a single Unity Root (+1) or n roots. For composite base a, the number of Unity Roots is an integral power s of n, i.e. n^s where s is the number of prime factors with n Unity Roots. This holds for all s >= 0..

3.2.2 For even exponent n, arbitrary base a, there may either be two Unity Roots U = {+1, -1} or the number of Unity Roots is a multiple of 2. The exact number depends upon the composition of the base a. The only case or real interest herein is Pythagoras for which the number of roots is discussed in section (3.5). The main point to note is that, unlike odd exponent, there are always at least two Unity Roots for n = 2, arbitrary base and that the -1 root, not always present for arbitrary odd exponent, is the key to all the repeat residues. See section (3.4) on Unity Root Mappings and (3.9) on such mappings and Pythagoras.

3.2.3 A set of n Unity Root's is denoted by upper case U where U = {u_0, u_1, u_2, ... u_(n-1) }, u_0 is the trivial root +1 and u_1 is the smallest non-trivial root, usually shortened to the single letter ‘u’.

3.3 Properties

3.3.1 The n Unity Roots are cyclic. Thus, all roots can be generated from the primitve Unity Root u, i.e. u is a generator.

u_0 = u^0 = 1
u_1 = u^1 = u
u_2 = u^2
.
.
u_k = u^k
.
.
u_(n-1) = u^(n - 1)

3.3.2 The Unity Roots form an n'th order cyclic group under multiplication, modulo a^n. The n'th roots of unity, which are generally complex, also form a cyclic group of order n and, consequently, the two groups are isomorphic.

This is as near as this paper gets to complex numbers from where most work in Diophantine equations usually proceeds onward to the algebraic extension of the rationals to complex numbers.

Because of this isomorphism there are analogues between the work presented here and that of algebraic number theory. In particular, the Unity Root Polynomial 'f(u)n', which is discussed extensively in section (3.6) of this paper is, for prime exponent n, more generally known as a 'Cyclotomic Polynomial'. Secondly, polynomial factorisation into complex n'th roots of unity also has an analogue in congruential arithmetic, section (4.1).

3.3.3 The smallest non-unity, 'primitive' Unity Root is designated 'u', or 'u_1'. This is a generator of the cyclic group and, unless otherwise stated, when we refer to a Unity Root u we mean this smallest root u_1.

3.3.4 With u as the generator the complete set of Unity Roots is

3.3.4.1 $U = \{u^0, u^1, u^2, \ldots u^{(n - 1)} \}$

with the first two cases written simply as

3.3.4.2 $u^0 = 1$

3.3.4.3 $u^1 = u$

then the set (3.3.4.1) becomes

3.3.4.4 $U = \{1, u, u^2, \ldots u^{(n - 1)} \}$

3.3.5 Theorem: Unity Root > Base

The non-trivial, Unity Root u is always greater than the base a

Proof

A Unity Root is defined as a solution to the congruence

3.3.5.1 u^n - 1 = 0 (mod a^n)

which implies that, for some integer k

3.3.5.2 u^n - 1 = k*a^n

and re-arranging this we get

3.3.5.3 u^n = 1 + k*a^n

Since u > 1 for the generator root, we see that (3.3.5.3) implies

3.3.5.4 u^n > k*a^n

The value of k cannot be zero since this would imply u = 0. So, for positive u,

3.3.5.5 k >= 1

which implies

3.3.5.6 k*a^n >= a^n

and inequality (3.3.5.4) becomes

3.3.5.7 u^n > a^n

Taking n'th roots, we see that

3.3.5.8 u > a

and hence the smallest integer value u can take is (a + 1) and we conclude that the Unity Root is always greater than the base.

3.4 Unity Root Mappings

Taking the defining equation for a Unity Root (3.1.1) and multiplying throughout by b^n, where b is an arbitrary integer, 1 < b < a^n

3.4.1 u^n*b^n = b^n (mod a^n)

If we define a second integer c

3.4.2 $c = u*b \pmod{a^n}$

then we see that (3.4.1) can be written in terms of c as follows

3.4.3 $c^n = b^n \pmod{a^n}$

But this result shows that c^n and b^n are congruent (mod a^n), hence they have identical residues (mod a^n) and thus form a Candidate Pair (b,c), i.e. c is a repeat residue of b when defined by (3.4.2).

Alternatively expressed, we say that 'c is a Unity Root mapping of b (mod a^n)', i.e. b maps to c under the Unity Root u (mod a^n).

If there was only the single Unity Root, u = 1, c would actually be identical to b and the result would be trivial. However, for certain base and exponent, as prior stated in (2.2.5), there can be n or more Unity Roots. Thus, if there are at least n Unity Roots, u_k, $0 <= k < n$, there are at least n repeat residues of $b^n \pmod{a^n}$ at location $c = u_k*b$, in accordance with (3.4.2). Since b is arbitrary, if we know all the Unity Roots, we can obtain all the repeat residues for any value b. The problem of finding Candidate Pairs (b,c), where c is defined by (3.4.2), is really just one of finding the Unity Roots $x^n \pmod{a^n}$. Furthermore, these conclusions were made with no reference to a specific form of the exponent n, it can be odd or even. We therefore have a unified approach to finding Candidate Pairs (b,c) (mod a^n) or their Dual counter-part pairs (a,c) (mod b^n) by determination of the Unity Roots for the modulus, a^n or b^n respectively.

The problem seemingly becomes a lot simpler. It certainly is a lot simpler in that, with a unified approach, we only have to identify the Unity Roots to generate Candidate Pairs instead of visual inspection of a residue tables search for values with identical residues. Better still, because the Unity Roots form a cyclic group, we only need to find one of them in order to be able to generate all n. In other words, a single Unity Root (mod a^n), will allow us to determine the repetition of every residue (mod a^n) known to occur. What we cannot do, however, is determine the initial set of residues, we can only determine their repeat occurences. Whilst it would seem that determination of a single Unity Root will unlock the secrets of Repeat Residues and Candidate Pairs, the determination of Unity Roots is not trivial and, currently, we have no analytic solution for an arbitrary exponent. Fortunately, an algorithmic method to find the roots does exist and is detailed in section (3.7.3)

Since FLT is true, we can see that there must be one or more properties of the Unity Roots that constrain the value of c in (3.4.2) such that the Candidate Pair (b,c) can never satisfy the Quotient Condition. The reality is that, whatever the value for u, it always generates a value c such that either the Root Gap (1.10.1) is greater than a or, when the Root Gap is smaller than a, e.g. for Consecutive Identical Residues, the value of c is still beyond Bmax+1, Section (1.19), Theorem (1.19.1) and consequently the Quotient Gap is larger than unity. Ultimately, by studying Unity

Roots, we might be able to gain insight into why Candidate Pairs never meet the Quotient Condition and why there are no FLT counter-examples, i.e. why FLT holds true.

Although for general exponents, n > 2, we currently have no consistent explanation for Unity Root values, we do nevertheless have one, non-trival case (n != 1) to examine, namely Pythagoras. This does have solutions and it does have Unity Roots. It is discussed again in section (3.9).

3.4.4 Definition: Winding Number

By definition (3.4.2), the Unity Root mapping of b on to c, (mod a^n), produces a value c such that

3.4.4.1 $c = u*b \pmod{a^n}$

which implies for some integer w, w >= 0, termed the 'Winding Number'

3.4.4.2 $u*b = w*a^n + c$

If w = 0 we term it the Zero Winding Number and, if w > 0, we term it a non-Zero Winding Number. We shall see that if the Candidate Pair (b,c) has a Zero Winding number it cannot be an FLT counter-example.

3.4.5 Definition: Wrapover

If the Winding Number w, defined by (3.4.4.2), has a value greater than zero then the mapping (3.4.4.1) is said to 'Wrapover'.

The winding number is effectively the same as a quotient and generally it is the context that differentiates their usage. The term 'quotient' is used when talking about any arbitrary value x^n written in quotient, remainder form, e.g. x^n = q*a^n + r, where q is the quotient and r is the remainder. Winding number is currently used exclusively for Unity Root mappings defined by the integer w in (3.4.4.2).

3.4.6 Theorem: Winding Number & Root Gap

A Candidate pair (b,c) (mod a^n) cannot be an FLT Counter-example if the Unity Root mapping of b on to c has a zero Winding Number.

Alternatively stated, if the Unity Root mapping of b on to c, (mod a^n), produces a value c = u*b less than the modulus a^n, i.e. c a^n and has a Zero Winding Number (3.4.4), then the Root Gap is always such that Rg >= a^2 and hence, by Theorem (1.12), the Quotient Condition can never be met.

Proof

Using (3.4.2) for the value c in the Candidate Pair (b,c), the Root Gap (1.10.1) is given by

3.4.6.1 $Rg = u*b \pmod{a^n} - b$

If the value of u and b is such that the product u*b is less than the modulus, i.e. zero winding, then

3.4.6.2 $u*b < a^n$

and the Root Gap expression (3.4.6.1) becomes

3.4.6.3 $Rg = (u - 1)*b$

Now, by Theorem (3.3.5), the Unity Root is greater than the base a, which for integers implies

3.4.6.4 $u >= a + 1$

hence

3.4.6.5 $u - 1 >= a$

and, multiplying throughout by b, we get

3.4.6.6 $(u - 1)*b >= a*b$

Therefore, by comparison with (3.4.6.1), we can see that for a zero Winding Number the Root Gap satisfies the following inequality:

3.4.6.7 $Rg >= a*b$

Since, by convention, b is chosen such that

3.4.6.8 $b > a$

then we see that the Root Gap satisifies the inequality

3.4.6.9 Rg >= a^2

And hence is is greater than the base a. Consequently, by Theorem (1.12), the Quotient Condition can never be met.

To drive the point home, we can also say that a Candidate Pair must wrapover to be a potential FLT counter-example, i.e. it must have a non-zero Winding Number, w > 0 in (3.4.4.2).

3.5 Counting Unity Roots

For completely arbitrary exponent and base the number of Unity Roots can be numerous and even multiples of the exponent. Nevertheless, we are primarily interested only in odd, prime exponents and the singular, even prime exponent case n = 2, for which the rules are relatively simple for either prime or composite base. Unity Roots for composite base a can be determined from the prime factors and it is therefore the determination of Unity Roots for primes that is the real issue and difficulty.

3.5.1 If n is an odd prime, a is prime and not of the 2ln + 1 form and n != a, then there is one Unity Root in the interval [0, a^n) and that is u = +1.

3.5.1.1 Examples

n = 3, a = 2, U = {1}
n = 3, a = 5, U = {1}
n = 3, a = 11, U = {1}

3.5.2 If n is odd, prime, a is prime of the 2ln + 1 form, then there are n Unity Roots, u_0, u_1, u_2, ..u_(n-1) in the interval [0, a^n).

3.5.2.1 Examples

n = 3, a = 7, U = {1,18,324}

n = 3, a = 13, U = {1,1036,1160}

n = 5, a = 11, U = {1, 37101, 46709, 104450, 133835}

n = 5, a = 31, U = {1, 13801549, 13979094, 15561847, 28629152}

3.5.3 If n is odd, prime and n = a, there are n Unity Roots, u_0, u_1, u_2, ..u_(n-1) in the interval [0, a^n) but there is only one Unity Root in the Minimal Residue Sequence [0, a^(n - 1)), since n | a, see section (2.1.2.2). Of course, if n = a, then a cannot be of the 2ln + 1 form.

3.5.3.1 Examples

n = 3, a = 3, U = {1, 10, 19}

Here the Minimal Residue Sequence size is 3^3 / 3= 9 and the second root, u = 10, is actually = 1 + 1*3^2, similarly, 19 = 1 + 2*3^2.

n = 5, a = 5, U = {1, 626, 1251, 1876, 2501}

Here the Minimal Residue Sequence is of size 5^5 / 5 = 625 and the roots can be written in terms of multiples of this value as follows:

626 = 1 + 1*625
1251 = 1 + 2*625
1876 = 1 + 3*625
2501 = 1 + 5*625

3.5.4 If n is an odd prime and a is composite with one or more factors of the 2ln + 1 form then there are n Unity Roots for each prime factor of form 2ln + 1 in the interval [0, a^n) or in the interval [0, a^(n - 1)) according as to whether n !| a or n | a respectively.

3.5.4.1 n = 3, a = 14, U = {1,361, 1353}

Here a = 14 has the two factors 2 and 7, only the factor 7 is of the 2ln + 1 form and so there are three roots

3.5.4.2 n = 3, a = 21, U = {1,361, 667}

Here a = 21 has only two unique factors, the factor 7 is of the form 2ln + 1, the other factor is 3 and since n divides the factor there are 3 Unity Roots for the factor 7 within the interval [0, 21^3 / 3).

In the Maximal interval, 21^3, within which the residue sequence for 0 <= x < 21^3 / 3 repeats three times, there are, as expected, repeats of these Unity Roots at

U = {3088, 3448, 3754, 6175, 6535, 6841}

Since the exponent divides the base, with a Minimal Residue Sequence size of 21^3 / 3 = 3087, the repeated roots can be expressed as

U = {1+3087, 361+3087, 667+3087,
1 + 2*3087, 361 + 2*3087, 67 + 2*3087}.

3.5.4.3 n = 3, a = 49, U = {1, 34967, 82681}

Here a = 49 has only one unique factor, of the 2ln + 1 form, i.e. 7, and so there are only three roots.

3.5.4.4 n = 3, a = 91

U = {1, 9948, 59320, 69267, 244903, 304222, 439401, 449348, 684303}

Here a comprises two unique factors 7 and 13, each of the form 2ln + 1, hence there are 9 (= 3*3) Unity Roots in the Maximal Residue Sequence of size 91^3.

3.5.5 If n is an odd prime and a is composite, with no prime factors of the 2ln + 1 form then there is one Unity Root, U = {+1}, in the interval [0, a^n) if n !| a or one Unity Root, U = {+1} in the interval [0, a^(n - 1)) if n | a.

3.5.5.1 Examples

n !| a

3.5.5.2 n = 3, a = 4, U = {1}

3.5.5.3 n = 3, a = 8, U = {1}

3.5.5.4 n = 3, a = 10, U = {1}

3.5.5.5 n = 3, a = 16, U = {1}

3.5.5.6 n = 3, a = 20, U = {1}

n | a

3.5.5.7 n = 3, a = 3, U = {1}

3.5.5.8 n = 3, a = 9, U = {1}

3.5.5.9 n = 3, a = 15, U = {1}

3.5.6 If n = 2 and a is an odd prime then there are two and only two Unity Roots U = {+1, -1} within the interval [0, a^n).

3.5.6.1 Examples

3.5.6.2 n = 2, a = 3, U = {1, 8}

3.5.6.3 n = 2, a = 5, U = {1, 25}

3.5.6.4 n = 2, a = 7, U = {1, 48}

3.5.7 If n = 2 and a is an odd composite then there are two Unity Roots per odd, unique prime factor within the interval [0, a^n).

3.5.7.1 Examples

3.5.7.2 n = 2, a = 9, U = {1, 80}

3.5.7.3 n = 2, a = 15, U = {1, 26, 199, 224}

3.5.7.4 n = 2, a = 21, U = {1, 197, 244, 440}

3.5.7.5 n = 2, a = 25, U = {1, 624}

3.5.7.6 n = 2, a = 105, U = {1, 1126, 1324, 2449, 8576, 9701, 9899, 11025}

Here a factors into 3, 5 and 7 and each factor has two Unity Roots so there are 8 Unity Roots in total.

3.5.8 If n = 2 and a is even then n | a and so the Minimal Residue Sequence is half of the Maximal, namely a^2 / 2. Within this interval the number of roots is dependant upon the composition of a. For each unique, prime factor of a / 2, there are two roots.

The specific case n = 2, a = 2 is slightly anomalous: since n = 2 and a is even, a / 2 = 1 and there is only one root in the interval 0 < u < 2^2 / 2, namely u = {+1}. In this case the root u = 1 is equivalent to the u = -1 root and there is only a single root in the Minimal Residue Sequence. Nevertheless, in the Maximal Sequence 0 < u < a^2, there are two unique roots +1 and +3 (3 = -1 mod 2^2). This is the only case where a is even but only has one root in the interval 0 < u < 2^2 / 2. Since we know Pythagoras has no solutions for a <= 2 it is of no consequence.

3.5.8.1 Examples

3.5.8.2 n = 2, a = 4, U = {1, 7}

Here a / 2 has one,unique prime factor 2 hence there are only two Unity Roots within the interval [0, 4^2 / 2).

3.5.8.3 n = 2, a = 6, U = {1, 17}

Here a / 2 has one, unique prime factor 3 hence there are only two Unity Roots within the interval [0, 6^2 / 2).

3.5.8.4 n = 2, a = 8, U = {1, 31}

Here a / 2 has one, unique prime factor 2 hence there are only two Unity Roots within the interval [0, 8^2 / 2).

3.5.8.5 n = 2, a = 10, u = {1, 49}

Here a / 2 has one, unique prime factor 5 hence there are only two Unity Roots within the interval [0, 10^2 / 2).

3.5.8.6 n = 2, a = 12, U = {1, 17, 55, 71}

Here a / 2 has two, unique prime factors 2 and 3 hence there are four Unity Roots. In fact, this is the smallest value for a to have 4 roots in the Minimal Residue Sequence, [0, 12^2 / 2).

3.5.8.7 n = 2, a = 14, U = {1, 97}

Here a / 2 has one, unique prime factor 7 hence there are only two Unity Roots within the interval [0, 14^2 / 2).

3.5.8.8 n = 2, a = 16, U = {1, 127}

Here a / 2 has one, unique prime factor 2 hence there are only two Unity Roots within the interval [0, 16^2 / 2).

3.5.8.9 n = 2, a = 18, U = {1, 161}

Here a / 2 has one unique, prime factor 3 hence there are only two Unity Roots within the interval [0,18^2 / 2).

3.5.8.10 n = 2, a = 60, U = {1, 199, 449, 649, 1151, 1351, 1601, 1799}

Here a / 2 has three, unique prime factors 2, 3 and 5 hence there are eight Unity Roots within the interval [0, 60^2 / 2). In fact, this is the smallest value for a to have 8 roots in the Minimal Residue Sequence. To get 16 roots, we have to go as far as a = 420, since a / 2 factors into the four prime factors 2, 3, 5 and 7.

3.6 The Unity Root Polynomial

Returning to the defining equation for a Unity Root (3.1.1), we can re-arrange it to become a problem in the determination of zero roots for the congruence

3.6.1 u^n - 1 = 0 (mod a^n)

This is the modular arithmetic analogue of the algebraic polynomial equation

3.6.2 u^n - 1 = 0

It is no surprise that both equations have the single root u = 1 and we can factor the left-hand side of the expressions as follows

3.6.3 u^n - 1 = (u - 1)(1 + u + u^2 + .. u^(n - 1))

3.6.4 Definition: Unity Root Polynomial

The 'Unity Root Polynomial', exponent n, denoted by f(u)n, is defined as

f(u)n = (1 + u + u^2 + .. u^(n - 1))

[Note that f(u)n is the sum of a geometric progression with n terms, the first term is 1 and the common ratio is u. We sometimes drop the suffix ‘n’ leaving just f(u) when it is obvious as to its usage, i.e. when the exponent is obviously n].

Factoring (3.6.1) as per (3.6.3) and substituting for the Unity Root Polynomial f(u)n, as defined by (3.6.4), we get

3.6.5 (u - 1)*f(u)n = 0 (mod a^n)

At this stage we could solve the congruence for each separate bracket.

3.6.6 (u - 1) = 0 (mod a^n)

3.6.7 f(u)n = 0 (mod a^n)

Or we can solve the combined congruence (3.6.5) assuming neither bracket is congruent to zero (mod a^n). This situation has no analogue in the solution of polynomials f(x). It is possible in modulo arithmetic to have solutions to the following congruence equation where neither A nor B is zero but the product is congruent to zero (mod C).

3.6.8 A*B = 0 (mod C)

For now, we will remain with the solutions to (3.6.6) and (3.6.7). Examination of the case (3.6.8) is (TBD).

With u = 1 as the primitive solution to (3.6.6), the remaining (n - 1) solutions are given by solving the following equation, for prime a (see further below),

3.6.9 f(u)n = 0 (mod a^n)

This equation is a Diophantine equation of order (n -1) which, as prior mentioned, doesn't always have integer solutions. In fact, from section (2.5.7), only if a is of form 2ln + 1 or composite with one or more factors of the 2ln + 1 form does (3.6.9) have integer solutions.

Note that if we treat f(u)n as a standard polynomial then its roots are the n'th roots of unity, excepting u = 1 which has been factored out. In this case, the polynomial always has n - 1 roots in the complex field.

Returning to equation (3.6.5). For some integer l, l >= 0, this equation can be written as

3.6.10 (u - 1)*f(u)n = l*a^n

If (u - 1) and a are co-prime, then (u - 1) | l which implies that, for some integer m m > 0,

3.6.11 (u - 1) = m * l

and, for some integer s, s > 0,

3.6.12 f(u)n = s*a^n

3.6.13 Theorem

With f(u)n defined by (3.6.4) then u is a Unity Root (mod f(u)) and u is a Unity Root (mod (u - 1)).

Proof

By (3.6.3)

3.6.13.1 u^n - 1 = (u - 1)*f(u)n

and, taking residues (mod f(u)n),

3.6.13.2 u^n - 1 = 0 (mod f(u)n)

which can be alternatively expressed as

3.6.13.3 u^n = 1 (mod f(u)n)

and hence u is a Unity Root (mod f(u)n).

Similarly, by taking residues (mod (u - 1)),

3.6.13.4 u^n - 1 = 0 (mod (u - 1))

alternatively expressed

3.6.13.5 u^n = 1 (mod (u - 1))

and hence u^n is a Unity Root (mod (u - 1)).

3.6.14 Theorem: Unity Root Sum = 0 (mod a^n)

The sum of the Unity Roots for prime base a is congruent to zero (mod a^n).

This is the modulo arithmetic analogue to the summation of the n'th roots of unity, which always sums to zero.

Proof

Considering the positive, Unity Roots, 0 < u < a^n, modulus a^n, then, using (3.3.4.4), if we sum these roots we get

3.6.14.1 Sum(U) = 1 + u + u^2 + ... u^(n - 1)

But by (3.6.4) we see that the rhs of this sum is identical to the Unity Root Polynomial f(u)n, i.e.

3.6.14.2 Sum(u) = f(u)n

Hence, by (3.6.7)

3.6.14.3 Sum(u) = 0 (mod a^n)

and we see the sum of the Unity Roots, (mod a^n), is congruent to zero (mod a^n).

Notes

Since all roots u are such that 0 < u < a^n, equation (3.6.14.3) implies that for some integer k, k > 0

3.6.14.4 Sum(u) = k*a^n

For the n = 3 case we can be more specific and deduce that k = 1 in (3.6.14.4) if we keep with positive roots, by convention (0.3.5.5), i.e.

3.6.14.5 Sum(u) = a^3

Writing the sum out in full

3.6.14.6 1 + u + u^2 = a^3

We know that there are three roots, one of which is 1. For certain a, the other two are unique. The very largest they can be, when all positive, are a^3 - 2 and a^3 - 1 within the range 0 < u < a^3. If we sum all three we get 2*a^3 - 2 and therefore, by (3.6.14.4), k has to be 1 since the largest sum is still 2 short of 2*a^3.

If we express some Unity Roots in the positive form and others in the negative form then we can get k = 0 and we then have an identical, analogous result to summing the n'th roots of unity, which sum to zero. In the case of a cubic, where we have to solve a quadratic to get the roots, see example (3.6.10) below, we automatically get one positive and one negative solution, see (3.6.10.11) and (3.6.10.12) which, together with the root u = 1, sum directly to zero.

Since the left-hand side of (3.6.14.6) is f(u)3, we can substitute back for f(u)3 into (3.6.10) to give

3.6.14.7 (u - 1)*a^3 = l*a^3

which, upon cancelling a^n from both sides, implies

3.6.14.8 (u - 1) = l

We see from this that the value of the factor l for a cubic exponent, prime base a, is in fact one less than the Unity Root.

3.6.15 Conjecture: Umin

The smallest, non trivial value of a Unity Root, Umin, is conjectured as satisfying the inequality

3.6.15.1 Umin > (n - 1)_/(a^n - 1) (the term '(n - 1)_/' denotes the n-1'th root)

This is a conjecture and not a rigorously proved theorem since a proper analytic study of the error term has not been performed but taken from a reasonable estimate, verified by computer.

Reasoning

Considering only positive, primitive Unity Roots, 0 < u < a^n, modulus a^n.

Using the sum of the roots, sum(u) as defined in (3.6.14.1), equation (3.6.14.4), for some integer k, k > 0, gives

3.6.15.2 1 + u + u^2 + .. u^(n - 1) = k*a^n

Since we are considering only positive, primitive Unity Roots, 0 < u < a^n, the smallest value for integer k is 1 so we can place the following inequality on the lhs sum(u) as follows

3.6.15.3 1 + u + u^2 + .. u^(n - 1) >= a^n

For n > 2, u > 2, the largest term in the sum on the lhs will be u^(n - 1) and, for increasing a, since u > a by (3.3.5), this term will becomes more dominant as a increases. Therefore a first approximation to u, which is an over-estimate, can be obtained by neglecting the first n - 1 terms on the lhs to leave

3.6.15.4 u^(n - 1) ~=~ >= a^n (the '~=~' term denotes approximately)

The approximation is actually good for the numbers of interest. The smallest value of a is 7 and the smallest exponent is 3. In this case, approximating u by the square root of 7 gives u = 18.5 to 1dp. The actual value of u is 18.

If we denote the over-estimated error by e, the inequality can be re-written

3.6.15.5 u^(n - 1) >= a^n - e

As n and u become larger the approximation gets better, i.e. the over-estimated error term e becomes smaller. In fact it can be shown that the error is approximately given by

3.6.15.6 e ~=~ 1 / (n - 1)

For example, for n = 3, the error is approximately 1 / 2 and the error decreases as n grows larger. This is actually a very good approximation of the error and computer analysis reveals it is always less than 0.5203 for the worst case of n = 3. Thus, by giving the maximum error of 1, we can conjecture that the minimum Unity Root value 'Umin' is given by the expression

3.6.15.7 Umin = (n - 1)_/(a^n - 1)

As a consequence of this conjecture, it can also be shown that Umin > Bmax (see (1.19) for Bmax) and so two Unity Roots can never form an FLT counter-example since the minimum Unity Root exceeds the maximum permitted value of b in a candidate Pair (b,c).

Lastly, a computer analysis of Umin and the error term for various u and n verifies these findings at least for small base and exponent.

3.6.16 f(u) Factor properties

The factor properties of the unity Root Polynomial f(u)n are quite extensive and allow us to say many things about the type and number of factors of f(u)n.

It has been prior mentioned that, for prime exponent n, f(u)n is what is known in the subject of Number Theory as a 'Cyclotomic Polynomial', reference Mathworld [4], keword 'Cyclotomic Polynomial'. Some of the Properties of f(u)n presented here may have analogous properties in the subject of Cyclotomic Polynomials, albeit a rigorous cross check has not been performed.

3.6.16.1 If f(u)n is prime then it is of the form 2ln + 1 if u > 1.

Since, by Theorem (3.6.13), u is a Unity Root (mod f(u)n) and, since u != 1 + k*f(u), integer k, k >= 0 then, by the arguments in sections (2.5.7) and (2.5.9), f(u)n must be of the 2ln + 1 form since it has a Unity Root other than the trivial u = +1. Note that since f(u)n is prime, by definition, then n !| f(u) unless n = f(u) and n is prime. However, it is not possible that n = f(u)n simply by the construction of f(u) except if u = 1. If u = 1, then f(u) = n see property (3.6.16.4) and this Unity Root is always present for any base a (= n = f(u)n), not just those of the 2ln + 1 form. Hence the caveat on the u = 1 case.

3.6.16.2 If f(u)n is composite and u is not of the form 1 + k*n (see below) then every factor is of the form 2ln + 1

The reason we put in the caveat 'not of the form 1 + k*n' is because, as we shall see, there can be one other legitimate factor equal to the exponent n, at locations 1 + k*n. This arises by consideration of the next two properties.

Suppose f(u)n factors into two prime factors k and m

3.6.16.2.1 f(u)n = k*m

then by (3.7.5.1)

3.6.16.2.2 u^n = 1 (mod k*m)

and thus

3.6.16.2.3 u^n = 1 (mod k)

and

3.6.16.2.4 u^n = 1 (mod m)

That is, we see that if u is a Unity Root for composite base f(u)n, then it is also a Unity Root u^n of the prime factors k and m of f(u)n. If u is not of the form 1 + k*n, then u is a non-unity, Unity Root of the primes k and m. But by property (3.6.16.1) we see that with primes k and m as base in (3.6.16.2.3) and (3.6.16.2.4), they must therefore also be of the form 2ln + 1. This argument can be extended for when f(u)n is composite with any number of prime factors and thus every one of the prime factors must also be of the form 2ln + 1 if u is not of the form 1 + k*n

3.6.16.3 If P is a prime factor of f(u)n, i.e. P | f(u)n, then at a point u', where u' = u + k*P, for some integer k, k > 0, then a | f(u')n.

For example, if n = 3, u = 3, then f(3)3 = 13. Let P = 13, i.e. the one and only prime factor of 13, then at any point 3 + k*13, then 13 | f(3 + k*13)3. If k = 1, u' = 16 and, indeed, we see f(16)3 = 273 which factors as 3*7*13.

Proof of this comes from the general property of a polynomial f(x), degree n, with rational coefficients c0, c1, .. cn as given by,

3.6.16.3.1 $f(x) = c0 + c1*x + c2*x^2 + .. cn*x^n$

such that if, for some value x = u, arbitrary modulus A,

3.6.16.3.2 $f(u) = r \pmod A$

then, for some integer k, k >= 0

3.6.16.3.3 $f(u + k*A) = r \pmod A$

This is proven by showing that it is true for each term in (3.6.16.3.1), e.g. for the general term l.

If

3.6.16.3.4 $cl*u^l = r \pmod A$

then

3.6.16.3.5 $cl*(u + k*A)^l = r \pmod A$

If we expand the term $(u + k*A)^l$ by the binomial theorem we will see that all terms have a factor of A and hence are congruent to 0 (mod a). This leaves only the single term u^n, hence

3.6.16.3.6 $cl*(u + k*A)^l = cl*u^l \pmod A$

and, by comparison with (3.6.16.3.4),

3.6.16.3.7 $cl*(u + k*A)^l = r \pmod a$

3.6.16.4 The value of f(u)n for u = 1 is always n since, by the definition of f(u)n (3.6.4), it is simply a series sum of n terms where each term is unity when u = 1. Hence the total sum is n, i.e. f(1)n = n for all exponent n.

This property shows us that f(1) is always divisible by the exponent and hence n | f(1). In addition, property (3.6.16.3) shows that if n | f(1)n, then n | f(1 + k*n)n for all integer k, k >= 0. We can thus arrive at the following factor property.

3.6.16.5 If f(u)n is composite and u is of the form 1 + k*n, then every factor is either of the form n or 2ln + 1.

Proof (TBD)

3.6.16.6 Any factor of f(u) of the form 2ln + 1 appears n times within the region 0 <= x < u.

Proof (TBD)

3.6.16.7 Any factor of f(u) of the form n appears once and only once within the region 0 <= x < u.

Proof (TBD)

3.6.16.8 The value of f(u) is composite for any u if the exponent is even.

Let the exponent n be even, of the form

3.6.16.8.1 n = 2m

then, by the definition of f(u), equation (3.6.4)

3.6.16.8.2 u^(2m) - 1 = (u - 1)*f(u)2m

the left-hand side factors as

3.6.16.8.3 u^(2m) - 1 = (u^m - 1)*(u^m + 1)

and we can factor the term (u^m - 1) as

3.6.16.8.4 u^m - 1 = (u - 1)*f(u)m

Substituting for (u^m - 1) from (3.6.16.8.4) into (3.6.16.8.3) gives

3.6.16.8.5 u^(2m) - 1 = (u - 1)*f(u)m*(u^m + 1)

Equating (3.6.16.8.2) and (3.6.16.8.5) we get

3.6.16.8.6 (u - 1)*f(u)m*(u^m + 1) = (u - 1)*f(u)2m

Upon cancelling the (u - 1) term this leaves us with the relation

3.6.16.8.7 f(u)m*(u^m + 1) = f(u)2m

which shows us that f(u)2m factors into two terms f(u)m and (u^m + 1) hence, for any even exponent, the value of f(u) is composite.

With regard to primality of f(u)n, this property (3.6.16.8) disposes of all even composite exponents. The next property eliminates odd composite exponents.

3.6.16.9 The value of f(u) is composite for any u if the exponent is odd composite.

Suppose the exponent n is composite with two odd, prime factors k and m, i.e.

3.6.16.9.1 n = km

Let u be any arbitrary value then, by the definition of f(u)km

3.6.16.9.2 u^(km) = 1 (mod f(u)km)

which implies that

3.6.16.9.3 u^(km) - 1 = (u - 1)*f(u)km

But since u^(km) can also be written as either

3.6.16.9.4 u^(km) = (u^k)^m

or

3.6.16.9.5 u^(km) = (u^m)^k

then u^k is also an m'th Unity Root of f(u)m, and u^m is also a k'th Unity Root of f(u)k such that

3.6.16.9.6 (u^k)^m = 1 (mod f(u)m)

and

3.6.16.9.7 (u^m)^k = 1 (mod f(u)k)

Substituting u^k for u in equation (3.6.16.8.4) gives

3.6.16.9.8 (u^k)^m - 1 = (u^k - 1)*f(u^k)m

Swapping the label m for k in (3.6.16.8.4) and substituting the term u^m for u in the same equation gives

3.6.16.9.9 (u^m)^k - 1 = (u^m - 1)*f(u^m)k

All three equations (3.6.16.9.8), (3.6.16.9.9) and (3.6.16.9.3) have identical left hand sides and can be equated so that

3.6.16.9.10 (u^k - 1)*f(u^k)m = (u^m - 1)*f(u^m)k = (u - 1)*f(u)km

Since both k and m are odd, by definition, we can factor the terms in (u^k - 1) and (u^m - 1) above, using the definiton (3.6.4) of f(u), we get

3.6.16.9.11 (u^k - 1) = (u - 1)*f(u)k

3.6.16.9.12 (u^m - 1) = (u - 1)*f(u)m

And, upon substituting for (u^k - 1) and (u^m - 1) into (3.6.16.9.10) and cancelling the common factor of (u - 1) we finally arrive at

3.6.16.9.13 f(u)km = f(u)k * f(u^k)m = f(u)m * f(u^m)k

We see f(u)km is composite, comprising at least two factors and it also gives us a nice identity from which to compute the value of any composite, f(u)km.

Notice that (3.6.16.9.13) is symmetric upon interchange of k and m, as would be expected. Furthermore, if m and k are equal, we get

3.6.16.9.14 f(u)m * f(u^m)m = f(u)m^2

If u = 1, we know that

f(1)m = m
f(1^m)m = m
f(1)m^2 = m^2

and we see that (3.6.16.9.14) correctly verifies as

m*m = m^2

If u = 2, we know that

f(2)k = 2^m - 1
f(2)m = 2^k - 1

and inserting for f(2)k and f(2)m into (3.6.16.9.13), we get

(2^m - 1) * f(2^m)k = 2^km - 1
(2^k - 1) * f(2^k)m = 2^km - 1

Since m and k are unique, the only way the rhs can factor in two ways, as above, is if, for some integer d, 2^km - 1 is of the form

(2^m - 1)*(2k - 1)*d = 2^km - 1

For example, if m = 3, k = 5, we find d= 151, since

(2^3 - 1)*(2^5 - 1)*d = 2^15 - 1

7*31*151 = 3276

The u = 2 case provides us with an instant factoring of the commonly factored number 2^n - 1, known as a Mersenne Number, see below. We can conclude from this composite exponent property (3.6.16.9) that, if n is composite, 2^n - 1 has at least two factors. Conversely, if we wish to test to see whether 2^n - 1 is prime then we only need consider values for which n is prime.

Numbers of the form 2^n - 1 are known as Mersenne Numbers and the result, just mentioned, is a well known result on the subject, see Section (4.4).

3.6.16.9.15 Example

The smallest, odd, composite exponent occurs when k = m = 3 and thus n = km = 9.

u = 2, k = 3, m = 3, n = km = 9

f(2)3 = 7 (prime)
f(2^3)3 = f(8)3 = 73 (prime)

f(2)9 = 511 = 7*73

Hence

f(2)3 * f(2^3)3 = f(2)9

Repeating for u = 3, we get

u = 3, k = 3, m = 3, n = km = 9

f(3)3 = 13 (prime)
f(3^3)3 = f(27)3 = 757 (prime)
f(3)9 = 9841 = 13*757

Hence

f(3)3 * f(3^3)3 = f(3)9

If we go back to the derivation of the Unity Root function f(u), section (3.6.4), then back substituting for f(u) into (3.6.3), we get an expression for the factorisation of u^n - 1 as

3.6.16.9.16 u^n - 1 = (u - 1)*f(u)

The expression (u^n - 1) is quite a commonly seen function in mathematics and, since we know the form of factors for f(u), we see from (3.6.16.9.16) this also gives us the form of factors for u^n - 1. In the special case that u = 2, we get the Mersenne numbers Mn = 2^n - 1. Since the factor (u - 1) is 1 for u = 2, the factorisation of Mersenne numbers is one of factorising the Unity Root function when 2 is the Unity Root of some base f(2). This particular case is discussed in more detail in Section (4.4).

3.6.16.9.17 Every number f(u) is equivalent to a number comprising only n unity digits when expressed in base u, i.e. f(u) base u is 1111...1.

For example, if u = 10, i.e. decimal base 10, all the numbers f(u) are of the form 1, 11, 111, etc for exponents n = 1, 2, 3. A quick glance at table (3.7.7) confirms that all row entries for u = 10 are indeed, 1, 11, 111 etc.

This is not difficult to show since, substituting for u = 10 in f((u)

f(10) = 1 + 10 + 10^2 + ...

i.e.

f(10) = 1 + 1*10 + 1*100 + ...

f(10) = 111...

This also tells us that for a binary base, u = 2, all the digits are one, and hence numbers of the form 2^n-1 have all their bits set.

3.6.16.10 Conjugate Unity Root function f'(u')

If the exponent is odd then, for every Unity Root u,

3.6.16.10.1 $u^n = 1 \pmod{a^n}$

there is a conjugate root u'

3.6.16.10.2 $u' = -u$

such that

3.6.16.10.3 $u'^n = -1 \pmod{a^n}$

Therefore, if there are n Unity Roots (mod a^n), there are also n conjugate Unity Roots. If U is the set of Unity Roots (mod a^n)

3.6.16.10.4 $U = \{u_0, u_1, \ldots u_{(n-1)} \}$

then the set of conjugate Unity Roots, U', is simply the negation of the positive Unity Roots.

3.6.16.10.5 $U' = \{-u_0, -u_1, \ldots -u_{(n-1)} \}$

Generally, throughout this paper, we choose to work with the positive form of Unity Roots. Nevertheless, many results and theorems for Unity Roots also apply to the conjugate forms.

Of interest with regard to factoring, see further below, is the conjugate Unity Root function f'(u') which we define by analogy with its Unity Root counterpart f(u), equation (3.6.4).

Rearranging (3.6.16.10.3)

3.6.16.10.6 $u'^n + 1 = 0 \pmod{a^n}$

This is the modular arithmetic analogue of the algebraic polynomial

3.6.16.10.7 u^n + 1 = 0

We can factor the left-hand side of the expressions as follows

3.6.16.10.8 u'^n + 1 = (u' + 1)*(1 - u' + ... (-1)^ru'^r + ... u'^(n - 1))

and thus define the 'Conjugate Unity Root Polynomial' f'(u')n as follows

3.6.16.10.9 f'(u')n = (1 - u' + ... (-1)^ru'^r + ... u'^(n - 1))

This polynomial is an oscillating sum, valid for odd exponents only.

If we substitute for u' in terms of u from (3.6.16.10.2) into (3.6.16.10.9), we see the two Unity Roots functions f(u) and f'(u') are, related

3.6.16.10.10 f'(-u)n = f(u)n

Because there is a 1:1 correspondence between Unity Roots and their conjugates, we can assert that, if the base a is of the 2ln + 1 form, there are n conjugate Unity Roots, as given by the set U' in equation (3.6.16.10.5). Furthermore, since the factor properties of the Unity Root function f(u) were derived by consideration of Unity Root properties we conclude the same factor properties must also apply to the conjugate Unity Root function. In particular, it shows us that the factors of f'(u')n are limited to the exponent n itself, or factors of the form 2ln + 1. Unlike f(u)n, valid for odd and even exponents, we have strictly only defined f'(u')n for odd exponent.

Lastly, if we can make statements about the factors of f'(u')n, then we can make statements about the frequently used function u'^n + 1, where n is odd.

Back substituting for f'(u')n from equation (3.6.16.10.9) into (3.6.16.10.8), we get an expression for the factorisation of u'^n + 1 as

3.6.16.10.11 (u'^n + 1) = (u' + 1)*f'(u')n

Thus, we see the factors of u'^n + 1 are (u' + 1) and f'(u')n when n is odd.

It would be nice, but unfortunately flawed, to think that we could use (3.6.16.10.11) to make claims on the factors of Fermat numbers Fn defined via

3.6.16.10.12 Fn = 2^(2^n) + 1

Unfortunately f'(u')n was defined exclusively for odd exponents and we see that the exponent for Fn is always even, of the form 2^n.

Examples

3.6.16.10.13 u' = 2, n = 3

2^3 + 1 = 3*3

Here u' + 1 = 3 and also the exponent, n = 3, divides f'(2)3 = 3

3.6.16.10.14 u' = 2, n = 5

2^5 + 1 = 3*11

Here u' + 1 = 3 and the other factor 11 divides f'(2)5. The factor 11 is of the form 2ln + 1, n = 5, l = 1.

3.6.16.10.15 u' = 3, n = 3

3^3 + 1 = 4*7

Here u' + 1 = 4 and the other factor 7 divides (equals) f'(3)3. The factor 7 is of the form 2ln + 1, n = 3, l = 1.

3.6.16.10.16 u' = 3, n = 5

3^5 + 1 = 4*61

Here u' + 1 = 4 and the other factor 61 divides (equals) f'(3)5. The factor 61 is of the form 2ln + 1, n = 5, l = 6.

3.6.16.10.17 u' = 5, n = 3

5^3 + 1 = 6*3*7

Here u' + 1 = 6 and the other factors 3 and 7 divide f'(5)3. The factor 3 is the same as the exponent, and the other factor 7 is of the form 2ln + 1, l = 1, n = 3.

3.6.16.11 Primality Testing

Because we can make many statements on the factors of f(u), section (3.6.16), it suggests we can deduce the composition or primality of f(u)n for various u and n. The key properties in Section (3.6.16), with respect to factorisation, are summarised as follows.

3.6.16.11.1 If n is composite, then f(u)n is composite.

3.6.16.11.2 If x is a prime factor of f(u)n it is either of the form x = n or x = 2ln + 1, integer l, l >= 1.

3.6.16.11.3 If x is a prime factor of f(u)n and x = n then x is always a factor of f(u)n at locations u = 1 + k*n, integer k, k >= 0.

3.6.16.11.4 If x is a prime factor of f(u)n and x = n then there is only one occurence of the factor x = n in the interval 0 <= u < x and that is at u = 1.

3.6.16.11.5 If x is a prime factor of f(u)n and x = 2ln + 1, integer l, l >= 1, then it will repeat n - 1 times in the interval 0 <= u < x.

3.6.16.11.6 If x is a prime factor of f(u)n and x = 2ln + 1, integer l, l >= 1, then it will be located at the Unity Root locations in the interval 0 <= u < x, u^n = 1 (mod x).

From these factor properties we can make the following assertion

For any number P = f(u)n, prime exponent n, to test the primality of P we only need to perform trial division on P for all prime numbers of the form 2ln + 1 less than the square root of P.

The key point is that primes numbers of the form 2ln + 1 are rarer than ordinary primes because, of course, not every integer is of the 2ln+1 form. Therefore any primality test using trial division will not have to perform nearly as many trial divisions when testing prime candidates f(u)n, as would have to be performed for any arbitrary prime candidate, i.e. the trial division only divides by numbers of the 2ln+1 form.

In the smallest exponent case, n = 3, there are 11 primes less than 100 of the form 6l+1

{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97}

This is actually quite a lot but it is still less than the total of 26 primes, the primes not of the form 6l+1, less than 100 which are

{2, 3, 5, 11, 17, 23, 29, 41, 47, 53, 59, 61, 71, 83, 89}

For larger exponent n, they become more scarce as, of course, do all primes.

Primality testing of very large numbers, e.g. 1000 plus digits, cannot be exhaustively performed by trial division since there are far too many primes and computational capability is not sufficient to do all the necessary trial divisions in any reasonable time span. Nevertheless trial division, using say the first million primes, is a good start to quickly eliminate composites. If we pick a prime candidate of the form f(u)n then, from what has just been said, we can go much further with the trial division, i.e. we can start with a larger prime candidate than might ordinarily be chosen since the first million primes, of the form 2ln + 1, will reach to a much larger trial divisor than the millionth prime.

Example

Let n = 1009 (prime)

The first 17 primes of the form 2l*1009 + 1 are, for l = 1 to 99,

{10091, 12109, 30271, 40361, 42379, 64577, 72649, 88793, 94847, 121081, 125117, 131171, 149333, 155387, 163549, 179603, 199783}

If we over-estimated the density of these primes and said there were 20 in the range 0-200000 we would have 1 prime every 10000. If we kept with this density we could reasonably estimate that the first million primes of 2l*1009 + 1 form would stretch all the way to 10^10. Thus, if we had a number of 20 digits, i.e. a maximum value of 10^20 - 1, and hence a square root < 10^10, then this tentative list of the first million primes would be sufficient to provide an exhaustive divisibilty test for a number constructed from f(u)1009. In fact, since the prime density decreases as the density of ordinary primes decreases with increasing number size, this is a pessimistic argument and the first million primes of the 2l*1009 + 1 form would arguably stretch well beyond 10^10. That said, we have to keep in mind that any prime candidate we test must be of the form f(u)1009, which has a term u^1008 in the f(u) polynomial, and so the prime candidate will not be a small number. Nevertheless, our first million trial divisions will stretch to prime factors at least of size 10^10, whereas the first million ordinary primes are of order 10^7 (TBD - needs some verfification work - there are about 6.6 million, use ln(n) / n etc.)

The smallest prime candidate we can pick for f(u)1009 is when u = 2. In which case we have the Mersenne number 'M1009', f(2)1009 = 2^1009 - 1 which has about 300 digits.

[Mersenne Primes are discussed again in more detail in section (4.4)].

If we wanted to perform an exhaustive prime divisibility test we would have to divide by all primes of the form 2l*1009 + 1 all the way up to approx 10^150. Obviously, this is not possible. Nevertheless, as a trial division, we could start by dividing M1009 by the 17 primes given above. Similarly for f(3)1009 and any number f(u)1009.

All that said, trial division is only a first stage and even for special numbers f(u)n, with their considerably reduced number of prime factors, it will not currently suffice for 1000 digit plus numbers.

Following trial division, a second stage of primality testing, for example a Fermat type test using MFST, Section (4.5), could then be employed to eliminate virtually all composites. However, since the MFST test is Monte-Carlo based, and therefore some composites could pass as primes, a more advanced primality testing algorithm has to be employed to conclusively prove primality or otherwise. See (ref TBD) for more details.

3.7 Determination of Unity Roots

3.7.1 Introduction

The determination of Unity Roots u, equation (3.1.1) is a problem in solving an (n - 1)'th order Diophantine equation for which, at least to the authors knowledge, there appears to be no general analytic solution.

For the n = 3 case, see the example below, the problem reduces to the solution, in integers, of a Quadratic. Similarly, for n = 4, the problem reduces to the solution, again in integers, of a cubic. Since the quadratic solution is almost trivial we shall give an example of a cubic Unity Root problem.

3.7.2 Example n = 3

For the n = 3 case the Unity Root Polynomial is a quadratic so we can apply some standard techniques.

By (3.6.4) the Unity Root Polynomial f(u)3 is

3.7.2.1 $f(u)3 = 1 + u + u^2$

And, by (3.6.7), the Unity Roots, (mod a^3) are obtained by solving

3.7.2.2 $1 + u + u^2 = 0 \pmod{a^3}$

This can be re-written in an algebraic form for some integer k, k > 0

3.7.2.3 $1 + u + u^2 = k*a^3$

And, in principle, we can solve this using the analytic solution for a quadratic equation, albeit we do not know the value of integer k.

Comparing (3.7.2.3) with a standard quadratic equation

3.7.2.4 $Ax^2 + Bx + C = 0$

we get for the coefficients A,B and C

3.7.2.5 $A = 1, B = 1, C = 1 - k*a^3$

The quadratic discriminant D is defined by,

3.7.2.6 $D = B^2 - 4AC$

which, upon substituting for A, B and C from (3.7.2.5), gives

3.7.2.7 $D = 4k*a^3 - 3$

and, for non-complex solutions, this must satisfy

3.7.2.8 $D >= 0$

and therefore, by (3.7.2.7),

3.7.2.9 $4k*a^3 - 3 >= 0$

This is clearly true for all $a > 0$, $k > 0$.

For integer solutions the discriminant must also be a perfect square as the general solution is:

3.7.2.10 $u = [-B +/- \sqrt{D}] / 2A$

with the two solutions in positive and negative form

3.7.2.11 $u = (-B + \sqrt{D}) / 2A$

3.7.2.12 $u = (-B - \sqrt{D}) / 2A$

Therefore we must have, for some integer l, $l > 0$,

3.7.2.13 $D = l^2$

using (3.7.2.7) this implies

3.7.2.14 (4k*a^3 - 3) = l^2

To complete this cubic example, if we look at the specific case of a = 7 we see that if k = 1 then (3.7.2.14) gives us an integer solution for l = 37 since

3.7.2.15 (4*7^3 - 3) = 37^2

It seems remarkably fortuitous that the first value of k to try, i.e. k = 1, immediately gives a perfect square result. This certainly isn't the case for a = 13, n = 3, (a = 13 is the next '2ln + 1' prime after a = 7) we find that k = 489 and this gives u = 1036 or -1037.

The significance of this good fortune, if there is any, currently eludes the authors. Nevertheless, continuing with the solution for n = 3, a = 7, with l = 37, i.e. D= 37^2, we get for the Unity Roots u, using (3.7.2.11) and (3.7.2.12),

3.7.2.16 U = {18, -19}

Since -19 = 324 (mod 7^3), the complete set of Unity Roots a = 7, n = 3, in positive primitive form, is

3.7.2.17 U = {1, 18, 324}

Notice that 324 = 18^2. From the properties (3.3.1) and (3.3.2), the roots are cyclic and, with the generator u = 18, the other roots are u^2 and u^0, i.e. 324 and 1 respectively.

With u = 18 the sum of the roots, as given by (3.6.14.4), is confirmed to be exactly 7^3, i.e. 343.

3.7.2.18 1 + 18 + 18^2 = 343

Note that if we use u = 18^2, i.e. 324, the sum becomes

3.7.2.19 1 + 324 + 324^2 = 307*343

which is also seen to be a multiple of the modulus, 7^3.

3.7.3 Algorithmic Determination

Although we do not have an analytic solution to determine Unity Roots for an arbitrary base and exponent we can, by an algorithmic method, obtain one or more of the Unity Roots (mod a^n) given the Unity Roots (mod a). Due to the cyclic group properties of the roots all other roots can be then be generated from a single root.

An analytic solution for the determination of Unity Roots (mod a), for arbitrary exponent, is a separate problem for which we also do not have an analytic solution. For small base they are not too hard to find and a method based upon the Unity Root polynomial is given following in section (3.7.5)

The algorithm to determine Unity Roots (mod a^n) works on the principle that the Unity Roots, u^n (mod a^n), are also Unity Roots u^n (mod a^(n - 1)), u^n (mod a^(n - 1)) etc. down to u^n (mod a).

Algebraically expressed, if

3.7.3.1 u^n = 1 (mod a^n)

then

3.7.3.2 u^n = 1 (mod a^(n - 1))

3.7.3.3 u^n = 1 (mod a^(n-2))

etc. down to (mod a), i.e.

3.7.3.4 u^n = 1 (mod a)

To use the method we have to first locate the Unity Roots for equation (3.7.3.4)

If we know a Unity Root ‘u1’ (mod a) such that u1 is in the region 1 < u1 < a, then we know that a Unity Root (mod a^2) must lie at some location u1 + s1*a for some to-be-determined integer s1, s1>= 0, since, from what has been said above, if u1 is a Unity Root (mod a^2), it must also be a Unity Root (mod a).

[Note that here ‘u1’ denotes a non-trivial root (mod a^1), ‘u2’ denotes a non-trivial root (mod a^2), etc.].

u1 is thus defined by the usual congruence

3.7.3.5 u1^n = 1 (mod a)

and, for some integer s1, s1>= 0, we know that

3.7.3.6 $(u1 + s1*a^1)^n = 1 \pmod{a^2}$

We now have to find the integer s1. If we expand the lhs and take residues (mod a^2) then the only term that remains is linear in the constant integer s1 and we get

3.7.3.7 $u1^n + n * s1 * a * u1^{(n - 1)} = 1 \pmod{a^2}$

This can easily be re-written as a Linear Diophantine equation in unknowns s1 and t1.

3.7.3.8 $n * s1 * a * u1^{(n - 1)} + t1 * a^2 = 1 - u1^n$

This does have solutions which can be determined as per Euler's Algorithm. We know there must exist a solution, without recourse to any of the usual GCD considerations of the coefficients of s1 and t1, because if a is of the 2ln + 1 form there must be Unity Roots (mod a^n) and hence Unity Roots for all exponents from n to 1 as per (3.7.3.1) to (3.7.3.4).

Of the two solutions to (3.7.3.8) only s1 is of use and t1 can be junked. With s1 determined, we can now define an integer u2

3.7.3.9 $u2 = u1 + s1*a^1$

such that, by (3.7.3.6),

3.7.3.10 $u2^n = 1 \pmod{a^2}$

And, since we now have a Unity Root u2, (mod a^2), where u2 is in the region $1 < u2 < a^2$, then we know that a Unity Root (mod a^3) must lie at some location $u2 + s2*a^2$ for some to-be-determined integer s2, $s2 >= 0$. This is because, from what has been said above, if u is a Unity Root (mod a^3), it must also be a Unity Root (mod a^2).

So, for some integer s2, $s2 >= 0$, we know that

3.7.3.11 $(u2 + s2*a^2)^n = 1 \pmod{a^3}$

We now have to find the integer s2. If we expand the lhs of (3.7.3.9) and take residues (mod a^3) the only term that remains is linear in the constant integer s2 and we get

3.7.3.12 $u2^n + n * s2 * a^2 * u2^{(n - 1)} = 1 \pmod{a^3}$

Which can be written as a LDE in unknown's s2, and t2.

3.7.3.13 n * s2 * a^2 * u2^(n - 1) + t2 * a^3 = 1 - u2^n

Once again, this does have solutions for s2 and t2 and, of the two solutions, only s2 is of use and t2 can be junked.

In this way we continue the whole process to get a Unity Root (mod a^n).

In general, with the r-1'th Unity Root 'ur_1' determined such that

3.7.3.14 (ur_1)^n = 1 (mod a^(r-1))

then for some, to-be-determined integer sr_1, sr_1 >= 0, the r'th Unity Root ur is located at

3.7.3.15 ur = (ur_1) + sr_1*a^(r-1)

such that

3.7.3.16 ur^n = 1 (mod a^r)

And, substituting for ur using (3.7.3.15) into (3.7.3.16), expanding and taking residues (mod a^r), we get the following LDE in the unknowns 'sr_1' and integer, 'tr_1' (sr_1 is the (r-1)'th. iterate of constant s, similarly for tr_1).

3.7.3.17 n*sr_1*a^r*(ur_1)^(n - 1) + tr_1*a^r = 1 - (ur_1)^n

This LDE can be solved for sr_1 to give the r'th Unity Root ur. The process repeating to determine the (r+1)'th Unity Root etc. until r = n when we get the desired n'th order Unity Root u given by

3.7.3.18 u = un_1 + sn_1*a^n

The integer unknown 'sn_1' (the n-1'th iterate of s) is obtained by substituting for u from (3.7.3.18) into

3.7.3.19 u^n = 1 (mod a^n)

and solving the resulting LDE.

This method, although laborious, is ideally suited for a computer.

The limitation with this method is that we do need to know a Unity Root (mod a) other than the trivial u = 1. In some cases this is not too difficult to obtain.

3.7.4 Example: Unity Roots (mod 7^3)

Find the Unity Roots u (mod 7^3),

3.7.4.1 u^3 = 1 (mod 7^3)

Suppose u1 is a Unity Root to the (mod 7) problem

3.7.4.2 u1^3 = 1 (mod 7)

then the solution set U1 of Unity Roots to (3.7.4.2) is, by simple hand-calculation,

3.7.4.3 U1 = {2, 4}

Let us use the lowest of these two roots

3.7.4.4 u1 = 2

then, by (3.7.3.9), we know the Unity Root (mod 7^2) is of the form

3.7.4.5 u2 = 2 + 7*s1

and we must now solve for s1

3.7.4.6 u2^3 = 1 (mod 7^2)

Substituting for u2 from (3.7.4.5) into (3.7.4.6) and eliminating terms in 7^2 and higher, since they are congruent to 0 mod 7^2, we get

3.7.4.7 2^3 + 3 * 2^2 * 7 * s1 = 1 (mod 7^2)

Factoring 2^2 this becomes

3.7.4.8 4 * (2 + 3 * 7 * s1) = 1 (mod 7^2)

Defining x as

3.7.4.9 x = (2 + 3 * 7 * s1)

then (3.7.4.8) can be re-written

3.7.4.10 4x = 1 (mod 7^2)

which can be expressed as a LDE in unknowns x and y

3.7.4.11 4x - 49y = 1

and has solutions, for arbitrary integer t,

3.7.4.12 x = -12 + 49t

3.7.4.13 y = -1 + 4t

We only require the solution for x. Substituting for x back into (3.7.4.9), and tidying-up, we now get a LDE in s1 and t as follows

3.7.4.14 7t - 3*s1 = 2

which has solutions, for arbitrary integer w,

3.7.4.15 s1 = 4 + 7w

3.7.4.16 t = 2 + 3w

and so we now have a solution for s1. Substituting for s1 into (3.7.4.5) we get a solution for u2 that satisfies (3.7.4.6), i.e.

3.7.4.17 u2 = 2 + 7*(4 + 7w)

which simplifies to

3.7.4.18 u2 = 30 + 7^2 * w

For w = 0, we get the primitive, positive root u2 = 30 and verifying

3.7.4.19 30^3 = 1 (mod 7^2)

So far, so good. Now we finally have to determine the Unity Root (mod 7^3). Defining u3 as follows, for some unknown integer s2,

3.7.4.20 u3 = 30 + 7^2 * s2

we must now solve for s2 by substituting for u3 into the Unity Root equation

3.7.4.21 u3^3 = 1 (mod 7^3)

and solving as a LDE.

We could, at this stage guess u3 since in its most primitive form we know it is in the range 1 < u3 < 7^3. If we tried s2 = 0, 1, 2, 3, 4, 5, 6 then, by trial and error, one of these seven values would satisfy u3^3 = 1 (mod 7^3). Nevertheless this is only practical for small bases. Secondly, it would not constitute a general algorithmic method. For those impatient, the correct value for s2 is 6 which gives u3 = 324. However, let us go through the algorithmic process to verify this.

Substituting for u3 from (3.7.4.20) into (3.7.4.21) and eliminating terms in 7^3 and higher, since they are congruent to 0 (mod 7^3), we get

3.7.4.22 30^3 + 3 * 30^2 * 7^2 * s2 = 1 (mod 7^3)

factoring 30^2

3.7.4.23 30^2*(30 + 3 * 7^2 * s2) = 1 (mod 7^3)

defining x as

3.7.4.24 x = (30 + 3 * 7^2 * s2)

then (3.7.4.23) can be re-written

3.7.4.25 30^2 * x = 1 (mod 7^3)

which can be expressed as a LDE in unknowns x and y

3.7.4.26 30^2 * x - 343 * y = 1

which has solutions, for arbitrary integer t,

3.7.4.27 x = 226 + 343t

3.7.4.28 y = 593 + 30^2 * t

We only require the solution for x. Substituting for x back into (3.7.4.24), we now get a LDE in s2 and t as follows

3.7.4.29 7*t - 3*s2 = -4

which has solutions, for arbitrary integer w,

3.7.4.30 s2 = 6 + 7w

3.7.4.31 t = 2 + 3w

So we now have a solution for s2 and, substituting for s2 into (3.7.4.20), we get a solution for u3 that satisfies (3.7.4.21)

3.7.4.32 u3 = 30 + 7^2 * (6 + 7w)

which simplifies to

3.7.4.33 u3 = 324 + 7^3w

For w = 0 we get the positive root u3 = 324 and, verifying this,

3.7.4.34 324^3 = 1 (mod 7^3)

We can use this root to find the other non-unity, Unity Root. Note that for a cubic, prime base, there are three roots of which one is unity. The second root we have just found is 324 and, since the roots sum to a^3 in the cubic case, Theorem (3.6.14), we know the third root must be 343 - (1 + 324) = 18. Alternatively, we could use 324 as the generator where the other root = u3^2 (mod a^3). Doing so we find that 324^2 = 18 (mod 7^3) and hence 18 is confirmed as the other root. Conversely, note that 324 = 18^2 (mod 7^3). Since any element is also a generator we would expect 324 to be a perfect square (mod a^3).

The complete set of cubic Unity Roots, (mod 7^3), is therefore

(3.7.4.35) U = {1, 18, 324}

3.7.5 Unity Roots (mod a)

The algorithmic method to determine a Unity Root (mod a^n), as detailed in the previous section, requires prior knowledge of a Unity Root (mod a). Unfortunately, at least to the authors knowledge, there appears to be no general analytic method by which Unity Roots (mod a) can be determined for arbitrary n. Nevertheless, tabulating the Unity Root polynomial f(u)n, equation (3.6.4) and table (3.7.7), can give us some roots relatively easily.

Theorem (3.6.13) proves that for arbitrary u, u is Unity Root (mod f(u)n), i.e.

3.7.5.1 u^n = 1 (mod f(u)n)

If we interpret f(u) as the base modulus 'a'

3.7.5.2 a = f(u)n

then we see that u^n is a Unity Root, (mod a), as desired.

3.7.5.3 u^n = 1 (mod a)

Of course, there are only certain values f(u) can take so it would appear that we cannot use this method for any arbitrary a. However this is not so and we can actually find all desired Unity Roots, (mod a), by using f(u)n as the base. We will see that f(u) is often composite with the desired factor a, i.e. for integer k, if f(u)n = k*a then u^n is still a Unity Root (mod a) according to (3.7.5.1). Note too that it is also a Unity Root (mod k).

3.7.5.4 Example, u = 5, n = 3

Suppose we pick a Unity Root u = 5 then the cubic Unity Root function f(u)3 is

f(u)3 = 1 + 5 + 5^2

i.e.

f(5)3 = 31

Therefore we know that

5^3 = 1 (mod 31)

and, verifying, we see this is true since

5^3 = 4*31 + 1

Although the base modulus f(u)3 = 31 is not a perfect power, we know from section (3.7.3) that we will be able to obtain, by algorthmic methods, the roots for any base that is a power of 31, given this root u = 5.

3.7.5.5 Example, u = 7, n = 3

Suppose we pick a Unity Root u = 7 then the cubic Unity Root function f(u)3 is

f(u)3 = 1 + 7 + 7^2

i.e.

f(7)3 = 57

Therefore we know that

7^3 = 1 (mod 57)

and, verifying, we see this is true since

7^3 = 6*57 + 1

Furthermore, if we expand the whole of 7^3, as given immediately above, into prime factors and their powers, i.e.

7^3 = 2 * 3^2 * 19 + 1

then we also see that

7^3 = 1 (mod 2)

7^3 = 1 (mod 3)

7^3 = 1 (mod 3^2)

7^3 = 1 (mod 19)

and therfore u = 7 is a Unity Root mod 2, 3, 3^2 and 19

3.7.6 A perfect power f(u)

If the base f(u) is composite there might be values of u for which it is a perfect power or contains, as a factor, a perfect n'th power. This is the case for u = 18, n = 3 as in the following example.

3.7.6.1 Example, u = 18, n = 3

Suppose we pick a Unity Root u = 18 then the Unity Root function f(u) for exponent n = 3 is

f(u)3 = 1 + 18 + 18^2

i.e.

f(18)3 = 343

Therefore we know that

18^3 = 1 (mod 343)

and, since,

343 = 7^3

we have a Unity Root, u = 18, (mod 7^3)

18^3 = 1 (mod 7^3)

It is important to note here that both the exponent n = 3 and the perfect power in the base modulus is also 3. Since they are the same we see that u = 18 is a cubic root to the cubic modulus a^3 = 7^3 and we have effectively found (by luck) a Unity Root (mod a^3).

It is 'lucky' in that we picked a value u = 18 which just so happened to have an f(u)3 function which contained, as a factor, a perfect cube. In this case the f(u)3 value was exactly 7^3 albeit it could equally well have been some multiple k*7^3 and still be valid.

3.7.7 Tabulation f(u)

(TBD)

3.7.8 How does this help us find Unity Roots (mod a)?

Suppose we pick an arbitrary value for a. For now we assume a is an odd prime. The exponent will always be assumed to be odd, prime, n >= 3. The value a will also have to be of the 2ln + 1 form to be of interest, i.e. have n roots within the interval [0, a^n).

[Note that if a is an odd prime but not of the form 2ln + 1, and n != a, then it has one and only one primitive Unity Root at u = 1 and all other primitive roots at 1 + k*a^n, integer k, k >= 1. If a is prime and n = a, and therefore cannot be of the 2ln + 1 form, there is one and only one Unity Root within each Minimal Residue Sequence , size a^n / n, at location 1 + k*a^(n - 1), integer k, 0 <= k < n].

To find a Unity Root (mod a) we would look down the column for exponent n and see where a appears as either the value of f(u)n or as one of its factors. We then read across to find which value of u generates the value f(u)n.

For example, suppose we require the Unity Root for

a = 41, n = 5

We note 41 = 2 * 4 * 5 + 1 hence the value a = 41 is of the 2ln + 1 form. If we look down the n = 5 column to find the first occurence of 41 as a factor of f(u)5 then we see that the value of f(u)5 = 11111 (= 41*271) at u = 10 and so 10^5 = 1 (mod 41). Since 271 is the other factor, we also know that 10^5 = 1 (mod 271).

Because there is always a value of f(u) for whatever integer u we choose, We can arrive at the conclusion that every integer u, is a Unity Root, for some base f(u), exponent n.

3.7.9 Special Cases, (mod a)

3.7.9.1 a = 2n + 1

Section (2.6.11) states that for prime modulus a, exponent n such that a is of the form given by (3.7.9.1) then the residue r, (mod a), for any integer x, 0 < x < a, as given by,

3.7.9.2 x^n = r (mod a)

can only either be +1 or -1. What we do not know is whether the residue is -1 or +1. However, if the residue is -1 we know the conjugate residue at (a - x) is +1 and vice versa. If we know just one value x (excepting x = +1 and x = -1, see further) which gives a residue of +1 or -1 then, since all the roots are cyclic, the other n-1 roots are at locations x^2, x^3 etc. We will eventually cycle through all n roots that give the same residue. The value x acts as the generator of the group.

[Note that the root x = +1, which gives a residue of +1, cannot be used as a generator since repeated exponentiation gives the same value +1. Likewise for the root at x = a - 1 which has the residue r = -1].

To find all the roots we simply have to pick an initial value, say x = 2, determine its residue and then find all the other n - 1 roots by cyclic generation. Once we have all the roots for, say residue r = +1, the remaining n values of x, which are not roots of +1, are the roots for the conjugate residue, a - x (mod a).

3.7.9.3 Example

a = 11, n = 5

Firstly, we see a is of the 2n + 1 form so we know it has 5 Unity Roots

$$x^5 = +1 \pmod{11}$$

and 5 conjugate roots

$$(11 - x)^5 = -1 \pmod{11}$$

If we start with x = 2 we find that this has a residue r = -1 since

$$2^5 = -1 \pmod{11}$$

Therefore, to get the next root of -1, we use x = 2 as a generator and the remaining roots, not including -1, are thus x = 4, x = 8, x = 5 since

$$2^2 = 4 \pmod{11}$$
$$2^3 = 8 \pmod{11}$$
$$2^4 = 5 \pmod{11}$$

Verifying we see that, as expected,

$$4^5 = -1 \pmod{11}$$
$$8^5 = -1 \pmod{11}$$
$$5^5 = -1 \pmod{11}$$

The other root is given by x = -1, i.e. x = 10 (mod 11). Thus, the five roots with a residue of -1 are

$$(2, 4, 5, 8, 10\}$$

and this leaves the roots of +1 as

$$\{1, 3, 6, 7, 9\}$$

3.8 Composites

3.8.1 Introduction

In this section, we shall show that the Unity Roots of a composite can be determined from the Unity Roots of the prime factors.

3.8.2 Theory: Unity Roots of Factors

We will work with an arbitrary modulus A which, within this paper, is normally either A = a or A = a^n.

If the base A is composite, comprising two unique co-prime factors k and m, i.e.

3.8.2.1 A = km

and, if u is a Unity Root (mod a) such that, by the usual definition,

3.8.2.2 u^n = 1 (mod A)

then expanding u^n in quotient remainder form we get

3.8.2.3 u^n = l*A + 1

Substituting for A from (3.8.2.1) in terms of its factors k and m

3.8.2.4 u^n = l*km + 1

we see that the Unity Root u is also a Unity Root of the factors k and m since

3.8.2.5 u^n = 1 (mod k)

3.8.2.6 u^n = 1 (mod m)

Denoting a Unity Root of factor k by u(k) and that of factor m by u(m) where $0 < u(k) < k^n$, $0 < u(m) < m^n$ then, by definition,

3.8.2.7 u(k)^n = 1 (mod k)

and

3.8.2.8 u(m)^n = 1 (mod m)

Thus, by (3.8.2.5) and (3.8.2.6), for some to-be-determined, integer constants c(k) and c(m), the Unity Root u of the composite A can be expressed in terms of the Unity Roots u(k) and u(m) of its factors, k and m respectively, as follows

3.8.2.9 u = u(k) + c(k)*k

3.8.2.10 u = u(m) + c(m)*m

In such a form we see that equations (3.8.2.5) and (3.8.2.6) are simultaneously satisfied if we can find constants c(k) and c(m). This can be done by equating (3.8.2.9 and 3.8.2.10) and solving for c(k) and c(m) as unknowns of a LDE.

Before proceeding we shall examine how many Unity Roots there are so we can determine the number of equations to solve.

Defining the number Nk of Unity Roots for factor k as follows

3.8.2.11 Nk = number of Unity Roots, u^n = 1 (mod k),

Then Nk can have one of the following possible values

Nk = n if k = 2ln + 1, 0 < u < k^n
Nk = 1 if k!= 2ln + 1 and k!= n, 0 < u < k^n
Nk = 1 if k = n, 0 < u < k^n / n
Nk = n if k = n, 0 < u < k^n

Similarly, defining the number Nm of Unity Roots for factor m as follows

3.8.2.12 Nm = number of Unity Roots u^n = 1 (mod m)

Then Nm can have one of the following possible values

Nm = n if m = 2ln + 1, 0 < u < m^n
Nm = 1 if m!= 2ln + 1 and m!= n, 0 < u < m^n
Nm = 1 if m = n, 0 < u < m^n / n
Nm = n if m = n, 0 < u < m^n

Finally, defining the number Nkm of Unity Roots for the composite A (= km) as follows

3.8.2.13 Nmk = number of Unity Roots u^n = 1 (mod A)

then the composite A has Nmk Unity Roots given by the product of Nk and Nm

Nmk = Nm * Nk
Nmk = 1, n or n^2, see (3.8.2.11) and (3.8.2.12)

Returning to equations (3.8.2.9) and (3.8.2.10); because there are Nk values of u(k) and Nm values of u(m), equation (3.8.2.9) actually comprises Nk equations and equation (3.8.2.10) comprises Nm equations. If we equate them, which we shall do so in a moment, we will have Nm*Nk separate equations (= Nmk by (3.8.2.13)), which cannot all possibly be dependent.

Since the expressions (3.8.2.9) and (3.8.2.10) are linear in the constants, by equating them and rearranging, we get

3.8.2.14 c(k)*k^n - c(m)*m^n = u(m) - u(k)

which are the aforementioned Nmk LDEs in the 2Nmk unknowns c(k) and c(m). These LDEs can be solved by by algorithmic methods. Of course if Nmk is n^2 this is a lot of LDEs to solve. Fortunately we do not have to solve this many. Firstly, and most importantly, we know that the roots u are cyclic and all we have to find is a single, non-unity, Unity Root to act as a generator for all other Unity Roots. One might then think we can go from having to solve a maximum of n^2 equations to merely having to solve only one. Perhaps, not surprisingly, the truth lies in between.

We will proceed assuming each factor k and m has n roots

3.8.2.15 Nk = n

3.8.2.16 Nm = n

and therefore Nmk has, by (3.8.2.13), n^2 possible roots.

3.8.2.17 Nmk = n^2

Excluding the trival root +1, the number of non trivial roots is given by

3.8.2.18 Nmk - 1 = n^2 - 1

Since each factor has Nk = Nm = n - 1 non trivial roots, all of which can be derived from one of them as generator, the total number of independent generators ‘Ng’ is given by

3.8.2.19 Ng = (Nmk - 1) / (n - 1)

Substituting for Nmk from (3.8.2.18)

3.8.2.20 Ng = (n^2 - 1) / (n - 1)

and factoring out (n - 1) we get for Ng

3.8.2.21 Ng = n + 1

Thus the total number of independent, non-trivial generators for the composite a, comprising two, odd prime factors k and m, is (n + 1). For instance if n = 3 there are 4 generators. The following Example Data illustrates this.

3.8.3 Example Data

3.8.3.1 a = 91, k = 7, m = 13

u(7) = {1, 18, 324}

u(13) = {1, 1036, 1160}

91^3 = 753571

N7 = 3

N9 = 3

N91 = N7*N9 = 9

The nine Unity Roots of 91^3 are

U(91) = {1, 9948, 59320, 69267, 244903, 304222,
439401, 449348, 684303}

Since

Nk = Nm = 3

Then

Nkm = Nm*Nk = 9

And the number of generators

Ng(91) = (Nm*Mk - 1) / (Nm - 1) = 4

Four possible generators are {9948, 59320, 69257, 304222} and the other roots they generate, by squaring (in the cubic case), are given by

9948^2 = 244903 = 1 (mod 91^3)

59320^2 = 439401 = 1 (mod 91^3)

69267^2 = 684303 = 1 (mod 91^3)

304222^2 = 449348 = 1 (mod 91^3)

3.8.4 Mulitple Factors

We can generalise the above arguments to r prime factors. In this case the maximum total number of Unity Roots, given each factor had n roots, would be n^r

3.8.4.1 Ng = (n^r - 1) / (n - 1)

If not all roots have n factors, i.e. some (most) may have only the single trivial root +1 if they are not of the 2ln + 1 form, then n^r in (3.8.4.1) is replaced by n^r' where r' is the number of factors with n roots.

In example (3.8.5), given below, only one of the two factors, namely 7, has 3 Unity Roots since n = 3 and it is of the 2ln + 1 form. The other factor has only one root so the total number of generators is 1, according to (3.8.4.1) where 1 = (3^1 - 1) / (3 - 1).

If the modulus A is a^n, as is the most common modulus used throughout this paper, and a is composite, i.e. a = km, then A^n = a^n = (km)^n. We can re-cycle the same arguments above using the base A = a^n and replacing k with k^n and m with m^n.

If the base a is prime, even though the modulus a^n is no longer prime, it is the only unique prime factor and therefore, in terms of the number of roots, it is the same as for a prime modulus.

Section (3.9) gives a more detailed exposition on determining Unity Roots for composites, with regard to the Pythagorean case, including some lengthy examples. A couple of examples for odd exponent are given below. For more detail in understanding the process see also section (3.9).

3.8.5 Example

3.8.5.1 n = 3, a = 14, k = 2, m = 7

The Unity Roots of the composite a, and factors k and m are

3.8.5.2 U(14) = {1, 361, 1353}

3.8.5.3 U(2) = {1}

3.8.5.4 U(7) = {1, 18, 324}

Since the composite 14 only contains a single prime factor of the form 2ln+1 (= 7) there are only three roots for the composite. These are not the same as the factors however, as will be seen.

For the factor k = 2, by equation (3.8.2.9), we know that all U(14) are of the form

3.8.5.5 u_0(14) = +1 + c_0(2)*2^3
u_1(14) = +1 + c_1(2)*2^3
u_2(14) = +1 + c_2(2)*2^3

where there are three constants c_i(2), i =0, 1, 2 to be determined for each of the three U(14) roots.

For the factor m = 7, by equation (3.8.2.10), we know that all U(14) are also of the form

3.8.5.6 u_0(14) = +1 + c_0(7)*7^3
u_1(14) = +18 + c_1(7)*7^3
u_2(14) = +324 + c_2(7)*7^3

Equating each root u_i(14), i =0, 1, 2 in (3.8.5.5) with (3.8.5.6), we get the following three LDEs, each in two unknowns, namely the constants c_i(2) and c_i(7), i = 0, 1, 2

3.8.5.7 c_0(2)*2^3 - c_0(7)*7^3 = 0

3.8.5.8 c_1(2)*2^3 - c_1(7)*7^3 = 17

3.8.5.9 c_2(2)*2^3 - c_2(7)*7^3 = 323

Since, by their cyclic properties, we can get all the roots from a single solution, say u_1(14), we need only solve one of the LDEs (3.8.5.8) or (3.8.5.9) to get the two, non-unity roots. Nevertheless, solving all these LDEs gives, for arbitrary integer constants f, g and h we get

3.8.5.10 c_0(2) = f*7^3
c_0(7) = f*2^3

3.8.5.11 c_1(2) = 45 + g*7^3
c_1(7) = 1 + g*2^3

3.8.5.12 c_2(2) = 169 + h*7^3
c_2(7) = 3 + h*2^3

To get the constants within the 0 < c_i < 14^3 range, simply set f, g and h to zero and then substitute back into either (3.8.5.5) or (3.8.5.6) to finally give for the three roots of the composite 14

3.8.5.13 U(14) = {1, 361, 1353 }

These can be verified as correct

3.8.5.14 361^3 = 1 (mod 14^3)

3.8.5.15 1353^3 = 1 (mod 14^3)

and, by the cyclic property,

3.8.5.16 361^2 = 1353 (mod 14^3)

3.9 Pythagoras and Unity Roots

3.9.1 Prime base a

For n = 2, arbitrary base (composite or prime), there are always at least two Unity Roots +1 and a^2 - 1 in the interval 0 < u < a^2. If the base a is prime there are only two roots, (mod a) or (mod a^2), written in the positive form as the set U as follows

3.9.1.1 U = {+1, a^2 - 1}

It is usually simpler to use the negative form for clarity of algebraic manipulation and -1 is often used in place of a^2 - 1, i.e. we write U as

3.9.1.2 U = {+1, -1}

In particular, for prime base a, we shall see that it is always the negative Unity Root -1 that is responsible for Pythagorean triples.

3.9.1.3 Theorem: Pythagoras, Negative Unity Root Mapping

If the base a is prime and (b,c) is a Candidate Pair, (mod a^2), such that b maps to c via the Unity Root u, i.e.

3.9.1.3.1 c = u*b (mod a^2)

and, if (a, b, c) is a Pythagorean triple, then the Unity Root responsible for the mapping is always negative, i.e. u = -1.

Proof

Writing the Pythagoras Equation as

$$c^2 - b^2 = a^2$$

and factoring the lhs

$$(c + b)*(c - b) = a^2$$

then, by Theorem (1.14), we know that if the base a is prime then the factor (c - b) is such that

$$c - b = 1$$

This implies that the other factor (c + b) is

$$c + b = a^2$$

Taking residues (mod a^2)

$$c = -b \pmod{a^2}$$

and comparing this with (3.9.1.3.1) we see that

$$u = -1$$

If u were to be +1 then we would have

$$c = b \pmod{a^2}$$

rearranging

$$c - b = 0 \pmod{a^2}$$

which implies for integer l

$$c - b = l*a^2$$

If l = 0, this implies c = b and we get

$$2*b^2 = a^2$$

which has no integer solution

If l != 0, then

| c - b | >= a^2

which will not give us a Unity Root gap, since Theorem (1.12) proves that, for prime base a, c - b < a, where c > b as per the convention throughout this paper.

We thus conclude that if (a, b, c) is a Pythagorean triple then the Candidate Pair (b,c) is such that c = -b (mod a^2) and b maps to c via the negative Unity Root only.

We shall see that for composites this is only true for one or more factors but not all of them.

3.9.1.3.2 What does Theorem (3.9.1.3) mean physically?

For prime, odd base a, a > 2, the entire residue sequence x^2 (mod a^2), for 0 <= x < a^2, is symmetric about the mid-point which is actually the half-integer point (a^2) / 2. Any Candidate Pair (b,c) is such that the b value lies in the lower half and that, by Theorem (3.9.1.3), the value c is a mirror image of b about the centre point, lying in the upper half of the residue sequence, c > a^2 / 2. Alternatively stated, c is the value b flipped about the centre point. However, by Theorem (1.14), we know that c is numerically one greater than b. The only way to satsify these two Theorems is if b is exactly the largest integer not greater than the mid-point and that c is the smallest integer, not less than the mid-point. Since the mid-point is half integral at a^2 / 2 we conclude that, for prime base a,

b = (a^2 - 1) / 2

c = (a^2 + 1) / 2

One can verify that the resulting triple (a, b, c) satisfies the Pythagoras equation (1.1.2).

3.9.2 Composites base a

If a is composite there are two roots for each unique prime factor of a and hence there are 2^r roots, where r is the number of unique, prime factors. For simplicity we shall proceed assuming r = 2, i.e. only two unique prime factors.

Let a be composite with two, unique prime factors k and m, i.e.

3.9.2.1 a = k*m

Each prime factor has two roots, (mod a^2), denoted u(k) and u(m)

3.9.2.2 U(k) = {+1, k^2 - 1} = {+1, -1} (mod k^2)

3.9.2.3 U(m) = {+1, m^2 - 1} = {+1, -1} (mod m^2)

From what has been said about the Unity Roots of composites, section (3.8.2), the Unity Roots u, (mod a^2), for some integer constants c(k) and c(m), will be of the form

3.9.2.4 u = u(k) + c(k)*k^2

3.9.2.5 u = u(m) + c(m)*m2^2

With two factors there are four separate roots for the composite (two for each unique prime factor) given by the set U(km)

3.9.2.6 U(km) = {u_0, u_1, u_2, u_3 }

And, for each of the four roots in the set, there are four constants c(k) and four constants c(m), i.e. eight constants in all (8= 2*n^2, see section (3.8.2) equations (3.8.2.9) and (3.8.2.10)), which satisfy the equations

3.9.2.7 u_0 = u(k) + c_0(k)*k^2

3.9.2.8 u_0 = u(m) + c_0(m)*m^2

3.9.2.9 u_1 = u(k) + c_1(k)*k^2

3.9.2.10 u_1 = u(m) + c_1(m)*m^2

3.9.2.11 u_2 = u(k) + c_2(k)*k^2

3.9.2.12 u_2 = u(m) + c_2(m)*m^2

3.9.2.13 u_3 = u(k) + c_3(k)*k^2

3.9.2.14 u_3 = u(m) + c_3(m)*m^2

At this stage we do not know exactly which roots u(k) are to be inserted in which equation. For example, is u(k), in the expression for u_0, equation (3.9.2.7), equal to +1 or –1? Similarly for all the other seven equations (3.9.2.8) to (3.9.2.14). We also

need to determine the 8 constants c_0(k), c_0(m) etc.. To do this we equate the respective expressions for u_0, u_1 etc to get four LDEs, each in two unknowns which are the constants c_0(k), c_0(m) etc.

3.9.2.15 c_0(k)*k^2 - c_0(m)*m^2 = u(m) - u(k)

3.9.2.16 c_1(k)*k^2 - c_1(m)*m^2 = u(m) - u(k)

3.9.2.17 c_2(k)*k^2 - c_2(m)*m^2 = u(m) - u(k)

3.9.2.18 c_3(k)*k^2 - c_3(m)*m^2 = u(m) - u(k)

Since each root u(m) and u(k) is either +1 or -1, there are four combinations for their difference given by u(m) - u(k) on the rhs of the above equations.

3.9.2.19 c_0(k)*k^2 - c_0(m)*m^2 = 0

3.9.2.20 c_1(k)*k^2 - c_1(m)*m^2 = -2

3.9.2.21 c_2(k)*k^2 - c_2(m)*m^2 = +2

3.9.2.22 c_3(k)*k^2 - c_3(m)*m^2 = 0

In fact, since u(m) - u(k) = -(u(k) - u(m)), and all u(k) and u(m) are restricted to +/-1 only, only half the equations are actually unique. For instance, (3.9.2.20) is the negative equivalent of (3.9.2.21) where the constants linking the two equations are givenby c_2(k) = -c_1(k) and c_2(m) = -c_1(m). Similarly, the two equations (3.9.2.19) and (3.9.2.22) are identical since -0 = +0. Solving (3.9.2.19) we get

3.9.2.23 c_0(k)*k^2 = c_0(m)*m^2

Which gives, for co-prime factors k and m, arbitrary integer l,

3.9.2.24 c_0(k) = l*m^2

3.9.2.25 c_0(m) = l*k^2

Since equations (3.9.2.19) and (3.9.2.22) are identical, we get for c_3(k) and c_3(m)

3.9.2.26 c_3(k) = c_0(k)

3.9.2.27 c_3(m) = c_0(m)

Inserting for c(0)k from (3.9.2.24) into (3.9.2.7) we get the zero'th order Unity Root

3.9.2.28 u_0 = u(k) + l*(km)^2

We would get the same result for u_0 if we had inserted for c(0)m from (3.9.2.25) into (3.9.2.8).

With u(k) = +1 we see that u_0 is the familiar unity, Unity Root (mod a^2). Using equation (3.9.2.3) we get

3.9.2.29 u_0 = +1 + l*a^2

With u(k) = -1 we get the conjugate unity, Unity Root (mod a^2). This expression can be thought of as also deriving from the duplicated equation for c_3(k) and c_3(m), see (3.9.2.22).

3.9.2.30 u_0 = -1 + l*a^2

What about the other two, non -trivial, i.e. non-unity, Unity Roots given by solving equation (3.9.2.20) and (3.9.2.21). Firstly, as prior mentioned, we need only solve one of them, say the first one (3.9.2.20). Doing this will give us c_1(k) and c_1(m). If we multiply (3.9.2.21) by -1, we see that

3.9.2.31 c_2(k) = -c_1(k)

3.9.2.32 c_2(m) = -c_1(m)

We have to be slightly careful here in that if we want positive roots we have to put either c_1(k) and c_1(m) or c_2(k) and c_2(m) in the more general solution form. Assuming c_1(k) and c_1(m) are positive then c_2(k) and c_2(m) are adjusted as follows, for arbitrary integers s and t.

3.9.2.33 c_2(k) = -c_1(k) + s*m^2

3.9.2.34 c_2(m) = -c_1(m) + t*k^2

We get c_1(k) and c_1(m) by solving the LDE (3.9.2.20) and, in doing so, we have now determined all eight constants, c_0(k), c_0(m) to c_3(k), c_3(m) as specified in equations (3.9.2.7) to (3.9.2.14).

Of course, this method generalises to any number of unique prime factors and not just two as specified above.

The fact that we can derive the upper-half constants c_2, c_3, from the negative of the lower-half c_0 and c_1, also reduces the number of LDEs from n^2 to actually n^2 / 2, i.e. from 4 to 2 in the Pythagorean case.

Section (3.8.2) showed that the constants c(k), c(m) can be obtained by solution of a LDE if the Unity Roots of the prime factors are known. Of course they are always +/- 1 for n = 2 so there is no problem in computing c(k) and c(m).

Having established the form of the roots for prime or composite base, the main aim of this section is to show that for composite base, if (b,c) is a Candidate Pair, (mod a^2), such that b maps to c via a Unity Root u, then the Unity Root u is of the negative form for one or more of the prime factors k but not for all prime factors.

3.9.3 Theorem: Pythagoras Negative Unity Root Mapping

If the base a is composite with m unique prime factors k_0, k_1, k_2, ... k_r ... k_(m-1), 0 <= r < m, i.e. a is factored as

3.9.3.1 a = k_1*k_2* ... k_r^2 ... k_(m-1)

and (b,c) is a Candidate Pair such that b maps to c via the Unity Root u, i.e.

3.9.3.2 c = u*b (mod a^2)

then the Unity Root u is of the 'negative form' (explained shortly) for one or more of the prime factors k but not for all prime factors.

A Unity Root u (mod a^2), of a composite base a, is considered of the 'negative form' when it is expressed using the negative unity root u(k_r) of the r'th prime factor k_r of the base a (3.9.3.1), i.e. with u(k_r) given by

3.9.3.3 u(k_r) = -1

then the negative form of the Unity Root u, as in (3.9.3.2), expressed using u(k_r) is given by

3.9.3.4 $u = u(k\_r) + c(k\_r)*k\_r\text{^}2$

Proof

If we look back at equations (3.9.2.15) to (3.9.2.18) for the case of two unique, prime factors k and m, we had four possible combinations for forming the sum u(m) - u(k), given for each prime factor there were two roots, +1 or -1, i.e.

3.9.3.5 $U(m) = \{+1, -1\}$

3.9.3.6 $U(k) = \{+1, -1\}$

and the four possible differences are given by

3.9.3.7 $U(m) - U(k) = \{0, -2, +2, 0\}$

Of the four combinations, the +2 and 0 resultant is a linear (-1 factor) combination of the -2 and 0 solutions. Thus there were in fact only 2^2 / 2 linearly independent combinations.

For m unique prime factors, k_r, 0 <= r < m, the number of linearly independent combinations grows exponentially as 2^(m - 1). Nevertheless, there is only one case whereby the Unity Root u is a combination of only positive Unity Roots for each of the factors, i.e.

3.9.3.8 $u(k\_r) = +1 \text{ for } 0 <= r < m$

In such a case, the Unity root of the composite can be written in any one of the following m different forms for each of the m prime factors k_0 to k_(m-1).

3.9.3.9 $u = +1 + c(k\_0)*k\_0\text{^}2$

$u = +1 + c(k\_1)*k\_1\text{^}2$

.

.

.

$u = +1 + c(k\_r)*k\_r\text{^}2$

.

.

.

$u = +1 + c(k\_(m - 1))*k\_(m - 1)\text{^}2$

If we equate any pair of equations in (3.9.3.9), for example the equations for factor k_0 and k_r, we get the equation

3.9.3.10 c(k_0)*k_0^2 - c(k_r)*k_r^2 = 0

which, since all the factors are co-prime, has the general solution, for arbitrary integer l,

3.9.3.11 c(k_0) = l*k_r^2 = 0

3.9.3.12 c(k_r) = l*k_0^2 = 0

Equating any pair of terms in (3.9.3.9) will give a zero on the rhs as the +1 Unity Root always cancels to leave 0. Thus, every one of the equations is similar and there is only one consistent, general solution for the r'th constant c(k_r), arbitrary integer l, given by

3.9.3.13 c(k_r) = l*(k_1^2*k_2^2* ... k_r^2 ... k_(m - 1)^2) / k_r^2

i.e. c(k_r) is the continued product of the squares of all the prime factors k_r, 0 <= r < n excepting the factor k_r.

This then gives for the solution for the Unity Root u of the composite a, as

3.9.3.14 u = +1 + l*(k_1^2*k_2^2* ... k_r^2 ... k_(m - 1)^2)

which, by the definition of the composite base a (3.9.3.1), is just

3.9.3.15 u = +1 + l*a^2

For any value l other than l = 0 this gives non-primitive Unity Roots, i.e. | u | > a^2 and outside of the [0,a^2) interval. Thus we find that the Unity Root +1 for the composite base is comprised of the +1 Unity Roots of all its factors.

If we do a similar analysis for the conjugate Unity Roots, u(k_r), for all the m factors k_r, 0 <= r < m, i.e.

3.9.3.16 u(k_r) = -1 for 0 <= r < m

we will arrive at the solution

3.9.3.17 u = -1 + l*a^2

i.e. the negative Unity Roots for the prime factors combine to give the negative Unity Root of the composite.

Generalising these two special cases where all the Unity Roots of the factors are either +1 or -1, equation (3.9.3.4) expands, for 0 <= r < m, into the following m equations, for each particular Unity Root u,

3.9.3.18 u = u(k_0) + c(k_0)*k_0^2
u = u(k_1) + c(k_1)*k_1^2
.
.
.
u = u(k_r) + c(k_r)*k_r^2
.
.
.
u = +(k_(n - 1) + c(k_(m - 1))*k_(m - 1)^2

For the trivial Unity Root, u = +1, we set all u(k_r) = +1, 0 <= r < m. Likewise for the conjugate unity Unity Root, u = -1, we set all u(k_r) = -1. In between these two extremes, all other m^2 - 2 Unity Roots u will be obtained from some combination whereby at least one of the Unity Roots of the factors u(k_r) is different to the others. i.e. if m - 1 of the factor roots u(k_r) are all +1 then the m'th factor root u(k_(m - 1)) must be -1.

As per Theorem (3.9.1.3), the u = +1 root for composite a cannot be a solution since, by (3.9.3.2), we would have

3.9.3.19 c = b (mod a^2)

Lastly, since u = +1 is the only case when all the factor roots are also +1, any other root u, which maps b to c (mod a^2) must always be expressible in terms of at least one negative Unity Root, -1, of one or more of its prime factors.

3.9.3.20 What does this Theorem mean physically?

Referring back to the same question (3.9.1.3.2) for prime base, Theorem (3.9.1.3), it means that there is at least one prime factor k such that, when examining a residue sequence (mod k^2), there will be symmetry in the residue sequence about the mid-point k^2 / 2 (more generally any point l*k^2 / 2, integer l, see Example (3.9.4)) such that the value c is a mirror image of b about this symmetry point. Note, the mid-point is always given by (c + b) / 2.

For one or more prime factors, k, the mid-point, (c + b) / 2 of the Candidate Pair (b,c) (mod a^2), is a symmetry point of the residue sequence, (mod k^2), occurring at a point l*k^2 / 2 for some integer l. Where this is the case, the value b maps to c via the negative Unity Root, u(k) = -1 (mod k^2), of the prime factor k. Conversely, the residue sequence will NOT be symmetric about the mid-point if the value b maps to c via the positive Unity Root, u(k) = +1 (mod k^2).

This does not mean to say there is no onbvious symmetry in the residue sequence (mod k^2) for those factors k where the Unity Root u(k) is +1. However, the residues about the mid-point will not appear symmetric when u(k) = +1. The following Example (3.9.4) will illustrate this.

The above remarks apply to even exponent and, in particular, the Pythagorean case. Indeed, we have prior shown in section (2.4.4) that this point symmetry can reproduce all the Pythagorean triples.

In the case of odd exponent, whilst there is always a negative Unity Root, arguments presented in section (2.5) show that this negative Unity Root mapping cannot produce an FLT counter-example because it leads to a quotient sum greater than 2, see equation (2.5.1.14). Nevertheless, odd exponents can produce positive Unity Roots that can still map a value b to a value c such that b and c are relatively close. By 'relatively' we mean that the root gap, c - b is less than the base a and consequently such a Candidate Pair (b,c) might meet the Quotient Condition, Theorem (1.12).

3.9.4 Example

A good example of composite base is the Pythagorean triple (20, 21, 29)

Both the lowest value (a = 20) and the middle value (b = 21) are composite. We shall start by looking at the standard residue table for the base a = 20, modulus 20^2, Candidate pair (b,c) = [21,29].

3.9.4.1 a = 20, b = 21, c = 29

We shall split the base into the co-prime factors 4 and 5.

3.9.4.2 k_0 = 4

3.9.4.3 k_1 = 5

Of course, 4 is not actually prime. Nevertheless, it does comprise only one unique prime factor and, especially when counting Unity Roots for arbirtrary even base, can be regarded as a prime factor. This is because, like any prime base, it only has two roots in the Minimal Residue Sequence since 2 is its only factor and 2 also divides the exponent (n=2) - hence a Minimal Residue Sequence. The two roots in this Minimal Residue Sequence, are +1 and +7, section (3.5.8). The other key point is that 4 is co-prime to the other factor 5.

The Unity Roots of the composite base a = 20 and its factors k_0 and k_1 are as follows

3.9.4.4 U(20) = {+1, 49, 151, 199, 201, 249, 351, -1 }

3.9.4.5 U(4) = {+1, 7, 9, -1}

3.9.4.6 U(5) = {+1, -1}

[A point of note is that the exponent, n = 2, divides the base and thus the Minimal Residue Sequence size is actually (20^2) / 2, i.e. 200, although all the Unity Roots have been listed between 0 < u <20^2. Similarly, for the factor 4, the Minimal Residue Sequence size is actually (4^2) / 2, i.e. 8, although all the Unity Roots have been listed between 0 < u < 4^2. This is intentional to avoid extra complication and keep things simple. If we used only the roots in the Minimal Residue Sequence we would actually have to use a reduced modulus of 20^2 / 2 for u(20) and a reduced modulus of 4^2 / 2 for u(8). As an example, if b = 21, c = 29 and c = u(20)*b (mod 20^2) then u(20) = 249. The value u(20) = 249 is outside of the Minimal Residue Sequence since it is greater than 20^2 / 2. However, the equivalent root within the Minimal Residue Sequence is 49 = 249 mod 20^2 / 2. Using this root we also find c = u*b (mod 20^2 / 2) but c != u*b (mod 20^2). i.e. we have to consistently use a reduced modulus, the size of the Minimal Residue Sequence, when working only with roots in the Minimal Residue Sequence].

Ignoring the two trivial Unity Roots +1 and -1 (-1 = 399 mod 20^2), the non-trivial, Unity Roots U(20), in terms of the factor roots u(4) and u(5) are

3.9.4.7 U(20) = { 49, 151, 199, 201, 249, 351 }

and each root expands as follows

3.9.4.8 49 = +1 + 3*4^2
49 = -1 + 2*5^2

151 = +7 + 9*4^2
151 = +1 + 2*5^2

199 = +7 + 12*4^2
199 = -1 + 8*5^2

201 = +9 + 12*4^2
201 = +1 + 8*5^2

249 = +9 + 15*4^2
249 = -1 + 10*5^2

351 = -1 + 16*4^2
351 = +1 + 14*5^2

The Unity Root u(20) that maps b = 21 to c = 29 is u(20) = 249, i.e.

3.9.4.9 29 = 249*21 (mod 20^2)

And, by (3.9.4.8),

3.9.4.10 $249 = -1 \pmod{5^2}$

So that the Unity Root u(20) is in the negative form with regard to the Unity Root u(5) of its factor k_1 = 5 since u(5) = -1 for u(20) in (3.9.4.8).

3.9.4.11 $29 = -1*21 \pmod{5^2}$

Examining the residue table (mod 5^2), given below, for the factor k_1 = 5, we see that the residue sequence is symmetric about the mid-point (29+21) / 2 (= 25).

Residue Table a = 5, n = 2

x	x^n	residue r (mod a^n)	residue quotient (mod a)	p
0	0	0	0	0
1	1	1	1	0
2	4	4	4	0
.				
.				
19	361	11	1	14
20	400	0	0	16
21	441	16	1	17
22	484	9	4	19
23	529	4	4	21
24	576	1	1	23
25	625	0	0	25
26	676	1	1	27
27	729	4	4	29
28	784	9	4	31
29	841	16	1	33
30	900	0	0	36
31	961	11	1	38

We see that entries for x = 21 and x = 29 have an identical residue (= 16) and thus (21,29) is a Candidate Pair (mod 5^2). Since the symmetry point is at x = 25, the value x = 29 represents a flip of the point x = 21 about this symmetry point, i.e. 29 is a mirror image of 21.

We confirm that there is a Pythagorean triple to be found for the Candidate Pair (21,29) by expanding 21^2 and 29^2 in quotient, remainder form

3.9.4.12 $21^2 = 17*5^2 + 16$

3.9.4.13 $29^2 = 33*5^2 + 16$

Subtracting 21^2 from 29^2 gives

3.9.4.14 29^2 - 21^2 = 16*5^2

and we see that the Quotient Gap is 16 i.e. a perfect square (= 4^2), i.e.

3.9.4.15 29^2 - 21^2 = 20^2

and we get the Pythagorean triple (20, 21, 29).

If we now examine the other factor k_0 (= 4), we see from (3.9.4.8) that u(4) = +1 for u(20) = 249 i.e. u(20) is only in the positive form for the factor u(4) unlike k_1 (= 5) which is in the negative form since u(5) = -1. If we look at the residue table (mod 4^2) for k_0, given below, although not easy to see, the residues about the same mid-point (29+21) / 2 (= 25) are not symmetric. The symmetry is actually slightly off centre at the point x = 24. However, no matter how small the offset, it destroys the symmetry at the mid-point.

Residue Table a = 4, n = 2

x	x^n	residue r (mod a)^n	residue quotient (mod a)	p
0	0	0	0	0
1	1	1	1	0
2	4	4	0	0
.				
.				
19	361	9	1	22
20	400	0	0	25
21	441	9	1	27
22	484	4	0	30
23	529	1	1	33
24	576	0	0	36
25	625	1	1	39
26	676	4	0	42
27	729	9	1	45
28	784	0	0	49
29	841	9	1	52
30	900	4	0	56
31	961	1	1	60

We see therefore that Theorem (3.9.3) is confirmed in this example since the symmetry only exists about the mid-point for the factor k_1 (= 5) where u(5) = -1 for u(20) = 249 but the symmetry does not exist for the factor k_4 (= 4). That is, u(20) is in the negative form with regard to the factor k_1 but in the positive form with regard to the factor k_0.

We shall now examine the dual case of this example, i.e. where the base is the composite, middle value b = 21, modulus 21^2, with dual Candidate Pair (a,c) = (20,29).

3.9.4.16 b = 21

a = 20
c = 29

The base b factors into the two unique prime factors 3 and 7

3.9.4.17 k_0 = 3

3.9.4.18 k_1 = 7

The Unity Roots of the composite b, k_0 and k_1 are

3.9.4.19 U(21) = {1, 197, 244, 440 }

3.9.4.20 U(7) = {1, 48}

3.9.4.21 U(3) = {1, 8}

Ignoring the two trivial Unity Roots +1 and -1 (-1 = 440 (mod 21^2)), the non-trivial, Unity Roots u(21), in terms of the factor roots u(3) and u(7), are

3.9.4.22 197 = -1 + 22*3^2

197 = +1 + 4*7^2
244 = +1 + 27*3^2
244 = -1 + 5*7^2

The Unity Root u(21) that maps a = 20 to c = 29 is u(21) = 244, i.e.

3.9.4.23 29 = 244*20 (mod 21^2)

And, by (3.9.4.22),

3.9.4.24 244 = -1 (mod 7^2)

So that the Unity Root u(7) that maps a = 20 to c = 29 is u(7) = -1, i.e. in the negative from, which is confirmed since

3.9.4.25 29 = -1*20 (mod 7^2)

Examining the residue table (mod 7^2), given below, for the factor k_1 = 7 we see that the residue sequence is symmetric about the mid-point (29 + 20) / 2 (= 24.5) and that the residues for a = 20 and c = 29 are symmetric about this point.

Residue Table a = 7, n = 2

x	x^n	residue r (mod a)^n	residue quotient (mod a)	p
0	0	0	0	0
1	1	1	1	0
2	4	4	4	0
.				
.				
.				
19	361	18	4	7
20	400	8	1	8
21	441	0	0	9
22	484	43	1	9
23	529	39	4	10
24	576	37	2	11
25	625	37	2	12
26	676	39	4	13
27	729	43	1	14
28	784	0	0	16
29	841	8	1	17
30	900	18	4	18
.				
.				
.				
47	2209	4	4	45
48	2304	1	1	47
49	2401	0	0	49

In quotient and remainder form the a and c values are

3.9.4.26 20^2 = 8*7^2 + 8

3.9.4.27 29^2 = 17*7^2 + 8

and subtracting 20^2 from 29^2

3.9.4.28 21^2 - 20^2 = 9*7^2

we see the Quotient Gap is 9, i.e. a perfect square (= 3^2)

3.9.4.29 29^2 - 20^2 = 21^2

and we get the Pythagorean triple (21, 20, 29)

On the other hand, if we look at the residue table for the other factor k_0 = 3, i.e. residue table (mod 3^2) we see that the residue sequence is not symmetric about the mid point 24.5.

Residue Table a = 3, n = 2

x	x^n	residue r (mod a)^n	residue quotient (mod a)	p
0	0	0	0	0
1	1	1	1	0
2	4	4	1	0
19	361	1	1	40
20	400	4	1	44
21	441	0	0	49
22	484	7	1	53
23	529	7	1	58
24	576	0	0	64
25	625	4	1	69
26	676	1	1	75
27	729	0	0	81
28	784	1	1	87
29	841	4	1	93
30	900	0	0	100
34	1156	4	1	128
35	1225	1	1	136
36	1296	0	0	144

Theorem (3.9.3) is thus confirmed since the symmetry only exists about the mid-point for the factor k_1 (= 7) where u(7) = -1 for u(21) = 244 but the symmetry does not exist for the factor k_0 (= 3) where u(3) = +1. That is, u(21) is in the negative form with regard to the factor k_1 but in the positive form with regard to the factor k_0.

Generally speaking, the symmetry that exists for one factor, but not another, is no surprise since we are trying to equate a symmetry point (k_0^2 / 2) of a factor k_0 with the symmetry point (k_1^2 / 2) of a co-prime factor k_1. For instance, in this later example, trying to equate symmetry ppoints for each factor is equivalent to solving, for integers s and t, the following LDE

3.9.4.30 s*7^2 / 2 = t*(3^2) / 2

This does have a general solution for some integer l, l != 0, s = l*7^2 / 2, t = l*3^2 / 2, but the mid-point is then l*21^2 / 3 which is, of course, outside of the range of [20,29].

3.10 Summary of Conditions

This section gives a summary of all the conditions and constraints developed in this section (3) on a triplet (a, b, c), were it to be a an FLT counter-example.

If ‘u(a)’ is a Unity Root (mod a^n), as defined by (3.1.1), then the values b and c of a candidate pair (b,c) (mod a^n) are such that

3.10.1 c = u(a)*b (mod a^n)

In the Dual case, if ‘u(b)’ is a Unity Root (mod b^n) then the values a and c of a Dual candidate pair (a,c) (mod b^n) are such that

3.10.2 c = u(b)*a (mod b^n)

In the Skew-symmetric case, for odd exponent, Section (2.5.1), if ‘u(c)’ is a negative Unity Root (mod c^n), such that u(c)^n = -1 (mod c^n), then the values a and b of the Skew Candidate Pair (a,b) (mod c^n) are such that

3.10.3 b = -u(c)*a (mod c^n)

[Note that negative Unity Roots have not been specifically discussed in this paper because, for odd exponent, they are trivially the negative equivalents of the positive +1 Unity Roots and the theory behind them remains the same].

By arguments in (3.4.6), if u(a) is a Unity Root (mod a^n) then

3.10.4 u(a) > a

This constraint is also valid in the Dual case for Unity Root u(b), (mod b^n)

It is conjectured (3.6.15) that the minimum value of a Unity Root ‘Umin(a)’, (mod a^n) is given greater than or equal to the (n - 1)’th root of the modulus a^n

3.10.4.1 Umin(a) >= (n - 1)_/a^n

This conjecture is also valid in the Dual case for Unity Root Umin(b), (mod b^n)

Using the definition of the Winding Number ‘w’ (3.4.4), and by arguments in (3.4.6) concerning the Root Gap, if (b,c) is a Candidate Pair (mod a^n) then the Winding Number is greater than zero

3.10.5 $w > 0$

A non-trivial, Unity Root u(A), to any modulus A, such that u(A)^n = 1 (mod A), is a root to the following congruence for the Cyclotomic, 'Unity Root Polynomial' f(u(A)) (3.6.4) such that

3.10.6 $f(u(A)) = 0 \pmod{A}$

If the modulus A is a multiple of a perfect power of the base a, i.e. A = k*a^n, for integer k, k > 0, then we denote f(u(a)), exponent n, by 'f(u(a))n' and re-write (3.10.6) as

3.10.7 $f(u(a))n = 0 \pmod{a^n}$

This constraint is also valid in the Dual case for Unity Root u(b), (mod b^n)

In the special, cubic exponent case we have, by Theorem (3.6.14), an exact equation

3.10.8 $1 + u + u^2 = a^n$

This equation is also valid in the Dual case for Unity Root u(b), (mod b^n)

4 Miscellaneous

This section comprises miscellaneous applications arising from the work presented in sections (1) to (3). The topics are not central to the main work which is predominantly about the structure of Residue Sequences and their impact upon Pythagoras and FLT. Nevertheless, hopefully the topics in this section provide an interesting diversion for the readers.

4.1 Polynomial Factorisation

An early and falacious proof of FLT was submitted by Gabriel Lame' in 1847 to The Paris Academy. Essentially, it was based upon the factorisation of the FLT equation as follows, where q is an n'th root of unity and generally complex.

4.1.1 q^n - 1 = 0

and

4.1.2 c^n - b^n = (c - q^0*b)(c - q^1*b)(c - q^2*b)...(c - q^(n - 1)*b)

[Note that the first factor (c - q^0*b) = (c - b) and the second factor (c - q^1*b) = (c - qb) where q^0 = 1 is the trivial, unity Unity Root and q^1 = q, the smallest, non-trivial Unity Root].

The Lame' proof asserted that the bracketed terms on the rhs in (4.1.2) are co-prime to each other and, therefore, each had to be a perfect n'th power if the entire rhs was to be a perfect power, i.e. a^n. The proof was doomed in so much as the factorisation was assumed unique in the ring of cyclotomic integers, which it isn't for certain prime exponent termed irregular primes (Kummer 1849). However such irregular promes are relatively rare. For example, there are only eight irregular primes less than 160 which are {37, 59, 67, 101, 103, 131, 149, 157}.

History aside, using the isomorphism between the complex n'th roots of unity and Unity Roots (mod a^n), a similar factorisation can be performed using Unity Roots u, (mod a^n).

4.1.3 c^n - b^n = (c - u^0*b)(c - u^1*b)(c - u^2*b)...(c - u^(n - 1)*b) (mod a^n)

If b and c meet the Residue Condition (1.2.3) then

4.1.4 c^n - b^n = 0 (mod a^n)

and therefore, using the expansion in (4.1.3) and letting u^0 = 1, u^1 = u, we obtain

4.1.5 (c - b)(c - u*b)(c - u^2*b)...(c - u^(n - 1)*b) = 0 (mod a^n)

The factorisation on the lhs of (4.1.5) pre-supposes that there are n Unity Roots (mod a^n) which, for odd, prime exponent, is true if a is prime of the 2ln+1 form or a is composite with one or more prime factors of the 2ln+1 form.

From what has been said before, (4.1.5) is a necessary but not sufficient condition for the triple (a, b, c) to be an FLT counter-example. Since it is a congruence, the lhs can equal any multiple l of a^n. Sufficiency derives from the additional Quotient Condition (1.4.3) which states that the multiple l must be 1.

The polynomial expansion (4.1.5) could also be deduced, rather than derived by analogy with (4.1.2), by considering the roots of (4.1.2) - which is the method one might use when factoring an arbitrary polynomial.

We know immediately that b = c is a root of (4.1.2) and hence (c - b) is a factor. Furthermore, by the arguments given on Unity Root Mappings in section (3.4), we know that if c = u*b (mod a^n) then c^n = b^n (mod a^n). Hence,
(c - u*b) = 0 (mod a^n) and thus (c - u*b) is a factor of (4.1.5). Similarly, since the entire set of Unity Roots is U = {u, u^2, .. u^(n - 1)}, then (c - u^2*b) is also a factor and, in general, (c - u^r*b) is a factor for 0 <= r < n. Hence we get n factors in total and the polynomial congruence c^n - b^n (mod a^n) factors as in (1.14.2). Of course, without the congruence condition, one has to revert back to using the n'th roots of unity denoted by q in (4.1.1).

4.1.6 Example

Let

n = 3 and a = 7

then the smallest, non-trivial Unity Root u is

u =18

By (4.1.3), the polynomial c^n - b^n factors as follows

c^3 - b^3 = (c - b)(c - 18*b)(c - 18^2*b) (mod 7^3)

and to meet the Residue Condition

c^3 - b^3 = 0 (mod a^n)

which, upon expansion in terms of Unity Roots, becomes

(c - b)(c - 18*b)(c - 18^2*b) = 0 (mod a^n)

If we convert (4.1.5) from a congruence back to an equation we get, for integer l,

4.1.7 (c - b)(c - u*b)(c - u^2*b)...(c - u^(n - 1)*b) = l*a^n

As mentioned, if l = 1 we have met the Quotient Condition and the triple (a, b, c) is an FLT counter-example. So too if l is a perfect power, i.e. l = k^n, then the triple (ka, b, c) is an FLT counter-example.

Firstly, if n = 2, (4.1.7) reduces to

4.1.8 (c - b)(c - u*b) = l*a^2

Here we see that if u = -1 then (4.1.8) becomes

4.1.9 (c - b)(c + b) = l*a^2

and expanding the brackets on the lhs gives

4.1.10 c^2 - b^2 = l*a^2

This confirms the findings in section (3.9) on Pythagoras and Unity Root mappings that it is only the negative Unity Root (u = -1) that is responsible for generating Candidate Pairs in solutions to the Pythagoras Equation, i.e.

4.1.11 c = -1 * b (mod a^2)

This may seem obvious since, if the Unity Root were to be positive, then c and b would be equal since c = u*b (mod a^2). However, the general solution for a positive root b is actually c = k*a^2 + b for integer k, k >= 0, so it is not a foregone conclusion that a form of u = +1 cannot be used for the mapping of b to c.

If a is prime in (18.1.10) then, since (c - b) != (c + b) except when c and b are identically zero, by prime factorisation we are forced to conclude that either

4.1.12 c - b = +l

and

4.1.13 c + b = a^2

or, for integer s, t, s >= 1, t > s, subject to the condition

4.1.14 l = s*t

then each bracketed term is of the general form

4.1.15 (c - b) = s*a

4.1.16 (c + b) = t*a

The above solutions apply to the general Diophantine equation (4.1.10) where l is not presumed unity. To avoid any contradictions between (4.1.15) and (4.1.16) notice that t > s. Since s >= 1, t >= 2 so, invariably, l >= 2.

Without dwelling further on Pythagorean triples, the only values for s and t which lead to valid solutions, are either

4.1.17 l = +1, c - b = +1, c + b = k^2, prime a, c^2 - b^2 = a^2

or, for l >= 4, integer k, k >= 2

4.1.18 l >= 4, s = 1, t = k^2, l = k^2 and so c^2 - b^2 = (ka)^2

The real motivation for studying the factorisation of (4.1.7) is that it gives us a way to study the value of l. If we refer back to section (2.2.5) on the Generalised Fermat Equation we mentioned 'k' values, equation (2.5.5.4). The l value in (4.1.7) above is similar and it would be nice to look at the possible values that occur.

Referring back to equation (4.1.8), which is essentially a Generalised Pythagoras Equation, for prime a, the factor (c - b) has to be unity by Theorem (1.14). It then meant that the other bracket (c - u*b) is a multiple of a^2. Indeed, since c = u*b (mod a^n), c - u*b = l*a^n.

If we suppose a is prime then we have (c - b) = 1 and equation (4.1.7) then becomes

4.1.19 (c - u*b)(c - u^2*b)...(c - u^(n - 1)*b) = l*a^n

If we refer back to the general n'th order congruence (4.1.5) then only one factor, call it the r'th factor (c - u^r*b), where 0 < r < n, can satisfy the congruence

4.1.20 (c - u^r*b) = 0 (mod a^n)

This is the same as saying there are no repeated roots.

We can also derive a similar expression to (4.1.19) for a^n + b^n. If we swap c with a, such that the Unity Roots are now defined as,

4.1.21 $u^n = 1 \bmod c^n$

and replace b with -b then, for odd exponent only, we can re-write (4.1.3) as

4.1.22 $a^n + b^n = (a + u^0*b)(a + u^1*b)(a + u^2*b)...(a + u^(n - 1)*b) \bmod c^n$

and therefore, for integer l, l >0

4.1.23 $(a + u^0*b)(a + u^1*b)(a + u^2*b)...(a + u^(n - 1)*b) = l*c^n$

Because the original congruence (4.1.5) is precisely a congruence relation, and not an exact equation, the further development of this factorisation in terms of integral unity roots has not been developed further and the Authors have left its study outstanding. No current reference to external work on the matter is currently known but that's not to say there isn't any!

4.2 Consecutive Identical Residues

Section (1.11) defined the pair of integer values b and c as 'Consecutive Identical Residues' if they are such that they form a Candidate Pair satisfying the relation

4.2.1 $c - b = 1$

The term 'Consecutive' follows because c is the next integer after b, for positive b, and that since (b,c) form a Candidate Pair, by definition, they have identical residues (mod a^n).

Consecutive Identical Residues are important since Theorem (1.14) proves that if the base a is prime then the Candidate Pair must have a Root Gap of unity as per (1.10.1) hence also (4.2.1) above.

In other words, if we are studying a prime base a, odd exponent, modulus a^n then any potential FLT counter-example (a, b, c) would be such that the values b and c are Consecutive Identical Residues. Thus, in principle, if we could prove there are no such Consecutive Identical Residues, we could dismiss all prime bases as giving rise to FLT counter-examples and this would prove FLT for any exponent, prime base a. Alas, Consecutive Identical Residues do exist, except they are scarce, see Observation (4.2.2.1) below. So the future challenge lies in proving that although Consecutive Identical Residues exist they are always such that the b value is greater than Bmax,

see Theorem (1.19.1). In experimental data this is confirmed. Indeed, Consecutive Identical Residues seem to have a b value much greater than Bmax.

For even exponent, odd base a, the symmetry in the residue sequence gives rise to numerous Consecutive Identical Residues. At its simplest level, if a is odd prime, for exponent n = 2, there is a symmetry point at the half integer point given by (a^2) / 2. Because the point is half-integral, the two integer values either side are consecutive, i.e. if b is the lower value, then b + 1 is the upper value. If the base is even there is still a symmetry point at a^2 / 2 but it is now integral and there is effectively one central value. The two integers either side of this are separated by a gap of 2 and are hence not consecutive.

Nevertheless, an even valued base also has symmetry within the Minimal Residue Sequence (2.1.2.2) and, if one can factor out an odd factor k, point symmetry about a half integral point k^2 / 2 can be found for at least one odd prime factor, see section (3.9.2). That said, Consecutive Identical Residues are only a necessity for odd, prime base and so to get into a discussion on the symmetry of a composite base, when talking about Consecutive Identical Residues, is irrelevant. Suffice to say, numbers such as a = 2^m, integer m, m >= 2, have no odd, prime factor and therefore they have no half-integral symmetry point. Nevertheless, there still exists a Pythagorean triple for every such number. This is simply because, being composite, they do not require Candidate Pairs to be consecutive. Pythagorean triples with a Consecutive Identical Residue, although common (at least one triple for every prime), they are a mere subset of all the Pythagorean triples, most having a Root Gap (c - b) much greater than 1.

4.2.2 Observations

Our own theoretical analysis of Consecutive Identical Residues is little developed and none of it published.

Nevertheless, we have made several observations that are summarised here:

4.2.2.1 The number of Consecutive Identical Residues, 'Nc', for odd exponent n, prime base a, is given by

4.2.2.2 Nc = (n - 1)

Since Nc is even, when n is odd, there are actually only half this number that are independent. Every Consecutive Identical Residue (b,c) is accompanied by its conjugate [a^n - b, a^n - c].

Thus, for n = 3, there is only one unique Consecutive Identical Residue, See (4.2.2.3) below.

4.2.2.3 If u is a Unity Root (mod a^n) and b and c are Consecutive Identical Residues then b maps to c via a Unity Root u

4.2.2.4 $c = u*b \pmod{a^n}$

Since, by the definition of a Consecutive Identical Residue,

4.2.2.5 $c = b + 1$

then substituting for b from (4.2.2.5) into (4.2.2.4) and converting from a congruence to an equation, for some integer l, we obtain a LDE in the two unknowns, b and l.

4.2.2.6 $(u - 1)*b + l*a^n = 1$

Since this LDE is soluble, if (u - 1) and a^n are co-prime, it implies we can find Consecutive Identical Residues given the Unity Root. Studying Consecutive Identical Residues thus becomes, once again, a problem in understanding Unity Roots.

Taking a specific example

4.2.2.7 $n = 3, a = 7, u = 18$

and substituting for n, a and u, we get the LDE

4.2.2.8 $17*b + l*343 = 1$

Which gives the solution

4.2.2.9 $b = 222, l = 11$

We thus get a Consecutive Identical Residue, Candidate Pair (b,c)

4.2.2.10 $b = 222, c = 223$

and another pair, conjugate to this pair, is

4.2.2.11 $b = 120, c = 121$

Verifying with a computer shows that these are the only two occurrences of a Consecutive Identical Residue for the n = 3, a = 7 case and only one of these is

independent. We usually take the smaller of the two, namely the Candidate Pair [120,121].

Another cubic example

4.2.2.12 n = 3, a = 13, u =1036

and substituting for n, a and u, we get the LDE

4.2.2.13 1035*b + l*2197 = 1

Which gives the solution

4.2.2.14 b = 1851, l = -872

We thus get a Consecutive Identical Residue, Candidate Pair (b,c)

4.2.2.15 b = 1851, c = 1852

and another pair, conjugate to this pair, is

4.2.2.16 b = 345, c = 346

A computer search verifies these two as the only occurrences.

4.3 Modified FLT Equation 'MFLT'

The problem of finding a Candidate Pair is almost trivial and leads to the GFLT equation (1.8.1). However, since FLT is proven, we know that no such Candidate Pairs can also meet the Quotient Condition. Is there any way we can obtain a compromise between far too many GFLT solutions and none when the Quotient Condition is included?

Fortunately there is a compromise and that is to impose two Residue conditions but no Quotient Condition. In other words, retain the Standard Residue Condition (1.2.3) and replace the Quotient Condition (1.4.3) with the Dual Residue Condition (1.17.1)

It has been prior noted in section (1.21) that trying to meet both the Standard Residue Condition (1.2.3) and the Dual Residue condition (1.17.1) is very difficult. In fact, it was rather hoped that this might be impossible and so kill off the FLT problem. Certainly the difficulty in meeting two Residue Conditions seemed impossible as a random scan of Residue Tables revealed no Candidate Pairs. To put the idea on an analytic basis however, a study of which potential Candidate Pairs could meet two

Residue Conditions was made and resulted in a new variant on the FLT equation (1.1.1), tentatively named the ‘Modified FLT equation' (MFLT), given below, for integer k, k>0:

4.3.1 c^n = k*a^n*b^n + a^n + b^n

If the 'k' factor is zero then this reduces to the FLT equation. This equation does actually have solutions.

Due to the volume of work it is generating, its study is to be detailed in a separate paper, as yet unpublished.

4.4 Mersenne Primes

A Mersenne number, 'Mn', integer exponent n, n >= 2, is a number of the form

4.4.1 Mn = 2^n - 1

Section (3.6.16.9.14) came to the known conclusion that if n is composite then Mn is composite. For instance, if the exponent is composite comprising two unique, prime factors k and m, i.e.

4.4.2 n = k*m

then Mn can be factored, for some integer d, as follows

4.4.3 Mn = (2^m - 1)(2k - 1)*d

Therefore, if we wish to test the primality of Mersenne numbers, we need only try testing those where the exponent is prime.

Additionally, from the factor summary in section (3.6.16.11), we can deduce the following:

To test the primality of a Mersenne number Mn, where n is prime, we only need to perform trial division on Mn with all prime numbers of the form 2ln+1, less than or equal to the square root of Mn.

The 'square root' bound on trial factors is standard for any prime test based upon factoring. It hardly needs stating that if a prime factor x is greater than the square root of P and if it divides P then the other factor is less than the square root of P. Of course if P is a perfect square then it is composite.

That trial factors of Mn are of the 2ln+1 form is also a known result; see Mathworld, Ref [4], keyword 'Mersenne Numbers'. Its derivation within this paper is based upon the Unity Root Polynomial and its factor properties.

We can get a quick and quite reasonable approximation for the upper bound of the square root of Mn as follows:

Since the exponent n is odd, let

4.4.4 n = 2m + 1

then

4.4.5 Mn = 2^(2m + 1) - 1

giving the inequality

4.4.6 Mn < 2^(2m + 1)

and taking the square root

4.4.7 _/Mn < 2^m * _ / 2 (the symbol '_/' denotes the square root)

since

4.4.8 _ /2 < 3 / 2

then

4.4.9 _/Mn < 3*2^(m - 1)

Of course, for small n less than approximately 30, we could use a calculator to simply find _/n.

4.4.10 Examples

4.4.10.1 n = 11, M11 = 2047

For M11 we find that _/M11 < 48. Indeed, 48^2 = 2304. In fact _/M11 < 46 so, the list of all trial divisors for M11 comprises all primes of the form 22l + 1 less than 48. This is not a very big list and, in fact, it contains the single prime number 23.This is

quite a remarkable fact that to test the primality of a four digit number, admittedly a very special number 2^11 - 1, we only need one trial divisor, namely 23. Performing the division, we see 2047 = 23*89, i.e. 23 is a divisor of M11. The other prime factor is 89 and, not surprisingly, this is also of the 22l + 1 form, where l = 4.

4.4.10.2 n = 13, M13 = 8191, _/M13 < 96

Primes of the form 26l + 1 less than 96 are 53 and 79 only. None of these two trial divisors is a factor of M13 so we conclude that M13 is prime.

4.4.10.3 n = 17, M17 = 131071, _/M17 < 384

Primes of the form 34l + 1 less than 384 are {103, 137, 239, 307}.

None of these trial divisors is a factor of M17 so we conclude that M17 is prime.

Skipping the prime n=19, for which M19 is also prime, we see in the next example that M23 is composite.

4.4.10.4 n = 23, M23 = 8288607, _/M23 < 3072

The first prime of the form 46l + 1 is 47. This is a factor of M23 and we find that M23 = 47*178481 and M23 is therefore composite. The factor 178481, which is prime, is also of the 46l + 1 form, since 178481 - 1 = 3880*46.

Because of the binary form of a Mersenne Number, primality tests for Mn can be implemented relatively fast on a computer, i.e. relatively fast when compared with the primality testing of an arbitrary prime number. Because of this binary advantage, the search for the largest Mersenne Prime is a continual worldwide project. The published work on Mersenne Numbers is huge and, as a starting point, readers are referred to GIMPS 'The Great Internet Mersenne Prime Search', search the Web for this.

For the layman, a relatively short but informative description can be found in [8]. This book also gives algorithmic details (but not the mathematics) of the 'Lucas Lehmer' primality test for Mersenne primes.

4.5 A Primality Test 'MFST'

The primality test we detail here is a variant of the Fermat test based upon Fermat's Little Theorem which we will abbreviate to FST (Fermat's Small Theorem). We have consequently named the test 'Modified FST' and henceforth abbreviated it to MFST.

SEE THE STRONG PSEUDOPRIME PRIMALITY TEST (TBD)

Although MFST is similar to the Fermat test its false alarm rate is better than that of the Fermat test and it also has the potential to reject all Carmichael Numbers.

Section (2.6.11), which discusses the repetition of residues (mod a), asserts that for prime modulus a (we shall use 'p' here), exponent n such that

4.5.1 $p = 2n + 1$

the residue r, (mod p), for any integer value x, $0 < x < p$ given by

4.5.2 $x^n = r \pmod p$

can only be either +1 or -1. Combining (4.5.1) and (4.5.2) we get

4.5.3 $| x^{((p - 1) / 2)} | = 1 \pmod p$

If we wished to test the primality of a candidate number p we could examine the absolute value of the residue |r|, given by (18.6.2), to see if it is unity for all x, $0 < x < p$. If we found a residue |r| not equal to unity we could then dismiss the base p as composite. Conversely, if ALL residues were either +/-1, then we have found a prime.

Obviously, for any large prime, it is not practical to test every value of x. However, at worst, you only need to try at most (p - 1) / 2 values for x since, if $x^n = 1 \pmod a$, then $(p - x)^n = -1 \pmod a$, i.e. if you know the first half residues $0 < x <= (p - 1) / 2$, then you automatically know the 2nd half values $(p - 1) / 2 < x < p$ from the first half values.

Nevertheless, it is still not practical to test this many values for any large prime. However, if we randomly picked an arbitrary value for x then, in general for an arbitrary base a, it is unlikely that the residue r will be exactly +1 or -1. If it is we could then test another x, say x + 1. The residue r for x + 1 is also relatively unlikely to be +1 or -1, the probability both residues are +1 or -1 then diminishes. In fact, computation shows this probability diminishes rapidly. So much so only a couple of tests are needed to reject most composites.

Of course, we haven't put any probabilities on MFST thus far. A complete analysis is outside the scope of this paper and is to be published in a separate paper should the authors not find references to it in previously published work.

Before outlining a procedure to perform the MFST primality test it should be noted that MFST is essentially a variant on the Fermat Test (hence the name we chose for it) with which it will be compared, see further below.

4.5.4 MFST Procedure

MFST can be performed with the following steps. It does assume computer Usage.

4.5.4.1 Pick (guess, construct) a large, prime candidate p.

4.5.4.2 Do a quick trial division check to eliminate simple composites, i.e. those with a prime factor less than say a million.

Let the exponent n be given by (4.5.1), so that by re-arrangement

4.5.4.3 $n = (p - 1) / 2$

Start with x = 2, compute the residue r_2

4.5.4.4 $r_2 = 2^n \pmod p$

If the residue r_2 is not +1 or -1, reject a as composite. Otherwise, try the next value x = 3 and then compute the residue r_3

4.5.4.5 $r_3 = 3^n \pmod p$

If the residue r_3 is not +1 or -1, reject a as composite. Otherwise, try the next value x = 4, compute the residue r_4 etc. Repeat this proceed for the x'th residue r_x etc. for $0<x<a$.

4.5.4.6 $r_x = x^n \pmod p$

As mentioned above, the test only need proceed from x = 2 to x = (p - 1) / 2. In reality, we only need try a few values of x to reject composites. Nevertheless, for an absolute proof, we would need to try all x up to x = (p - 1) / 2. This is just not practical and, just like the Fermat test, an ironclad answer as to a value's primality can only be obtained by employing another test, e.g. ref (TBD).

Nevertheless MFST appears to give, at worst, roughly half the false-alarm rate of FST with which we shall compare some results after a short description of FST. We will also show algebraically that our test is, in fact, a variant on FST but can avoid false alarms on Carmichael numbers, see further below.

4.5.5 The Fermat Test 'FST'

The standard, Monte-Carlo type, FST test works as follows: for arbitrary x, if p is prime, then Fermat's Little Theorem says that

4.5.5.1 $x^p - x = 0 \pmod p$

Here 'x' is referred to in the literature as the 'base'.

[Please note that we have, in this paper, extensively referred to the base as being the letter ‘a’ which is not the same as the Fermat base. Therefore, to avoid confusion, we will refer to 'p' in (4.5.5.1) as the 'Fermat base'].

To keep the numbers small, or at least as small as possible, the Fermat base is usually 2 or 3 as a first start, i.e. exactly as for our prime test.

If (4.5.5.1) is not satisfied then the candidate 'p' is definitely composite.

However, if (4.5.5.1) is satisfied, it does not necessarily mean that p is prime, albeit, it is likely to be prime. That is why FST is, like MFST, a Monte-Carlo test. For any particular Fermat base x there is a small probability that a composite 'p' will also pass the Fermat test. Such a composite, that passes the test to a particular Fermat base, is termed a 'Pseudoprime' to that Fermat base. To reduce the probability we can try another Fermat base, exactly as for our own primality test. Nevertheless, there are certain composites, called 'Carmichael Numbers', that will pass the test for all bases. See section (4.5.9) for a list. The lowest such Carmichael number is 561, which factors as 561 = 3*11*17. This particular number is discussed again in section (4.5.8) where an algebraic comparison of MFST and FST is given.

4.5.6 Experimental Comparison with the Fermat Test

The below data is produced from a comparison of MFST and FST for three bases, x = 2, 3 and 5 in(4.5.5.1). The test is performed for all odd p, p = 2l + 1, for all integer l, 0 < l < 5,000,000, i.e. all odd numbers p less than 10,000,000. All candidates were verified as composite by performing a division test using all primes between 0 and 3162 (= _/10,000,000).

Column 1: Prime candidate 'p'
Column 2: Count of MFST false alarms
Column 3: Count of Fermat test false alarms
Column 4: 1 denotes MFST false alarm
Column 5: 1 denotes Fermat test false alarm

Note all the numbers shown fail FST and hence a '1' in the last column. ALL the numbers 561..512461 are Carmichael numbers, see section (4.5.9) for a full list.

4.5.6.1 Odd numbers p = 2l + 1, 0 < l < 4,999,999

```
   561  0    1 0 1
  1105  0    2 0 1
  1729  1    3 1 1
  2465  1    4 0 1
  2821  1    5 0 1
  6601  1    6 0 1
  8911  1    7 0 1
 10585  1    8 0 1
```

```
   15841  2    9 1 1
   29341  2   10 0 1
   41041  3   11 1 1
   46657  4   12 1 1
   52633  4   13 0 1
   62745  4   14 0 1
   63973  4   15 0 1
   75361  5   16 1 1
  101101  5   17 0 1
  115921  6   18 1 1
  126217  6   19 0 1
  162401  7   20 1 1
  172081  8   21 1 1
  188461  8   22 0 1
  252601  8   23 0 1
  278545  8   24 0 1
  294409  8   25 0 1
  314821  8   26 0 1
  334153  9   27 1 1
  340561  9   28 0 1
  399001 10   29 1 1
  410041 10   30 0 1
  449065 10   31 0 1
  488881 11   32 1 1
  512461 11   33 0 1
  530881 12   34 1 1
  552721 12   35 0 1
  656601 12   36 0 1
  658801 12   37 0 1
  670033 13   38 1 1
  721801 13   39 0 1
  748657 13   40 0 1
  825265 13   41 0 1
  838201 14   42 1 1
  852841 14   43 0 1
  873181 14   44 0 1
  997633 15   45 1 1
 1024651 15   46 0 1
 1033669 15   47 0 1
 1050985 15   48 0 1
 1082809 15   49 0 1
 1152271 15   50 0 1
 1193221 15   51 0 1
 1461241 15   52 0 1
 1569457 15   53 0 1
 1615681 16   54 1 1
 1773289 17   55 1 1
 1857241 18   56 1 1
 1909001 18   57 0 1
 2100901 18   58 0 1
 2113921 19   59 1 1
 2433601 20   60 1 1
 2455921 21   61 1 1
 2508013 21   62 0 1
 2531845 21   63 0 1
 2628073 21   64 0 1
 2704801 22   65 1 1
 3057601 23   66 1 1
 3146221 23   67 0 1
 3224065 23   68 0 1
 3581761 24   69 1 1
```

```
3664585 24   70 0 1
3828001 25   71 1 1
4335241 25   72 0 1
4463641 26   73 1 1
4504501 26   74 0 1
4767841 26   75 0 1
4903921 27   76 1 1
4909177 27   77 0 1
5031181 27   78 0 1
5049001 28   79 1 1
5148001 29   80 1 1
5310721 30   81 1 1
5444489 30   82 0 1
5481451 30   83 0 1
5632705 30   84 0 1
5968873 31   85 1 1
6049681 31   86 0 1
6054985 31   87 0 1
6189121 32   88 1 1
6313681 32   89 0 1
6733693 32   90 0 1
6840001 33   91 1 1
6868261 33   92 0 1
7207201 33   93 0 1
7519441 34   94 1 1
7995169 35   95 1 1
8134561 35   96 0 1
8341201 35   97 0 1
8355841 36   98 1 1
8646121 36   99 0 1
8719309 36  100 0 1
8719921 37  101 1 1
8830801 38  102 1 1
8927101 38  103 0 1
9006401 39  104 1 1
9439201 40  105 1 1
9494101 40  106 0 1
9582145 40  107 0 1
9585541 41  108 1 1
9613297 42  109 1 1
9863461 43  110 1 1
9890881 44  111 1 1
```

We see that there are 44 false alarms for MFST compared with 110 false alarms for FST, i.e. MFST has less than half the false alarm rate.

[Note that there are 664579 primes less than 10,000,000 (10 million) starting with 2 and ending with 9,999,991. Since 2 is the only even prime, there are 664578 odd primes of the form 2l + 1, l >= 1].

It was noted that if the test was performed with only odd numbers of the form 4l+3, i.e. every other odd number such that (a - 1) / 2 was odd, MFST had 3 false alarms and FST had 11. The data, with format as per section (4.5.6) is given below. Notice that the Carmichael number 561 is not of the 4l + 3 form.

4.5.6.2 Odd numbers p = 4l + 1, 0 < l < 2,499,999

```
   8911  0    1 0 1
  90751  0    2 0 1
1024651  0    3 0 1
1152271  0    4 0 1
1530787  1    5 1 1
3116107  2    6 1 1
3375487  2    7 0 1
4314967  2    8 0 1
5481451  2    9 0 1
6539527  2   10 0 1
6787327  3   11 1 1
```

4.5.7 Algebraic Comparison with the Fermat Test

It was mentioned earlier in this section that MFST is really just a variant of FST. Nevertheless, it appears to give better results, i.e. a lower false alarm rate. We can see why this is so, as follows.

If we factorise the lhs of FST (4.5.5.1) we get

4.5.7.1 x^p - x = x*(x^((p - 1) / 2) - 1)*(x^((p - 1) / 2) + 1)

and so FST becomes

4.5.7.2 x*(x^((p - 1) / 2) - 1)*(x^((p - 1) / 2) + 1) = 0 (mod p)

The left hand side comprises at least three factors, which we shall denote by A, B and C as follows

4.5.7.3 A = x

4.5.7.4 B = (x^((p - 1) / 2) - 1)

4.5.7.5 C = (x^((p - 1) / 2) + 1)

The solution to 4.5.7.2 using A, B and C now becomes

4.5.7.6 A*B*C = 0 (mod p)

This splits into the following possible equations, any one of which would ensure the candidate prime p passes FST.

4.5.7.7 B = 0 (mod p)

4.5.7.8 C = 0 (mod p)

4.5.7.9 A*C = 0 (mod p)

4.5.7.10 B*C = 0 (mod p)

4.5.7.11 A*B*C = 0 (mod p)

Obviously, by choice of the Fermat base x != 0 and we cannot have A = 0.

If we substitute back for B and C from (4.5.7.4) and (4.5.7.5) into (4.5.7.7) and (4.5.7.8) respectively, upon re-arranging, we get

4.5.7.12 (x^((p - 1) / 2) = 1 (mod p)

4.5.7.13 (x^((p - 1) / 2) = -1 (mod p)

and combining them

4.5.7.14 | (x^((p - 1) / 2) | = -1 (mod p)

which is exactly the same as our MFST primality test (4.5.3).

The key point is that FST can pass any one of the five equations (4.5.7.7) to (4.5.7.11) whereas MFST satisfies only two of them. Consequently, FST can pass false alarms which are solutions to the three tests (4.5.7.9) to (4.5.7.11). Alternatively stated, any false alarm to MFST will also be a false alarm to FST, the converse is not true however so FST, as implemented by equation (4.5.5.1), can only give equivalent or worse false alarm rejection.

4.5.8 The Carmichael Number 561

Let p be defined as the smallest Carmichael number,

4.5.8.1 p = 561

which factors as 561 = 3*11*17, then

4.5.8.2 (p - 1) / 2 = 280

and

4.5.8.3 x^561 - x = x*(x^280 - 1)*(x^280 + 1)

Let x = 2 then

4.5.8.4 (2^280) - 1 = 67*67 (mod 561)

and, with some modulo arithmetic (2^280 = 2^140*2^140, 2^140 = 2^70*2^70, 2^70 = 2^35*2^35, 2^35 = 263 (mod 561)) we find that

4.5.8.5 2^280 = 1 (mod 561)

Hence, by (4.5.5.1) 561 will fail FST for base x = 2 and will fail MFST for the same base by (4.5.7.4) and (4.5.7.7).

However, if we now try the base x = 3,

Let x = 2, then

4.5.8.6 (3^280) - 1 = 440 (mod 561)

and

4.5.8.7 (3^280) + 1 = 442 (mod 561)

therefore

4.5.8.8 | (3^280) + 1 | != 1 (mod 561)

and so, by (4.5.3), MFST correctly rejects 561 as composite to base 3. However, using (4.5.8.6) for B and (4.5.8.7) for C in (4.5.7.10), we find that

4.5.8.9 (3^280 + 1)*(3^280 - 1) = 440*442 (mod 561)

and since

4.5.8.10 440*442 = 0 (mod 561)

we see that the number 561 fails the FST for Fermat base x = 561.

4.5.9 Some Carmichael Numbers

The first 33 (up to approx 500,000) Carmichael numbers are given below.

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101, 115921, 126217, 162401, 172081, 188461, 252601, 278545, 294409, 314821, 34153, 340561, 399001, 410041, 449065, 488881, 512461

5 Summary of Conditions

This is an edited (shortened) collation of all the conditions and constraints, placed upon a triple (a, b, c), were it to be an FLT counter-example and as summarised at the end of each section.

5.1.1 The **Standard Residue Condition** (1.2.3)

b^n = c^n (mod a^n)

5.1.2 The **Standard Quotient Condition** (1.4.3)

If (b^n = p*a^n + r) and (c^n = q*a^n + r) then q-p = 1

5.1.3 The **Dual Residue Condition** (1.17.1)

a^n = c^n (mod b^n)

5.1.4 The **Dual Quotient Condition** (1.18)

If (c^n = q'*b^n + a^n) then q' = 1

5.1.5 The **Skew Residue Condition** (2.5.1.18)

b^n = -a^n mod c^n

5.1.6 The Root Gap, must be less than the base a Theorem (1.12)

Rg = c - b < a

5.1.7 If the base a is prime, the Root Gap (1.10.1) must be unity, Theorem (1.14).

Rg = c - b = 1

5.1.8 The Root Gap (1.10.1) must divide the base a

(c – b) | a

The Dual Root Gap (1.15.1) must divide the Dual base b

5.1.9 $(c - a) \mid b$

5.1.10 The Dual base b is always composite, Theorem (1.15)

5.1.11 By convention $a < b < c$, (0.3.3), the Dual Root Gap Rg' (1.15.1) is always greater than unity.

$Rg = (c - a) > 1$

5.1.12 The maximum value of b, Candidate Pair (b,c) is Bmax, Theorem (1.19.1).

$b < Bmax$

5.1.13 The maximum value of c, Dual Candidate Pair (a,c) is C'max, Theorem (1.20).

$c < C'max$

5.1.14 For integers x and k, $x >= 1$, $k >= 1$, the value a is either prime ($x = 1$) or composite ($x > 1$) with one or more factors of the form (2kn+1), i.e.

$a = x(2kn + 1)$

5.1.15 For integers y and l, $y >= 2$, $l >= 1$ the value b always composite with one or more prime factors of the form 2ln+1, i.e.

$b = y(2ln + 1)$

5.1.16 For integers z and m, $z >= 1$, $m >= 1$ the value c is either prime ($z = 1$) or composite ($z > 1$) with one or more factors of the form (2mn+1), i.e.

$c = z(2mn + 1)$

5.1.17 Candidate Pair (b,c), b maps to c by the Unity Root 'u(a)', (3.1.1)

$c = u(a)*b \pmod{a^n}$

5.1.18 Dual Candidate Pair (a,c), a maps to c by the Unity Root ‘u(b)’

c = u(b)*b (mod b^n)

5.1.19 Skew Candidate Pair (a,b), a maps to b by the Unity Root ‘u(c)’, (2.5.1.4)

b = -u(c)*a mod c^n

5.1.20 The Unity Root u(a), (mod a^n), is greater than the base a, (3.3.5)

u(a) > a

This constraint is also valid in the Dual case for Unity Root u, (mod b^n)

5.1.21 The minimum value of a unity root ‘Umin(a)’, (mod a^n) is greater than or equal to the (n - 1)’th root of the modulus a^n, Conjecture (3.6.15)

Umin(a) >= (n - 1)_/a^n

This conjecture is also valid in the Dual case for Unity Root u, (mod b^n)

5.1.22 If (b,c) is a Candidate Pair (mod a^n), then the Winding Number ‘w’ (3.4.4) is greater than zero

w > 0

5.1.23 A non-trivial, Unity Root u(A), to any modulus A, such that u(A)^n = 0 (mod a), is a solution to the Cyclotomic Polynomial f(u(A)) (3.6.4) such that

f(u(A)) = 0 (mod a)

6 References

1. Modular elliptic curves and Fermat's Last Theroem, A Wiles, Annals of Mathematics 142 (1995),443-551.

2. Alf J Van der Poorten, 'Notes on Fermat's Last Theorem'
3. Paulo Ribenboim, '13 Lectures on Fermat's Last Theorem'

4. E. W. Weisstein, Mathworld, A Wolfram Web Resource, http://mathworld.wolfram.com

5. MFLT, a variant of the FLT equation, R J Miller, 2004

6. H Davenport, 'The Higher Arithmetic', 6th Edition, Cambridge University Press, ISBN 0 521 41998 0 Hardback, ISBN 0 521 42227 2 paperback,

7. Computational Methods (TBD)
   Modified FLT Test
   Unity Root Algorithm
   LDE solver
   Large Numbers Library
   Factoring Program

8. Keith Devlin, Mathematics, The New Golden Age, Penguin Books, First Published 1998, ISBN 0-14-025865-5.

7 Data/Software

7.1 Residue Tables

7.1.1 n = 2, a = 3

```
-----------------------------------------

      Residue Table a = 3, n = 2

   x        x^n  residue r  residue quotient
                   (mod a^n)     (mod a)        p
---- ---------- ---------- -------- --------
   0          0          0        0        0
   1          1          1        1        0
   2          4          4        1        0
   3          9          0        0        1
   4         16          7        1        1
   5         25          7        1        2
   6         36          0        0        4
   7         49          4        1        5
   8         64          1        1        7
   9         81          0        0        9
```

7.1.2 n = 2, a = 4

```
-----------------------------------------

      Residue Table a = 4, n = 2

   x        x^n  residue r  residue quotient
                   (mod a^n)     (mod a)        p
---- ---------- ---------- -------- --------
   0          0          0        0        0
   1          1          1        1        0
   2          4          4        0        0
   3          9          9        1        0
   4         16          0        0        1
   5         25          9        1        1
   6         36          4        0        2
   7         49          1        1        3
   8         64          0        0        4
   9         81          1        1        5
  10        100          4        0        6
  11        121          9        1        7
  12        144          0        0        9
  13        169          9        1       10
  14        196          4        0       12
  15        225          1        1       14
  16        256          0        0       16
```

7.1.3 n = 2, a = 5

```
-----------------------------------------

      Residue Table a = 5, n = 2

   x        x^n  residue r  residue quotient
                   (mod a^n)     (mod a)        p
```

0	0	0	0	0
1	1	1	1	0
2	4	4	4	0
3	9	9	4	0
4	16	16	1	0
5	25	0	0	1
6	36	11	1	1
7	49	24	4	1
8	64	14	4	2
9	81	6	1	3
10	100	0	0	4
11	121	21	1	4
12	144	19	4	5
13	169	19	4	6
14	196	21	1	7
15	225	0	0	9
16	256	6	1	10
17	289	14	4	11
18	324	24	4	12
19	361	11	1	14
20	400	0	0	16
21	441	16	1	17
22	484	9	4	19
23	529	4	4	21
24	576	1	1	23
25	**625**	**0**	**0**	**25**

7.1.4 n = 3, a = 5

Residue Table a = 5, n = 3

x	x^n	residue r (mod a^n)	residue quotient (mod a)	p
0	0	0	0	0
1	1	1	1	0
2	8	8	3	0
3	27	27	2	0
4	64	64	4	0
5	125	0	0	1
6	216	91	1	1
7	343	93	3	2
8	512	12	2	4
9	729	104	4	5
10	1000	0	0	8
11	1331	81	1	10
12	1728	103	3	13
13	2197	72	2	17
14	2744	119	4	21
15	3375	0	0	27
16	4096	96	1	32
17	4913	38	3	39
18	5832	82	2	46
19	6859	109	4	54
20	8000	0	0	64
21	9261	11	1	74
22	10648	23	3	85
23	12167	42	2	97
24	13824	74	4	110
25	15625	0	0	125
26	17576	76	1	140
27	19683	58	3	157
28	21952	77	2	175
29	24389	14	4	195
30	27000	0	0	216
31	29791	41	1	238
32	32768	18	3	262
33	35937	62	2	287

34	39304	54	4	314
35	42875	0	0	343
36	46656	31	1	373
37	50653	28	3	405
38	54872	122	2	438
39	59319	69	4	474
40	64000	0	0	512
41	68921	46	1	551
42	74088	88	3	592
43	79507	7	2	636
44	85184	59	4	681
45	91125	0	0	729
46	97336	86	1	778
47	103823	73	3	830
48	110592	92	2	884
49	117649	24	4	941
50	125000	0	0	1000
51	132651	26	1	1061
52	140608	108	3	1124
53	148877	2	2	1191
54	157464	89	4	1259
55	166375	0	0	1331
56	175616	116	1	1404
57	185193	68	3	1481
58	195112	112	2	1560
59	205379	4	4	1643
60	216000	0	0	1728
61	226981	106	1	1815
62	238328	78	3	1906
63	250047	47	2	2000
64	262144	19	4	2097
65	274625	0	0	2197
66	287496	121	1	2299
67	300763	13	3	2406
68	314432	57	2	2515
69	328509	9	4	2628
70	343000	0	0	2744
71	357911	36	1	2863
72	373248	123	3	2985
73	389017	17	2	3112
74	405224	99	4	3241
75	421875	0	0	3375
76	438976	101	1	3511
77	456533	33	3	3652
78	474552	52	2	3796
79	493039	39	4	3944
80	512000	0	0	4096
81	531441	66	1	4251
82	551368	118	3	4410
83	571787	37	2	4574
84	592704	79	4	4741
85	614125	0	0	4913
86	636056	56	1	5088
87	658503	3	3	5268
88	681472	97	2	5451
89	704969	94	4	5639
90	729000	0	0	5832
91	753571	71	1	6028
92	778688	63	3	6229
93	804357	107	2	6434
94	830584	84	4	6644
95	857375	0	0	6859
96	884736	111	1	7077
97	912673	48	3	7301
98	941192	67	2	7529
99	970299	49	4	7762
100	1000000	0	0	8000
101	1030301	51	1	8242
102	1061208	83	3	8489
103	1092727	102	2	8741
104	1124864	114	4	8998
105	1157625	0	0	9261
106	1191016	16	1	9528
107	1225043	43	3	9800
108	1259712	87	2	10077
109	1295029	29	4	10360
110	1331000	0	0	10648

111	1367631	6	1	10941
112	1404928	53	3	11239
113	1442897	22	2	11543
114	1481544	44	4	11852
115	1520875	0	0	12167
116	1560896	21	1	12487
117	1601613	113	3	12812
118	1643032	32	2	13144
119	1685159	34	4	13481
120	1728000	0	0	13824
121	1771561	61	1	14172
122	1815848	98	3	14526
123	1860867	117	2	14886
124	1906624	124	4	15252
125	1953125	0	0	15625

7.1.5 n = 3, a = 7

Residue Table a = 7, n = 3

x	x^n	residue r (mod a^n)	residue quotient (mod a)	p
0	0	0	0	0
1	1	1	1	0
2	8	8	1	0
3	27	27	6	0
4	64	64	1	0
5	125	125	6	0
6	216	216	6	0
7	343	0	0	1
8	512	169	1	1
9	729	43	1	2
10	1000	314	6	2
11	1331	302	1	3
12	1728	13	6	5
13	2197	139	6	6
14	2744	0	0	8
15	3375	288	1	9
16	4096	323	1	11
17	4913	111	6	14
18	5832	1	1	17
19	6859	342	6	19
20	8000	111	6	23
21	9261	0	0	27
22	10648	15	1	31
23	12167	162	1	35
24	13824	104	6	40
25	15625	190	1	45
26	17576	83	6	51
27	19683	132	6	57
28	21952	0	0	64
29	24389	36	1	71
30	27000	246	1	78
31	29791	293	6	86
32	32768	183	1	95
33	35937	265	6	104
34	39304	202	6	114
35	42875	0	0	125
36	46656	8	1	136
37	50653	232	1	147
38	54872	335	6	159
39	59319	323	1	172
40	64000	202	6	186
41	68921	321	6	200
42	74088	0	0	216
43	79507	274	1	231
44	85184	120	1	248
45	91125	230	6	265
46	97336	267	1	283
47	103823	237	6	302

48	110592	146	6	322
49	117649	0	0	343
50	125000	148	1	364
51	132651	253	1	386
52	140608	321	6	409
53	148877	15	1	434
54	157464	27	6	459
55	166375	20	6	485
56	175616	0	0	512
57	185193	316	1	539
58	195112	288	1	568
59	205379	265	6	598
60	216000	253	1	629
61	226981	258	6	661
62	238328	286	6	694
63	250047	0	0	729
64	262144	92	1	764
65	274625	225	1	800
66	287496	62	6	838
67	300763	295	1	876
68	314432	244	6	916
69	328509	258	6	957
70	343000	0	0	1000
71	357911	162	1	1043
72	373248	64	1	1088
73	389017	55	6	1134
74	405224	141	1	1181
75	421875	328	6	1229
76	438976	279	6	1279
77	456533	0	0	1331
78	474552	183	1	1383
79	493039	148	1	1437
80	512000	244	6	1492
81	531441	134	1	1549
82	551368	167	6	1607
83	571787	6	6	1667
84	592704	0	0	1728
85	614125	155	1	1790
86	636056	134	1	1854
87	658503	286	6	1919
88	681472	274	1	1986
89	704969	104	6	2055
90	729000	125	6	2125
91	753571	0	0	2197
92	778688	78	1	2270
93	804357	22	1	2345
94	830584	181	6	2421
95	857375	218	1	2499
96	884736	139	6	2579
97	912673	293	6	2660
98	941192	0	0	2744
99	970299	295	1	2828
100	1000000	155	1	2915
101	1030301	272	6	3003
102	1061208	309	1	3093
103	1092727	272	6	3185
104	1124864	167	6	3279
105	1157625	0	0	3375
106	1191016	120	1	3472
107	1225043	190	1	3571
108	1259712	216	6	3672
109	1295029	204	1	3775
110	1331000	160	6	3880
111	1367631	90	6	3987
112	1404928	0	0	4096
113	1442897	239	1	4206
114	1481544	127	1	4319
115	1520875	13	6	4434
116	1560896	246	1	4550
117	1601613	146	6	4669
118	1643032	62	6	4790
119	1685159	0	0	4913
120	1728000	309	1	5037
121	1771561	309	1	5164
122	1815848	6	6	5294
123	1860867	92	1	5425
124	1906624	230	6	5558

125	1953125	83	6	5694
126	2000376	0	0	5832
127	2048383	330	1	5971
128	2097152	50	1	6114
129	2146689	195	6	6258
130	2197000	85	1	6405
131	2248091	69	6	6554
132	2299968	153	6	6705
133	2352637	0	0	6859
134	2406104	302	1	7014
135	2460375	36	1	7173
136	2515456	237	6	7333
137	2571353	225	1	7496
138	2628072	6	6	7662
139	2685619	272	6	7829
140	2744000	0	0	8000
141	2803221	225	1	8172
142	2863288	267	1	8347
143	2924207	132	6	8525
144	2985984	169	1	8705
145	3048625	41	6	8888
146	3112136	97	6	9073
147	3176523	0	0	9261
148	3241792	99	1	9451
149	3307949	57	1	9644
150	3375000	223	6	9839
151	3442951	260	1	10037
152	3511808	174	6	10238
153	3581577	314	6	10441
154	3652264	0	0	10648
155	3723875	267	1	10856
156	3796416	92	1	11068
157	3869893	167	6	11282
158	3944312	155	1	11499
159	4019679	62	6	11719
160	4096000	237	6	11941
161	4173281	0	0	12167
162	4251528	43	1	12395
163	4330747	29	1	12626
164	4410944	307	6	12859
165	4492125	197	1	13096
166	4574296	48	6	13336
167	4657463	209	6	13578
168	4741632	0	0	13824
169	4826809	113	1	14072
170	4913000	211	1	14323
171	5000211	300	6	14577
172	5088448	43	1	14835
173	5177717	132	6	15095
174	5268024	230	6	15358
175	5359375	0	0	15625
176	5451776	134	1	15894
177	5545233	295	1	16166
178	5639752	146	6	16442
179	5735339	36	1	16721
180	5832000	314	6	17002
181	5929741	300	6	17287
182	6028568	0	0	17576
183	6128487	106	1	17867
184	6229504	281	1	18161
185	6331625	188	6	18459
186	6434856	176	1	18760
187	6539203	251	6	19064
188	6644672	76	6	19372
189	6751269	0	0	19683
190	6859000	29	1	19997
191	6967871	169	1	20314
192	7077888	83	6	20635
193	7189057	120	1	20959
194	7301384	286	6	21286
195	7414875	244	6	21617
196	7529536	0	0	21952
197	7645373	246	1	22289
198	7762392	302	1	22630
199	7880599	174	6	22975
200	8000000	211	1	23323
201	8120601	76	6	23675

202	8242408	118	6	24030
203	8365427	0	0	24389
204	8489664	71	1	24751
205	8615125	337	1	25116
206	8741816	118	6	25486
207	8869743	106	1	25859
208	8998912	307	6	26235
209	9129329	41	6	26616
210	9261000	0	0	27000
211	9393931	190	1	27387
212	9528128	274	1	27778
213	9663597	258	6	28173
214	9800344	148	1	28572
215	9938375	293	6	28974
216	10077696	13	6	29381
217	10218313	0	0	29791
218	10360232	260	1	30204
219	10503459	113	1	30622
220	10648000	251	6	31043
221	10793861	337	1	31468
222	10941048	34	6	31898
223	11089567	34	6	32331
224	11239424	0	0	32768
225	11390625	281	1	33208
226	11543176	197	1	33653
227	11697083	97	6	34102
228	11852352	330	1	34554
229	12008989	216	6	35011
230	12167000	104	6	35472
231	12326391	0	0	35937
232	12487168	253	1	36405
233	12649337	183	1	36878
234	12812904	139	6	37355
235	12977875	127	1	37836
236	13144256	153	6	38321
237	13312053	223	6	38810
238	13481272	0	0	39304
239	13651919	176	1	39801
240	13824000	71	1	40303
241	13997521	34	6	40809
242	14172488	71	1	41319
243	14348907	188	6	41833
244	14526784	48	6	42352
245	14706125	0	0	42875
246	14886936	50	1	43402
247	15069223	204	1	43933
248	15252992	125	6	44469
249	15438249	162	1	45009
250	15625000	321	6	45553
251	15813251	265	6	46102
252	16003008	0	0	46656
253	16194277	218	1	47213
254	16387064	239	1	47775
255	16581375	69	6	48342
256	16777216	57	1	48913
257	16974593	209	6	49488
258	17173512	188	6	50068
259	17373979	0	0	50653
260	17576000	337	1	51241
261	17779581	176	1	51835
262	17984728	209	6	52433
263	18191447	99	1	53036
264	18399744	195	6	53643
265	18609625	160	6	54255
266	18821096	0	0	54872
267	19034163	64	1	55493
268	19248832	15	1	56119
269	19465109	202	6	56749
270	19683000	288	1	57384
271	19902511	279	6	58024
272	20123648	181	6	58669
273	20346417	0	0	59319
274	20570824	85	1	59973
275	20796875	99	1	60632
276	21024576	48	6	61296
277	21253933	281	1	61964
278	21484952	118	6	62638

279	21717639	251	6	63316
280	21952000	0	0	64000
281	22188041	57	1	64688
282	22425768	85	1	65381
283	22665187	90	6	66079
284	22906304	78	1	66782
285	23149125	55	6	67490
286	23393656	27	6	68203
287	23639903	0	0	68921
288	23887872	323	1	69643
289	24137569	316	1	70371
290	24389000	328	6	71104
291	24642171	22	1	71843
292	24897088	90	6	72586
293	25153757	195	6	73334
294	25412184	0	0	74088
295	25672375	197	1	74846
296	25934336	106	1	75610
297	26198073	76	6	76379
298	26463592	113	1	77153
299	26730899	223	6	77932
300	27000000	69	6	78717
301	27270901	0	0	79507
302	27543608	22	1	80302
303	27818127	141	1	81102
304	28094464	20	6	81908
305	28372625	8	1	82719
306	28652616	111	6	83535
307	28934443	335	6	84356
308	29218112	0	0	85184
309	29503629	141	1	86016
310	29791000	78	1	86854
311	30080231	160	6	87697
312	30371328	50	1	88546
313	30664297	97	6	89400
314	30959144	307	6	90259
315	31255875	0	0	91125
316	31554496	211	1	91995
317	31855013	260	1	92871
318	32157432	153	6	93753
319	32461759	239	1	94640
320	32768000	181	6	95533
321	33076161	328	6	96431
322	33386248	0	0	97336
323	33698267	232	1	98245
324	34012224	1	1	99161
325	34328125	342	6	100081
326	34645976	232	1	101008
327	34965783	20	6	101941
328	35287552	55	6	102879
329	35611289	0	0	103823
330	35937000	204	1	104772
331	36264691	330	1	105727
332	36594368	41	6	106689
333	36926037	29	1	107656
334	37259704	300	6	108628
335	37595375	174	6	109607
336	37933056	0	0	110592
337	38272753	127	1	111582
338	38614472	218	1	112578
339	38958219	279	6	113580
340	39304000	316	1	114588
341	39651821	335	6	115602
342	40001688	342	6	116622
343	40353607	0	0	117649

7.1.6 n = 4, a = 5

First fifty entries only, 0<=x<50

See b =38, c =41 for smallest Candidate Pair [38,41] mod 5^4.

Residue Table a = 5, n = 4

x	x^n	residue r (mod a^n)	residue quotient (mod a)	p
0	0	0	0	0
1	1	1	1	0
2	16	16	1	0
3	81	81	1	0
4	256	256	1	0
5	625	0	0	1
6	1296	46	1	2
7	2401	526	1	3
8	4096	346	1	6
9	6561	311	1	10
10	10000	0	0	16
11	14641	266	1	23
12	20736	111	1	33
13	28561	436	1	45
14	38416	291	1	61
15	50625	0	0	81
16	65536	536	1	104
17	83521	396	1	133
18	104976	601	1	167
19	130321	321	1	208
20	160000	0	0	256
21	194481	106	1	311
22	234256	506	1	374
23	279841	466	1	447
24	331776	526	1	530
25	390625	0	0	625
26	456976	101	1	731
27	531441	191	1	850
28	614656	281	1	983
29	707281	406	1	1131
30	810000	0	0	1296
31	923521	396	1	1477
32	1048576	451	1	1677
33	1185921	296	1	1897
34	1336336	86	1	2138
35	1500625	0	0	2401
36	1679616	241	1	2687
37	1874161	411	1	2998
38	**2085136**	**136**	**1**	**3336**
39	2313441	316	1	3701
40	2560000	0	0	4096
41	**2825761**	**136**	**1**	**4521**
42	3111696	446	1	4978
43	3418801	51	1	5470
44	3748096	596	1	5996
45	4100625	0	0	6561
46	4477456	581	1	7163
47	4879681	306	1	7807
48	5308416	291	1	8493
49	5764801	426	1	9223
50	6250000	0	0	10000

7.2 Unity Roots

7.2.1 n = 3

7.2.1.1 a = 7

a is of the 2kn+1 form so there are 3 roots

U ={1,18,324}

7.2.1.2 a = 13

a is of the 2kn+1 form so there are 3 roots

U ={1,1036,1160}

7.2.2 n = 4

7.2.2.1 a = 4

Since n|a, the Residues Sequence is Minimal of size 4^4/4, there are only two roots in the Minimal interval [0,4^3)

U = {1,63}

where 63=-1 mod 4^3

7.2.2.2 a = 5

a is of the ln+1 form so there are 4 roots

U = {1, 182, 443, 624}

7.2.2.3 a = 9

a is of the ln+1 form so there are 4 roots

U = {1, 182, 443, 624}

7.2.2.4 a = 13

a is of the ln+1 form so there are 4 roots

13^4 = 28561

U = {1, 239, 28322, 28560}

Consecutive Idetnical Residues

C = {119, 120, 14280, 14281, 28441, 28442}

7.2.3 n = 5

7.2.3.1 a = 11

a is of the 2kn+1 form so there are 5 roots

U ={1, 37101, 46709, 104450, 133835}

7.2.3.2 a = 31

a is of the 2kn+1 form so there are 5 roots

U ={1, 13801549, 13979094, 15561847, 28629152}