Journal of Applied Mathematics & Bioinformatics, vol.5, no.2, 2015, 21-48
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2015

A study of Fermat's Last Theorem and other Diophantine Equations

Olufemi O. Oyadare[1]

Abstract

This paper develops a framework of algebra whereby every Diophantine equation is made quickly accessible by a study of the corresponding row entries in an array of numbers which we call the *Binomial triangle*. We then apply the framework to the discussion of some notable results in the theory of numbers. Among other results, we prove a new and complete generation of *all* Pythagorean triples (without necessarily resorting to their production by examples), convert the collection of Binomial triangles to a Noetherian ring (whose identity element is found to be the well-known Pascal triangle) and develop an easy understanding of the *original* Fermat's Last Theorem (FLT). The application includes the computation of the Galois groups of those polynomials coming from our outlook on FLT and an approach to the explicit realization of arithmetic groups of curves by a treatment of some Diophantine curves.

Mathematics Subject Classification: $11G15; 11Y40; 11Rxx$
Keywords: Diophantine curves; Galois group; Arithmetic group

[1] Department of Mathematics, Obafemi Awolowo University, Ile-Ife, 220005, Nigeria.
E-mail: femi_oya@yahoo.com

Article Info: *Received* : January 17, 2015. *Revised* : February 26, 2015.
Published online : June 20, 2015.

1 Introduction

Let $x, y, n \in \mathbb{N} \cup \{0\}$, then the coefficients in the expansion of $(x+y)^n$, when considered as a polynomial in descending powers of x, are $1,\ {}^nC_1y,\ {}^nC_2y^2, \cdots, y^n$. For $y = 1$ these coefficients form the nth row of the Pascal triangle, while, for other values of y, the coefficients form the nth row of an array of numbers which we call the *Binomial triangles.* Numbers formed from these coefficients, by the application of the *digital-correspondence* map, are $n-$powers of natural numbers and may be extended to generate all $n-$powers of rational numbers only. This outlook simplifies every Diophantine equation and gives proof of results that are consistent with the expectations of their originators and true to the spirit of classical number theory, as we shall show in the case of rational solutions of the equation $u^n + v^n = w^n$, for $n = 2$ and its impossibility for non-zero rationals u, v and w, when integers $n > 2$, in §3. and §4., respectively. The approach to the present study is that instead of splitting the power n above, thus leading to its primality or otherwise (as it has always been done by many number theorists), we decide to split u, v and w and study the consequences of this choice. We believe this approach is more natural to the study of Diophantine equations, especially Fermat's Last Theorem.

The ideas of this paper emanated from a very elementary transformation of the finite Binomial theorem. After the introduction of the digital-correspondence map and the Binomial triangles in §2, we state and establish a purely algebraic reason for the existence and explicit form of all rational Pythagorean triples, leading to the partitioning of the integral ones in §3. Aside other mentioned approaches that may be taken to the study of Pythagorean triples, the ring of Binomial triangles is introduced and proved to be Noetherian. §4 contains an elementary proof of the *original* Fermat's Last Theorem which is seen to be greatly simplified by the introduction and investigation of some built-in polynomials of the Binomial triangles. Open problems on the ideal theory of the Noetherian ring of Binomial triangles, distribution and density of solutions of Diophantine equations, non-rational Pythagorean triples in other *fields* and the link with the *Wiles-Taylor proof* of FLT are all brought up in the remark at the end of each section. §5. contains two Lemmas and a Theorem, on the nature of these built-in polynomials we call *Fermat polynomials,* while we offer a novel approach to the yet-to-be-solved problem of computing

the *Mordell-Weil* groups of algebraic curves in §6. Some open problems are also contained in §7.

A preliminary version of Theorem 3.1 is contained in the announcement [9].

2 Digital-correspondence and Binomial triangles

A typical row in the Pascal triangle is $(1,\ {}^nC_1,\ {}^nC_2, \cdots, 1)$. Among its many properties we have that

$$1 +^n C_1 +^n C_2 + \cdots + 1 = 2^n,$$

for all $n \in \mathbb{N} \cup \{0\}$. For $n < 5$, each of the coefficients $1,\ {}^nC_1,\ {}^nC_2, \cdots, 1$, is a digit, so that any row may be viewed as a number having these coefficients as its digits. These numbers are $1, 11, 121, 1331$, and 14641, each of which is the respective nth power of 11, for $n = 0, 1, 2, 3, 4$. ([10.], *p.* 10) It may then be asked:

> *Is it a mere coincidence that for* $n \in \mathbb{N} \cup \{0\},\ n < 5$, *the number* $(1+1)^n$ *(where* 1 *is the repeated digit of the number* $11 = (10+1)$*) is exactly* 2^n *(the sum* $1 +^n C_1 +^n C_2 + \cdots + 1$*)? Indeed, what can we say of each of the remaining rows in the Pascal triangle with respect to* $(11)^n$*?*

We answer the second question above as follows. Since the 5th row in the triangle is $(1, 5, 10, 10, 5, 1)$ an appropriate transfer of tens, at the middle terms, gives the number 161051. This is 11^5. We have taken the top digit 1 in the Pascal triangle as the 0th row. The 6th row is $(1, 6, 15, 20, 15, 6, 1)$, which corresponds, after appropriate transfer of tens, to the number 1771561. This is 11^6. A first conclusion is therefore that these equalities are not mere coincidences and that there is a map taking $1+^nC_1+^nC_2+\cdots+1 = 2^n = (1+1)^n$ to $(11_{10})^n$. This map is expected to combine the coefficients, $(1,\ {}^nC_1,\ {}^nC_2,\ \cdots,\ 1)$, of the

Pascal triangle to form a whole number having the coefficients as the digits of the number (for $n < 5$) or form the number after appropriate transfer of tens (for $n \geq 5$). In order to define this map in its generality we shall first generalize the Pascal triangle.

We consider $n, y \in \mathbb{N} \cup \{0\}$ and the coefficients $(1,\ {}^nC_1y,\ {}^nC_2y^2, \cdots, y^n)$ of the finite binomial expansion of $(x+y)^n$. For different choices of n, the corresponding triangle is

$$
\begin{array}{c}
1 \\
1 \quad y \\
1 \quad 2y \quad y^2 \\
1 \quad 3y \quad 3y^2 \quad y^3 \\
1 \quad 4y \quad 6y^2 \quad 4y^3 \quad y^4 \\
1 \quad 5y \quad 10y^2 \quad 10y^3 \quad 5y^4 \quad y^5 \\
\cdots\cdots\cdots\cdots \\
\cdots\cdots\cdots\cdots \\
1 \quad {}^nC_1y \quad {}^nC_2y^2 \quad {}^nC_3y^3 \ldots {}^nC_ry^r \cdots y^n \\
\cdots\cdots\cdots\cdots
\end{array}
$$

We shall refer to this as the *Binomial triangle* and denote it as $T(y)$. Its build-up formula may be seen as $y({}^{n-1}C_{r-1}y^{r-1}) +^{n-1} C_ry^r =^n C_ry^r, \quad \forall\ r \in \mathbb{N}$, which becomes familiar when $y = 1$. In order to get a handle on our extension of the Pascal triangle we consider the Binomial triangle for $y = 2$. In this case the 2nd row is $(1, 4, 4)$, which corresponds to the number $144 = 12^2$, the 3rd row is $(1, 6, 12, 8)$ corresponding to the number $1728 = 12^3$, the 4th row is $(1, 8, 24, 32, 16)$ corresponding to the number $20736 = 12^4$, *etc.* We shall therefore say that the number 20736 *digitally corresponds* to the row $(1, 8, 24, 32, 16)$, and vice-versa. We shall denote the *digital-correspondence* map by $\delta : \mathbb{N}^{n+1} \to \mathbb{N}$ whose restriction to the subset $\{(1,\ {}^nC_1y,\ {}^nC_2y^2, \cdots, y^n) : n, y \in \mathbb{N} \cup \{0\}\}$ of $\mathbb{N}^{n+1}$ is given as

$$\delta(1,\ {}^nC_1y,\ {}^nC_2y^2, \cdots, y^n) = 1\ {}^nC_1y\ {}^nC_2y^2\ \cdots\ y^n,$$

where the right hand side is viewed as a whole number, whether tens are transferred (when $n \geq 5$ or $y \neq 1$) or not (when $n < 5$ and $y = 1$).

The truth behind our observations that the whole number

$$\delta(1,\ {}^nC_1y,\ {}^nC_2y^2,\cdots,y^n)$$

is always a power of n may be formalized for any row

$$N(y,n) := (1,\ {}^nC_1y,\ {}^nC_2y^2,\cdots,y^n)$$

in the Binomial triangles, $T(y)$. Here a natural number having an nth root in $\mathbb{N}$, for some $n = 2,3,4,\cdots$, shall be called *exact.* In this sense -4 is an exact integer of power 1 only (since $-4 = (-4)^1$), while 4 is an exact integer of powers 1 (since $4 = 4^1$) and 2 (since $4 = (2)^2$).

Lemma 2.1. *Let $y, n \in \mathbb{N} \cup \{0\}$ and define $f_n(y) = \delta(N(y,n))$. Each $f_n(y) \in \mathbb{N}$ and is exact of power n. Every exact number in $\mathbb{N}$ is of the form $f_n(y)$.*

Proof. We know that $(x+y)^n = x^n + ({}^nC_1y)x^{n-1} + ({}^nC_2y^2)x^{n-2} + \cdots + y^n$, so that, considering x as the *base of numeration* on both sides, we have

$$(1y_x)^n = (1\ \ {}^nC_1y\ \ {}^nC_2y^2\ \ \cdots\ \ y^n)_x.$$

That is,

$$(1y_x)^n = \delta(N(y,n))_x = f_n(y)_x \cdots\cdots\cdots (*)$$

as two equal numbers in base x. □

The above lemma shall be employed in Theorems 3.1, 4.2 and 4.3 in the following form. Our point of departure in the consideration of powers of integers (resp., rationals) is to view the set of *all* exact integers (resp., rationals) of power n in terms of the polynomials, f_n, as assured by the following lemma.

Corollary 2.2. *Let $\mathfrak{E}$ be the collection of all exact integers, explicitly given as*

$$\mathfrak{E} = \{\xi^n : \xi \in \mathbb{Z}^+ \text{ and } n \in 2\mathbb{N}\} \cup \{\xi^n : \xi \in \mathbb{Z} \text{ and } n \in \mathbb{N} \setminus 2\mathbb{N}\}.$$

Then the set $\mathfrak{E}$ is in a one-to-one correspondence with the set

$$\{f_n(y) : y \in \mathbb{Z}, n \in \mathbb{N}\}.$$

Proof. Define $\rho : \{f_n(y) : y \in \mathbb{Z}\} \to \mathfrak{E}$ as $\rho(f_n(y)) := \xi^n$, with $\xi = 10 + y,\ y \in \mathbb{Z}$. ρ is a one-to-one correspondence. □

Remark 2.3. 1. *On all exact rationals*: It may be seen, from the left side of $(*)$, that $f_n(y) = (10 + y)^n$, as earlier envisaged in the case of $y = 1$. This polynomial form for f_n allows us to extend its domain to all $y \in \mathbb{Q}$, giving *only all* exact rationals. The constant 10 in f_n may clearly be replaced with any other constant in $\mathbb{Z}$. The definition of $\mathfrak{E}$ above is designed to take adequate care of the unnecessary repetition of values of powers of integers brought about by the equality of $(-m)^{2n}$ and $m^{2n},\ m \in \mathbb{Z},\ n \in \mathbb{N}$, when computing natural powers of integers.

2. *On general Diophantine equations*: Our focus is to discuss the contribution of $f_n(y)$ to Diophantine equations, which we may generally write as

$$A_1\alpha_1^{n_1} + A_2\alpha_2^{n_2} + A_3\alpha_3^{n_3} + \cdots + A_p\alpha_p^{n_p} = B\beta^m,$$

for some constants $A_i, B \in \mathbb{Q},\ n_i, m \in \mathbb{N}$ and unknowns $\alpha_i, \beta \in \mathbb{Q},\ i = 1, 2, \cdots, p$. This translates, in our context, to studying

$$A_1 f_{n_1}(y_1) + A_2 f_{n_2}(y_2) + A_3 f_{n_3}(y_3) + \cdots + A_p f_{n_p}(y_p) = B f_m(y),$$

for some $y, y_i \in \mathbb{Q},\ i = 1, 2, \cdots, p$. A particular example is when $A_i = 1$ and $n_i = m = n$ with $p = 2$, which is the defining equation of FLT. That is,

$$f_n(y_1) + f_n(y_2) = f_n(y_3),$$

for $y_1 \neq y_2 \neq y_3$. It is necessary to illustrate the depth of insight of this formulation of Diophantine equations by tackling a formidable problem.

We shall illustrate our method with the problems of Pythagorean triples and FLT. In our context, these two problems are simultaneously captured by studying the possible values of $y \in \mathbb{Q}$ for which

$$Q_{n-1,a}(y) := f_n(y + a) - f_n(y),$$

$y \in \mathbb{Q},\ a \in \mathbb{Q} \setminus \{0\},\ n \in \mathbb{N}$, is the digital-correspondence of some $N(y_0, n), y_0 \in \mathbb{Q}$. We have set $y_1 = y_0,\ y_2 = y$ and $y_3 = y + a$, in $f_n(y_1) + f_n(y_2) = f_n(y_3)$ above to arrive at the equation $Q_{n-1,a}(y) := f_n(y + a) - f_n(y)$.

Our approach would then be to investigate, among other things, the *reason* for the existence of (rational) Pythagorean triples in §3, which we then employ to seek *Fermat's triples,* if they exist in §4.

3 Pythagorean triples in the context of Binomial trianglesIntroduction

Lemma 2.1 clearly says that $f_2(y), \forall\ y \in \mathbb{N} \cup \{0\}$, (indeed $\forall\ y \in \mathbb{Q}$) is a perfect-square in $\mathbb{Q}$ and that every perfect-square in $\mathbb{Q}$ is some $f_2(y)$. Hence the study of $f_2(y)$ in Pythagoras' theorem translates to studying the digital-correspondence of the second rows, $N(y, 2)$, of the Binomial triangles, $T(y)$, for different values of y. In this case $Q_{1,a}(y) = (2a)y + a(20 + a)$. The following result may be seen as a purely algebraic and rational proof of the existence of Pythagorean triples and of the truth of Pythagoras' theorem for rationals. It establishes, in our context, that some of the values of $Q_{1,a}(y)$ appear in the list of the digital-correspondences of $N(y_0, 2)$.

Theorem 3.1. *Let $a \in \mathbb{Q}\backslash\{0\}$. Then there exist $y \in \mathbb{Q}$ for which $Q_{1,a}(y)$ is a perfect-square. That is, $Q_{1,a}(y) = \delta(N(y+b, 2))$, for some $y \in \mathbb{Q},\ b \in \mathbb{Q}\backslash\{0, a\}$.*

Proof. Since $Q_{1,a}(y)$ is a linear polynomial in y we substitute $y = \alpha_2 x^2 + \alpha_1 x + \alpha_0,\ x \in \mathbb{Q}$, where the values of $\alpha_2, \alpha_1, \alpha_0 \in \mathbb{Q}$ are yet to be known, into $Q_{1,a}(y)$ in order to consider $Q_{1,a}(y)$ for a candidate in the list of values of $\delta(N(y + b, 2))$. That is,

$$Q_{1,a}(y) = Q_{1,a}(x) = (2a\alpha_2)x^2 + (2a\alpha_1)x + a(2\alpha_0 + 20 + a)$$

and, for it to be a complete square of a non-zero rational, we must have $Q_{1,a}(x) \equiv (px + q)^2$ for *all* $p, q, x \in \mathbb{Q}$. The choice of y and the above identity are informed by the one-to-one correspondence in Corollary 2.2, with $n = 2$.

This identity gives $\alpha_2 = \frac{1}{2a}p^2, \alpha_1 = \frac{1}{a}pq$ and $\alpha_0 = \frac{q^2 - a(20+a)}{2a}$, each of which belongs to $\mathbb{Q}$ uniquely, for *every* $p, q \in \mathbb{Q}$. Hence

$$y = \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left[\frac{q^2 - a(20 + a)}{2a}\right]$$

is the required y in $\mathbb{Q}$. Indeed, the discriminant of $Q_{1,a}(x)$ vanishes exactly when $\alpha_2 = \frac{1}{2a}p^2, \alpha_1 = \frac{1}{a}pq$ and $\alpha_0 = \frac{q^2-a(20+a)}{2a}$. □

The conclusion of Theorem 3.1 is that, for every $x, p, q \in \mathbb{Q}$ and $a \in \mathbb{Q}\backslash\{0\}$, the rational solutions, y, to the equation $Q_{1,a}(y) = \delta(N(y+b, 2))$ exist and are given as

$$y = \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left[\frac{q^2 - a(20+a)}{2a}\right].$$

The converse question to this result is that: *if this y is a given rational solution of $Q_{1,a}(y) = \delta(N(y+b, 2))$, does it imply that $x \in \mathbb{Q}$?* This question is addressed in the following theorem.

Theorem 3.2. *Let p, q and a be as in the proof of Theorem* 3.1, *with $p \neq 0$. Every rational solution*

$$y = \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left[\frac{q^2 - a(20+a)}{2a}\right]$$

of

$$Q_{1,a}(y) = \delta(N(y+b, 2))$$

corresponds to a rational value of x.

Proof. It is clear, from Theorem 3.1, that, if $x, p, q \in \mathbb{Q}$ and $a \in \mathbb{Q}\backslash\{0\}$, then the given y is a solution of $Q_{1,a}(y) = \delta(N(y+b, 2))$ and $y \in \mathbb{Q}$. Conversely, let the given y be a rational solution of $Q_{1,a}(y) = \delta(N(y+b, 2))$ and let (α, β, γ) be a rational Pythagorean triple with $\alpha < \beta < \gamma$. (That is, $(Q_{1,a}(y))^{\frac{1}{2}} < (f_n(y))^{\frac{1}{2}} < (f_n(y+a))^{\frac{1}{2}}$). Then $Q_{1,a}(y) = \alpha^2$. This gives, $2ay + a(20+a) = \alpha^2$. That is, $y = \frac{1}{2a}[\alpha^2 - a(20+a)]$. Hence,

$$\frac{1}{2a}[\alpha^2 - a(20+a)] = y = \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left[\frac{q^2 - a(20+a)}{2a}\right]$$

which reduces to a quadratic equation in x given as $p^2x^2 + 2pqx + (q^2 - \alpha^2) = 0$, with $p \neq 0$ (which is necessary in order to be able to find x). The solution of this quadratic is $x = \frac{-q \pm \alpha}{p} \in \mathbb{Q}$. □

Remark 3.3. 1. *On the coefficients of* y: Observe that it is necessary and sufficient for all $\alpha_i,\ i = 0, 1, 2$, to be rational in order to always have $y \in \mathbb{Q}$. The polynomial $Q_{1,a}(x)$ is *always* a perfect-square of members of $\mathbb{Q} \setminus \{0\}$, whatever the value of x in $\mathbb{Q}$. A closer look at Theorem 3.1 therefore reveals a very important conclusion that: *in order to justify the identity used, between* $Q_{1,a}(x)$ *(which is always a perfect-square in* $\mathbb{Q} \setminus \{0\}$*) and* $(px + q)^2$, p *and* q *must necessarily assume all values in* $\mathbb{Q}$, *and not just* $'some'$ *values in* $\mathbb{Q}$. This observation, which is the core of the method of Theorem 3.1, shall be needed when considering rational Pythagorean triples and the non-zero rational solutions (if any) of $u^n + v^n = w^n$, for $n > 2$. See also (1) of Remarks 4.4.

2. *On the constant* b: Now that we have a general expression for $y \in \mathbb{Q}$ that explains the existence of Pythagorean triples, we may compute the constant $b \in \mathbb{Q} \setminus \{0, a\}$ in $Q_{1,a}(y) = \delta(N(y + b, 2))$ as follows: $Q_{1,a}(y) = \delta(N(y + b, 2))$, for rational y, $\iff y^2 + (20 + 2b - 2a)y + (b^2 + 10b + 100 - a^2 - 20a) = 0$ has a perfect-square discriminant $\iff$ the quadratic $2a^2 - 2ba + 10b$, in a, has zero discriminant $\iff b = 20$.

A complete list of all *rational* Pythagorean triples is therefore possible *without* necessarily having to generate them from the basic example of the triple $(3, 4, 5)$, see [5]. This list is contained in the following result.

Corollary 3.4. *Let* $a, p, q, x \in \mathbb{Q}$ *with* $a \neq 0$. *The general expression for any rational Pythagorean triple is then* $(\alpha, \beta, \gamma) =$

$$\begin{cases} ((px+q), \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left(\frac{q^2-a^2}{2a}\right), \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left(\frac{q^2+a^2}{2a}\right)), & \text{if } \alpha < \beta < \gamma, \\ (\left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left(\frac{q^2-a^2}{2a}\right), (px+q), \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left(\frac{q^2+a^2}{2a}\right)), & \text{if } \beta < \alpha < \gamma. \end{cases}$$

Proof. We already know, from Theorem 3.1, that every Pythagorean triple in $\mathbb{Q}$ is

$$(\alpha, \beta, \gamma) = \begin{cases} (\sqrt{Q_{1,a}(y)}, \sqrt{f_2(y)}, \sqrt{f_2(y+a)}), & \text{if } \alpha < \beta < \gamma, \\ (\sqrt{f_2(y)}, \sqrt{Q_{1,a}(y)}, \sqrt{f_2(y+a)}), & \text{if } \beta < \alpha < \gamma, \end{cases}$$

where y is as found in the Theorem. Computing each of these triples with the said y gives the result. □

We arrive at the classical Diophantus's solution to the problem of primitive

solutions to $\alpha^2+\beta^2=\gamma^2$, if we set $x=0$ in Corollary 3.4 and clear the fractions.

Corollary 3.5. *Let $\alpha \in \mathbb{Q}$. Then there are $\beta, \gamma \in \mathbb{Q}$ such that (α, β, γ) is a rational Pythagorean triple. That is, every rational number is a first element of some rational Pythagorean triple.*

Proof. Every $\alpha \in \mathbb{Q}$ may be written as $\alpha = px+q$ for a choice of $p, q, x \in \mathbb{Q}$. The values of β and γ may then be computed from Corollary 3.4 for any $a \in \mathbb{Q} \setminus \{0\}$. □

The particular cases of *non-trivial, primitive* and *integral* Pythagorean triples may be deduced from these Corollaries, which may themselves be extended to include the study of Pythagorean $n-$tuples. See [1], p. 76. The generality inherent in the use of Binomial triangles is evident from the ease with which general Pythagorean triples are handled. We now partition all integral Pythagorean triples into disjoint classes.

Let $\mathbb{P}$ denote the set of all rational Pythagorean triples and denote the subset consisting of integral ones by $\mathbb{P}_{\mathbb{Z}}$. We do not distinguish between (α, β, γ) and $(\pm\alpha, \pm\beta, \pm\gamma)$ as (non-trivial) Pythagorean triples. With this in mind let

$$\mathbb{P}_m = \{(\alpha, \beta, \gamma) \in \mathbb{P}_{\mathbb{Z}} : \ gcd(\alpha, \beta, \gamma) = m\},$$

where $m \in \mathbb{Z}^+$. Clearly $\mathbb{P}_{\mathbb{Z}} = \bigcup_{m \in \mathbb{Z}^+} \mathbb{P}_m$. It may not be clear whether or not this is a disjoint union. This may be addressed by using an appropriate equivalence relation.

Theorem 3.6. *The equality $\mathbb{P}_{\mathbb{Z}} = \bigcup_{m \in \mathbb{Z}^+} \mathbb{P}_m$ is a disjoint union.*

Proof. Define a relation $\sim$ on members of $\mathbb{P}_{\mathbb{Z}}$ as

$$(\alpha_1, \beta_1, \gamma_1) \sim (\alpha_2, \beta_2, \gamma_2) \quad \textit{iff} \quad gcd(\alpha_1, \beta_1, \gamma_1) = gcd(\alpha_2, \beta_2, \gamma_2).$$

It is immediate that $\sim$ is an equivalence relation on $\mathbb{P}_{\mathbb{Z}}$. It is also clear that each $\mathbb{P}_m$ is a typical equivalence class in $\mathbb{P}_{\mathbb{Z}}/\sim$. □

It therefore follows that the set $\{\mathbb{P}_m : m \in \mathbb{Z}^+\}$ is a partition of $\mathbb{P}_{\mathbb{Z}}$.

Remark 3.7. 1. *On parametrization of rational Pythagorean triples*: We may as well use $f_2(\lambda y)$ in the manner in which $f_2(y+a)$ has been considered. The first result here is that, for every $\lambda \in \mathbb{Q} \setminus \{0,1\}$, we always have that

$$f_2(\lambda y) = \lambda^2 f_2(y) + R_{1,\lambda}(y),$$

where $R_{1,\lambda}(y) = 20\lambda(1-\lambda) + 100(1-\lambda^2)$. It can readily be shown that $R_{1,\lambda}(y) = \delta(N(\xi y, 2)),\ \xi \in \mathbb{Q} \setminus \{0,\lambda\}$, *iff*

$$y = \left[\frac{p^2}{20\lambda(1-\lambda)}\right] x^2 + \left[\frac{pq}{10\lambda(1-\lambda)}\right] x + \left[\frac{q^2 - 100(1-\lambda^2)}{20\lambda(1-\lambda)}\right]$$

for all $p, q, x \in \mathbb{Q}$. This gives another outlook to Corollary 3.4.

2. *On equivalence classes of Pythagorean triples*: The function

$$h : \mathbb{P}_{\mathbb{Z}} \to \mathbb{Z}$$

given as $h(\alpha,\beta,\gamma) = \gcd(\alpha,\beta,\gamma),\ \forall\ (\alpha,\beta,\gamma) \in \mathbb{P}_{\mathbb{Z}}$, is well-defined and constant-valued on each $\mathbb{P}_m$. It will be interesting to get the dependence of m on the parameters of the triples in Corollary 3.4. That is, to derive a function $\vartheta : \mathbb{Z}^3 \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Z}^+$ given as $m = \vartheta(p,q,x,a) = \gcd((px+q), \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left(\frac{q^2-a^2}{2a}\right), \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left(\frac{q^2+a^2}{2a}\right))$, where $((px+q), \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left(\frac{q^2-a^2}{2a}\right), \left(\frac{p^2}{2a}\right)x^2 + \left(\frac{pq}{a}\right)x + \left(\frac{q^2+a^2}{2a}\right)) \in \mathbb{P}_{\mathbb{Z}}$, as this will put results on h and $\mathbb{P}_m$ in proper perspectives. It may therefore be useful to note, from Corollary 3.4, that every $(\alpha,\beta,\gamma) \in \mathbb{P}$, with $\alpha < \beta < \gamma$, (respectively, $\beta < \alpha < \gamma$) may be reduced to the (*Diophantine*) form $(\alpha, \frac{\alpha^2-a^2}{2a}, \frac{\alpha^2+a^2}{2a})$, (respectively, $(\frac{\alpha^2-a^2}{2a}, \alpha, \frac{\alpha^2+a^2}{2a})$), (where $\alpha := px+q$ of Corollary 3.4) for any $a \in \mathbb{Q} \setminus \{0\}$. The well-known case of $\vartheta \equiv 1$ follows from here. The above *Diophantine form* of the Pythagorean triples gives a compact expression for the result of Corollary 3.4 and may be further discussed in the light of *Hall's matrices,* [5]. A step towards the derivation of an explicit expression for the function,

$$\vartheta : \mathbb{Z}^3 \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Z},$$

is to note, from the remark following Corollary 3.4, that $\vartheta(p,q,x,a) = 1$ at $x = 0$. We may then write $\vartheta(p,q,x,a) = 1 + x\tau(p,q,x,a)$, where $\tau : \mathbb{Z}^3 \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Z}$, whose explicit expression would enrich the study of $\mathbb{P}_m$.

A direct consequence of this outlook, which follows from the above *Diophantine form* of the Pythagorean triples, is seen in the following.

Corollary 3.8. (Diophantus) *The solutions of* $\alpha^2+\beta^2=\gamma^2$, *with* $\alpha,\beta,\gamma\in\mathbb{Z}$, *are all generated from* $\alpha=m^2-n^2$, $\beta=2mn$ *and* $\gamma=m^2+n^2$, *where* $m,n\in\mathbb{N}$ *and* $\gcd(m,n)=1$.

Proof. As computed above. □

The above Corollary puts the age-long result of Diophantus in its proper perspective; as a *Corollary* in the general scheme of things and not as a starting point to the study of Pythagorean triples. This explains the difficulty encountered in the futile attempts at using techniques of the classical proof given by Diophantus for Corollary 3.7.1 to understand Fermat's Last Theorem, in that

Diophantus' conclusion should only be seen as either the compact form of a simplified Corollary (by setting α *as* $px+q$ *in Corollary* 3.4*) or as a very remote case of a Corollary (by setting* $x=0$ *in Corollary* 3.4 *and clearing the fractions) that has been derived from a general outlook on powers of integers.*

It suggests that Fermat's Last Theorem may not be completely and properly understood (from the classical proof of Corollary 3.7.1) until the framework leading to Corollary 3.7.1 is well established. Indeed we need to completely understand the *natural mathematical emergence* of Pythagorean triples (and not just as a relationship between numbers stumbled on by members of the Pythagoras' Brotherhood) as well as their properties in order to employ them in higher considerations. A framework that may lead to this complete understanding is given here via binomial triangles.

Remark 3.9. *On rings and modules of Binomial triangles:* Let $n\in\mathbb{N}$ be fixed and consider the set $\mathfrak{N}(n):=\{N(y,n):\ y\in\mathbb{Z}\}$. The operations + and $\cdot$, defined on members of $\mathfrak{N}(n)$, as

$$N(y_1,n)+N(y_2,n):=N(y_1+y_2,n)\ \text{ and }\ N(y_1,n)\cdot N(y_2,n):=N(y_1y_2,n),$$

respectively, convert $\mathfrak{N}(n)$ into a commutative ring with identity, $N(1,n)$, whose *field of fractions* is $\{N(y,n):\ y\in\mathbb{Q}\}$. The map $y\mapsto T(y)$ is a one-to-one correspondence between $\mathbb{Z}$ and $\mathfrak{N}(n)$, implying that $\mathfrak{N}(n)$ is indeed

a Noetherian ring whose *ideal* structure is exactly as in $\mathbb{Z}$. If, in addition to these operations above, we define $\alpha N(y,n) := N(\alpha y, n)$ $\alpha, y \in \mathbb{Z}$, then $\mathfrak{N}(n)$ becomes a $\mathbb{Z}-$*module.* These properties on $\mathfrak{N}(n)$ are inherited by the set $\mathfrak{T}_{\mathbb{Z}}$, of all Binomial triangles, $T(y),\ y \in \mathbb{Z}$, leading to the requirements that, for $y_1,\ y_2,\ y,\ \alpha \in \mathbb{Z}$,

$$T(y_1) + T(y_2) := T(y_1 + y_2),\ T(y_1) \cdot T(y_2) := T(y_1 y_2),\ \text{and}\ \alpha T(y) := T(\alpha y).$$

In this formulation the *Pascal triangle,* $T(1)$, *is the (multiplicative) identity of the Noetherian ring* $\mathfrak{T}_{\mathbb{Z}}$ while the *linear functor,* T, may be seen to be both *covariant* and *contravariant* on $\mathbb{Z}$. The ring and module structures of $\mathfrak{T}_{\mathbb{Z}}$ are yet to be studied.

In the light of our success on Pythagorean triples above, we are encouraged to consider the *original* FLT.

4 Fermat's Last Theorem in the context of Binomial triangles

The consideration of each $f_n(y),\ n > 2$, is essentially the study of the other rows, after the 2nd, in each of the Binomial triangles. Following in the direction of our method in §3., we compute the corresponding polynomial, $Q_{n-1,a}(y),\ n > 2$, which is then sought in the list of digital-correspondences to $N(y,n)$.

Lemma 4.1. *Let* $a \in \mathbb{Q} \setminus \{0\}$. *Then* $Q_{n-1,a}(y) = nay^{n-1} + \frac{n(n-1)}{2!}(a^2 + 20a)y^{n-2} + \frac{n(n-1)(n-2)}{3!}(a^3+30a^2+300a)y^{n-3} + \cdots + (a^n + 10na^{n-1} + \cdots + 10^{n-1}na)$, *for all* $n \in \mathbb{N}, y \in \mathbb{Q}$.

Proof. Compute $f_n(y+a) - f_n(y)$. □

In seeking a position for every $Q_{n-1,a}(y),\ n > 2$, in the list of digital-correspondence to $N(y,n)$ we make the following eye-opening observation on $Q_{2,a}(y)$.

Theorem 4.2. (Euler's proof in [3], p. 39.) *There does not exist any $y \in \mathbb{Q}$ for which $Q_{2,a}(y)$ is a perfect cube. That is,*

$$Q_{2,a}(y) \neq \delta(N(y+b,3)),$$

$\forall\ y \in \mathbb{Q},\ b \in \mathbb{Q} \setminus \{0, a\}$.

Proof. We assume the contrary and proceed as in Theorem 3.1. If the polynomial

$$Q_{2,a}(y) = 3ay^2 + (3a^2 + 60a)y + (a^3 + 30a^2 + 300a)$$

is to be a perfect-cube in $\mathbb{Q}$, there must exist $y = \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0 \in \mathbb{Q}$ with $\alpha_3, \alpha_2, \alpha_1, \alpha_0, x \in \mathbb{Q}$, such that, after substituting y into $Q_{2,a}(y)$, the resulting polynomial, $Q_{2,a}(x)$, in x and of degree six, would be identical to $(px^2 + qx + r)^3$, for all $p, q, r \in \mathbb{Q}$. The choice of y and the above identity are informed by the one-to-one correspondence in Corollary 2.2, with $n = 3$.

By making this substitution and comparing the coefficients we arrive at seven relations, namely: $3a\alpha_3^2 = p^3$, $2a\alpha_2\alpha_3 = p^2q$, $a(2\alpha_1\alpha_3 + \alpha_2^2) = p^2r + pq^2$,
$6a(\alpha_0\alpha_3 + \alpha_1\alpha_2) + 60a\alpha_3 + 3a^2\alpha_3 = 6pqr + q^3$, $a(2\alpha_0\alpha_2 + \alpha_1^2) + 20a\alpha_2 + a^2\alpha_2 = pr^2 + q^2r$, $2\alpha_0\alpha_1 + 60a\alpha_1 + 3a^2\alpha_1 = 3qr^2$ and $\alpha_0^2 + (3a^2 + 60a)\alpha_0 + (a^3 + 30a^2 + 300a) = r^3$, from which we are expected to find the rational constants $\alpha_3, \alpha_2, \alpha_1$ and α_0 in terms of p, q and r. A consideration of the first three and last relations give, if $p \neq 0$ is assumed:

$$\alpha_3 = \sqrt{\frac{1}{3a}p^3}, \quad \alpha_2 = \frac{p^2q\sqrt{3a}}{2a\sqrt{p^3}}, \quad \alpha_1 = \frac{(4p^2r + pq^2)}{8a}\left(\sqrt{\frac{3a}{p^3}}\right)$$

and

$$\alpha_0 = \frac{-3a^2 - 60a \pm \sqrt{9a^4 + 356a^3 + 3480a^2 - 1200a + 4r^3}}{2}.$$

These relations imply that $y \notin \mathbb{Q}$, if we use (1) of Remarks 3.3. □

We may as well consider the use of $(px+q)^6$ instead of $(px^2+qx+r)^3$ in the proof of Theorem 4.2. However the use of $(px^2 + qx + r)^3$ accommodates more generality than $(px + q)^6$, since not all quadratics are completely factorisable

over $\mathbb{Q}$. In any of these options the deduced expressions for $\alpha_i,\ i = 0, 1, 2, 3$ do not satisfy the remaining three of the seven relations. A closer look at the proof reveals that this disorder in the identity, $Q_{2,a}(x) \equiv (px^2 + qx + r)^3$, is primarily due to the disparity in the number of terms in $Q_{2,a}(x)$ (which is *seven*) and the number of unknowns in the coefficients of y (which is *four*). There is no way to match these two numbers when $n > 2$, like what we have in the case of $n = 2$ in Theorem 3.1, where there are three terms in $Q_{1,a}(x)$ and *exactly* three unknowns in $y = \alpha_2 x^2 + \alpha_1 x + \alpha_0$. We shall consider, in §7(B) below, the remedy to this *Fermat pathology.*

The method of proof of Theorem 4.2 may be formalized in the following version of the *original FLT.*

Theorem 4.3. (Fermat's Last Theorem) *Let $a \in \mathbb{Q} \setminus \{0\},\ n > 2$. Then there does not exist any $y \in \mathbb{Q}$ for which $Q_{n-1,a}(y)$ is an exact rational of power n. That is,*

$$Q_{n-1,a}(y) \neq \delta(N(y + b, n)),$$

$\forall\ y \in \mathbb{Q},\ b \in \mathbb{Q} \setminus \{0, a\}$.

Proof. We substitute $y = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ into $Q_{n-1,a}(y)$ in Lemma 4.1 and observe that the only choices to be made of each $\alpha_k,\ k = 0, 1, 2, \cdots, n > 2$, for $Q_{n-1,a}(x)$ to be a digital-corresponding of some $N(y_0, n)$, would involve extraction of roots, since powers of y must have been computed in the process of substitution. This leads, via (1.) of Remarks (3.3), to the conclusion that $y \notin \mathbb{Q}$. □

The above method of proof shows that a structural reason for the non-existence of Fermat's triples is because, in seeking a position for $Q_{n-1,a}(y)$ among the values of $\delta(N(y, n))$ every substituted y into $Q_{n-1,a}(y)$ must be raised to some powers, thereby introducing extraction of roots when coefficients of y are later sought. The exception to this is in the cases of $n = 1, 2$, where $Q_{n-1,a}(y)$ are the constant and linear polynomials, respectively. This explains the existence of rational triples, (u, v, w), satisfying the Diophantine equations $u + v = w$ (when $n = 1$ in $u^n + v^n = w^n$) and $u^2 + v^2 = w^2$ (when $n = 2$ in $u^n + v^n = w^n$).

A Galois equivalence of this reason has also been exploited in the next section. It is noted that no extra condition on n, other than the *original* requirement of $n \in \mathbb{Z}$ and $n > 2$, was used to prove FLT.

Remark 4.4. 1. *On the significance of the constant* $a \in \mathbb{Q} \setminus \{0\}$: Corollary 3.5 reveals that every $a \in \mathbb{Q} \setminus \{0\}$ leads to a rational Pythagorean triple, while only *some* $a \in \mathbb{Q}\setminus\{0\}$ gives the integral Pythagorean triples. The same may be deduced from the consideration of the non-zero rational and integral solutions of other Diophantine equations, say, $u^3 - v^3 = w^2$. Indeed, substituting $y = \alpha_1 x + \alpha_0$ into $Q_{2,a}(y)$, which, when identical with $(px+q)^2, \forall\, p, q, x \in \mathbb{Q}$, gives

$$\alpha_1 = \frac{p}{\sqrt{3a}}, \quad \alpha_0 = \frac{2pq - (3a^2 + 60a)\alpha_1}{6a\alpha_1},$$

we see that the non-zero rational solutions of $u^3 - v^3 = w^2$ exist only when $a = \frac{k^2}{3}, \forall\, k \in \mathbb{Z}\setminus\{0\}, p, q, x \in \mathbb{Q},\ p \neq 0$, while the non-zero integral solutions exist only when $a = \frac{1}{3},$ for some $p, q, x \in \mathbb{Z},\ p \neq 0$. It therefore follows that the non-zero rational constant a, in $Q_{n-1,a}(y)$, measures the *distribution* and *density* of solutions of Diophantine equations, when they exist. This may be further explored.

2. *On unique factorization*: The method of this paper is to fix $n-$power of two arbitrary non-zero rationals, say α^n and β^n, and then seek for the possibility of a third one, γ^n, such that $\alpha^n + \beta^n = \gamma^n$, with $\alpha\beta\gamma \neq 0$. In this approach any two of α^n, β^n and γ^n may be fixed. However, our choice of $f_n(y + a) = f_n(y) + Q_{n-1,a}(y)$ over and above the other possibility of

$$f_n(y + a) + f_n(y) = P_{n,a}(y),$$

which leads to the study of the polynomial, $P_{n,a}$, of degree n, is informed by the non-zero rational solutions of $\alpha^2 + \beta^2 = \gamma^2$ which, if considered in the light of $P_{n,a}$, will lead us outside the base field of $\mathbb{Q}$. Indeed, considering any example of the *Pythagorean triples,* say $(3, 4, 5)$, it is advisable, based on our approach, to use 5 and 3 to seek for 4 by factorising the *difference of two squares* $5^2 - 3^2$ as

$$5^2 - 3^2 = (5 - 3)(5 + 3) = (2)(8) = (2)(2)(4) = 4^2$$

(which is a calculation accommodated in $\mathbb{Z}$ or $\mathbb{Q}$) or to use 5 and 4 to seek for 3 by factorising the *difference of two squares* $5^2 - 4^2$ as

$$5^2 - 4^2 = (5-4)(5+4) = (1)(9) = 3^2$$

(which is also a calculation accommodated in $\mathbb{Z}$ or $\mathbb{Q}$) than to use 3 and 4 to seek for 5 by factorising the *sum of two squares* $3^2 + 4^2$ as

$$3^2 + 4^2 = 3^2 - (4i)^2 = (3-4i)(3+4i) = \mid 3+4i \mid^2 = 5^2,$$

which, in the process, leads to the consideration of

$$K(i) := \{a + bi \in \mathbb{C} : \ a, b \in K = \mathbb{Z} \ \text{ or } \ \mathbb{Q}\}$$

outside the base field of $\mathbb{Q}$.
Thus, since factorisation in a fixed base field is the first step at extracting indices out of a number (and now, out of a polynomial), we have settled for the considerations of $Q_{n-1,a}(y)$ (which is the difference $f_n(y+a) - f_n(y)$), while we hope that the polynomials $P_{n,a}$ will be of immense use in aspects of *number theory* allowing the employment of the integral domain $\mathbb{Z}(i)$ or the field $\mathbb{Q}(i)$ of *gaussian numbers* and others. With the above approach we bypass the intricate manipulations involving *unique factorization* in *quadratic fields.* Other properties of the polynomials f_n and $Q_{n-1,a}$, beyond their present use in the proof of FLT, may also be studied.

3. *On non-rational Pythagorean triples*: Our present approach in §3 suggests the study of *non-rational* Pythagorean triples in quadratic fields, $\mathbb{Q}(\sqrt[n]{\sigma})$, (where σ is an nth root-free rational number), in fields, $\mathbb{F}_p$, of prime characteristics and in fields, $\mathbb{Q}_p$, of *p-adic* numbers. The significance of the constant $b = 20$ in the present field of $\mathbb{Q}$, as derived in Theorem 3.1, or as may be derived in any other number field, is still unknown.

5 Galois groups of Fermat Polynomials

The *original* Fermat's Last Theorem does *not* translate to the investigation of solvability of the Galois group, $Gal(Q_{n-1,a})$, of the polynomials $Q_{n-1,a}$,

as it is always expected in the application of Galois theory to polynomials, but to the investigation of the values assumed by the *order,* $\mid Gal(Q_{n-1,a}) \mid$, of $Gal(Q_{n-1,a})$, as we shall show shortly. This approach around the *Fermat polynomials,* $Q_{n-1,a}$, when combined with Theorem 4.3, gives the Galois group version of the original claim of Pierre de Fermat ([3.], p. 3). The results of this section may also be used to deduce the nature of the roots of $Q_{n-1,a}(y) = 0$, when $n > 2$.

Let L/K be a *field extension.* We know that the *degree*, $[L : K]$, of the extension satisfies $[L : K] = 1$ *iff* $L = K$. If the extension is, in addition, *normal* and *separable* we conclude that the Galois group, $Gal(L/K)$, of the extension is the *trivial* group. Now if $Gal(L/K)$ is the Galois group of a polynomial $f \in K[y]$, also written as $Gal(f)$ where L is a splitting field of f over K, then $\mid Gal(L/K) \mid = 1$ *iff* f has *all* its roots in K. That is, $\mid Gal(L/K) \mid = 1$ *iff* f is completely reducible over K. This observation may now be formalised.

Lemma 5.1. *$f \in K[y]$ is completely reducible over K iff $\mid Gal(f) \mid = 1$.*

Proof. Let L be a splitting field of f over K. Then L is a normal finite extension of K and $\mid Gal(f) \mid = 1$ *iff* $[L : K] = 1$ *iff* $L = K$. This means that f is completely reducible over K. □

Let L be a splitting field of f over K. We shall call a polynomial $f \in K[y]$ *incomplete with respect to* L/K whenever it has a linear factor in $L[y]$ which is not in $K[y]$. An *opposite* to the above Lemma is therefore possible.

Lemma 5.2. *Let L/K be a field extension. $f \in K[y]$ is incomplete with respect to L/K iff $\mid Gal(f) \mid \neq 1$.*

Proof. $(y - \alpha) \mid f(y)$ (for some $\alpha \in L \setminus K$) *iff* $K[\alpha]$ is a splitting field of f over K *iff* $[K[\alpha] : K] = 2$ *iff* $[N : K] \geq [K[\alpha] : K] = 2 \neq 1$(where N is the normal closure of $K[\alpha]$) *iff* $\mid Gal(f) \mid = [N : K] \neq 1$. □

We may now study the *Fermat polynomials,* $Q_{n-1,a}$, in the light of these Lemmas.

Theorem 5.3. *Each* $Q_{n-1,a}$, *with* $n > 2$, $a \in \mathbb{Q} \setminus \{0\}$, *is an incomplete member of* $\mathbb{Q}[y]$ *with respect to any field extension of* $\mathbb{Q}$.

Proof. We show that $\mid Gal(Q_{n-1,a}) \mid \neq 1$, *for all* $n > 2$, $a \in \mathbb{Q} \setminus \{0\}$. Let $\alpha_1, \alpha_2, \cdots, \alpha_{n-1} \in \mathbb{C}$ be the roots of the monic polynomial $q_{n-1,a} := \frac{1}{na} Q_{n-1,a}$, then, by the fundamental theorem of algebra,

$$q_{n-1,a}(y) = (y-\alpha_1)(y-\alpha_2)\cdots(y-\alpha_{n-1}) = y^{n-1} - s_1 y^{n-2} + s_2 y^{n-3} + \cdots + (-1)^{n-1} s_{n-1},$$

where

$$s_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_{n-1} = \frac{-(n-1)}{2!}(a+20),$$

$$s_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 \cdots + \alpha_{n-2}\alpha_{n-1} = \frac{(n-1)(n-2)}{3!}(a^2 + 30a + 300),$$

$$\cdots,$$

$$s_{n-1} = \alpha_1\alpha_2\cdots\alpha_{n-1} = \frac{(-1)^{n-1}}{n}(a^{n-1} + 10na^{n-2} + \cdots + 10^{n-1}n)$$

are *non-vanishing* elementary symmetric polynomials.

Now let L be a splitting field for $q_{n-1,a}$ over $\mathbb{Q}(s_1, s_2, \cdots, s_{n-1})$. Since the characteristics of $\mathbb{Q}$ is zero we conclude, from Theorem 10.10 of [7.], p. 178, that $Gal(q_{n-1,a}) = S_{n-1}$. Hence $Gal(Q_{n-1,a}) = S_{n-1}$, because $\alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ are also the roots of $Q_{n-1,a}$. Thus $\mid Gal(Q_{n-1,a}) \mid = (n-1)!$. Since it is known that $(n-1)! = 1$ *iff* $n = 1$ or $n = 2$, we therefore have that $\mid Gal(Q_{n-1,a}) \mid \neq 1$, for all $n \in \mathbb{N}$, with $n > 2$ and $a \in \mathbb{Q} \setminus \{0\}$. □

It is convenient to set S_{n-1} as the trivial group when $n = 1$, so that the popular choice of 0! as 1 is retained.

Remark 5.4.

1. It follows therefore that, for $n > 2$, the normal closure of any splitting field of $Q_{n-1,a}$ over $\mathbb{Q}$ cannot be $\mathbb{Q}$ itself. This is in contrast to the situation for $n = 1, 2$.

2. Since the proof of Theorem 5.3 computes the group $Gal(Q_{n-1,a})$, for *all* $n \in \mathbb{N}$, as S_{n-1}, whose order is $(n-1)!$, we may therefore conclude that

an underlying reason the equation $x^n = y^n + z^n$ *has solutions in non-zero rationals only when* $n = 1$ *(which follows from the field structure of* $\mathbb{Q}$*) and* $n = 2$ *(as established in Theorem* 3.1*), is because only* $0!$ $(=\mid Gal(Q_{0,a}) \mid$*, when* $n = 1$ *in* $\mid Gal(Q_{n-1,a}) \mid)$ *and* $1!$ $(=\mid Gal(Q_{1,a}) \mid$*, when* $n = 2$ *in* $\mid Gal(Q_{n-1,a}) \mid)$ *give the value* 1 *among all* $(n-1)!$*,* $n \in \mathbb{N}$. See the paragraph before Remarks 4.4 for an equivalence form of this reason.

3. *On Wiles-Taylor's proof of FLT*: It is expected that a profound theory would emerge out of the reconciliation of the modern theory of numbers, as has been put to use in [13.], with the properties of the polynomials, $Q_{n-1,a}$, of the present paper. Indeed it would be interesting to link the analysis of Binomial triangles to the *Shimura-Taniyama-Weil* conjecture and the results of *Diophantine geometry*.

6 Arithmetic groups of Diophantine curves

It is clear from above that $Q_{1,a}(x) = (2a)x + a(20+a)$ and that the non-zero rational points, (x, y), on the *Pythagorean* curve

$$P_a : \ y^2 = Q_{1,a}(x) = (2a)x + a(20+a)$$

are given as

$$(x, y) := (p^2\frac{z^2}{2a} + pq\frac{z}{a} + [\frac{q^2 - a(20+a)}{2a}], pz + q),$$

with $p, q, a \in \mathbb{Q} \setminus \{0\}, z \in \mathbb{Q}$. Define the non-empty set $G(P_a) \subset \mathbb{Q} \times \mathbb{Q}$ as $G(P_a) :=$

$$\{(x, y) \in \mathbb{Q}\times\mathbb{Q} : x = p^2\frac{z^2}{2a}+pq\frac{z}{a}+[\frac{q^2 - a(20+a)}{2a}], \ y = pz+q, \forall\ p, q, a \in \mathbb{Q}\setminus\{0\}, z \in \mathbb{Q}\}$$

on which we define a binary operation as follows:

Set $(x_1, y_1),\ (x_2, y_2) \in G(P_a)$ as $(x_1, y_1) = (p_1^2\frac{z^2}{2a} + p_1q_1\frac{z}{a} + [\frac{q_1^2 - a(20+a)}{2a}], p_1z + q_1)$ and $(x_2, y_2) = (p_2^2\frac{z^2}{2a} + p_2q_2\frac{z}{a} + [\frac{q_2^2 - a(20+a)}{2a}], p_2z + q_2)$, where $p_i, q_i, a \in \mathbb{Q} \setminus \{0\},\ z \in \mathbb{Q},\ i = 1, 2$. We set $(x_1, y_1) \cdot (x_2, y_2) := (x, y)$, where

$$x = (p_1p_2)^2\frac{z^2}{2a} + (p_1p_2)(q_1q_2)\frac{z}{a} + [\frac{(q_1q_2)^2 - a(20+a)}{2a}]$$

and

$$y = (p_1p_2)z + (q_1q_2).$$

The following result then becomes immediate.

Theorem 6.1. $(G(P_a), \cdot)$ *is an abelian group whose identity element is given as* $\mathbf{1} = (\frac{z^2}{2a} + \frac{z}{a} + [\frac{1-a(20+a)}{2a}], z+1)$, *with the inverse,* $(x,y)^{-1}$, *of every element,* $(x,y) \in G(P_a)$, *as* $(x,y)^{-1} = ((p^{-1})^2\frac{z^2}{2a} + (pq)^{-1}\frac{z}{a} + [\frac{(q^{-1})^2-a(20+a)}{2a}], p^{-1}z + q^{-1})$.

Proof. We verify the well-known axioms of an abelian group. □

It is known that, for each $a \in \mathbb{Q} \setminus \{0\}$, if $\mathbb{P}^1(\mathbb{Q})$ is the set of rational points of the projective 1−space, then $G(P_a) \simeq \mathbb{P}^1(\mathbb{Q})$ (*cf.* [6.], Theorem $A.4.3.1$), so that each of the groups, $G(P_a)$, may be seen as a concrete realization of $\mathbb{P}^1(\mathbb{Q})$.

The method outlined above for the Pythagorean curve may be employed to compute the arithmetic group of any Diophantine curve. According to Theorem 4.3, the set

$$G(F_a) := \{(x,y) \in \mathbb{Q} \times \mathbb{Q} : y^n = Q_{n-1}(x),\ n > 2\},\ a \in \mathbb{Q} \setminus \{0\},$$

consisting of *non-zero* rational solutions of the *Fermat* curve, $y^n = Q_{n-1}(x),\ n > 2$, is empty. For another example, the Diophantine curve attached to the non-zero rational solutions of $\alpha^3 - \beta^3 = \gamma^2$ is $y^2 = Q_{2,a}(x)$. That is, the curve is

$$E_a :\ y^2 = (3a)x^2 + (3a^2 + 60a)x + (a^3 + 30a^2 + 300a),$$

$a \in \mathbb{Q} \setminus \{0\}$. The non-zero rational points on E_a are then

$$(x,y) = (\frac{p}{\sqrt{3a}}z + \frac{2pq\sqrt{3a} - (3a^2+60a)p}{6ap}, pz + q),$$

where $p, q, z \in \mathbb{Q},\ p, q \neq 0$ and $a = \frac{k^2}{3}, \forall k \in \mathbb{Z} \setminus \{0\}$, from which the group operation may now be defined. The group $G(E_a)$ is infinite, and since the *genus* of the curve E_a is 0, it is also another concrete realization of $\mathbb{P}^1(\mathbb{Q})$. However, finite subgroup of $G(E_a)$ may be constructed from restrictions on its members. See [1], p. 255, for an example of this restriction.

This approach may be seen to have the capability of treating all the finiteness theorems of Diophantine geometry by explicitly computing the arithmetic

group of any Diophantine curve. See [6], p. *viii* for a list of these theorems.

Remark 6.2. On attitude to a proof of FLT.

It is somewhat sad that no one expects any longer that an elementary proof of the Fermat's Last Theorem will ever emerge. This is the conclusion of Michael Rosen [11], some few years after the long, indirect and very difficult proof of Andrew Wiles and Richard Taylor was given in [12] and [13]. This is borne out of the fact that many mathematicians were glad that the simple-looking embarrassing statement of the Theorem could at least be *said to have been finally proved* in 1994, after about 358 years of sustained attacks by the most brilliant of each generation. What is really more grieving to the theory of numbers and her workers is the fact that the *Wiles-Taylor proof* did not only purport to have proved FLT but buried the totality of both the Theorem and the expectations of the rich theory that has been anticipated to emerge from its eventual proof, thus lending credence to the thought that FLT is an isolated result of the theory of numbers.

This is exactly what is meant when Rosen said: *To the degree that they (i.e., the partial results which appeared over the course of the centuries and which attempted to shed light on FLT) deal strictly with FLT and not with any broader class of problems, it is an unfortunate fact that they are now obsolete.* Our approach in this paper therefore brings out the missed opportunities of the last three centuries that would have led straight to an easy understanding of the entire landscape of Diophantine Analysis of Equations, had it not been overlooked repeatedly. Indeed, if the FLT is the non-existence result of rational solutions of $u^n + v^n = w^n,\ n = 3, 4, 5, \cdots$, the polynomials, $Q_{n-1,a},$ and $P_{n,a}$, deduced from it in §4 (and others that may be deduced from other Diophantine equations) are worthy of an independent study, as done in §5., and of potential application to a wide range of subjects, as shown in the present section.

Our present approach has the added advantage in that it *does not deal strictly with FLT*, but, as may be seen in the last two sections, it is applicable to a wide range of subjects in algebraic number theory.

7 Direct consequences of the Fermat's Last Theorem

Contrary to what some experts in the modern theory of numbers would want us to believe, that the truth of the Fermat's Last Theorem (FLT) has no single application (even within number theory!) (see [4] and [8], we consider some direct consequences of the Theorem in the form of open problems in the fields of topology, number theory, ring theory and Galois theory, all of which are deduced from the outlook of the proof of the Theorem given above. Hints on how these problems could be resolved are also included. It is our modest conclusion that the absence of these problems in the aftermath of the 1994 Wiles-Taylor's proof of FLT is due mainly to the approach of study, which *wrongly* presupposes that FLT is an isolated result, and not that the truth of FLT has no single consequence.

7.1 On non-rational Fermat triples

It is well-known that there are several *quadratic* fields between the fields $\mathbb{Q}$ and $\mathbb{R}$, or between $\mathbb{Q}$ and $\mathbb{C}$. One way of generating these subfields of $\mathbb{R}$ or of $\mathbb{C}$ is by the computation of the splitting fields of polynomials in, say, $\mathbb{Q}[X]$ or $\mathbb{Q}[X_1, \cdots, X_m]$. The following problems are proposed:

7.1.1 On non-rational Fermat triples.

Which of these splitting fields over $\mathbb{Q}$ will uphold the truth of the FLT? That is, on which subfields, $\mathbb{F}$, of $\mathbb{R}$ or $\mathbb{C}$ is $Q_{n-1,a}(y) \neq \alpha^n$ for any $y, \alpha \in \mathbb{F}$. The cases of $\mathbb{F} = \mathbb{Q}(\sqrt[n]{\sigma})$, $\mathbb{F}_p$, $\mathbb{Q}_p$ have earlier been posited in Remark 4.4(3).

7.1.2 On non-rational Fermat triples

Which of the splitting fields of the fermat polynomials, $Q_{n-1,a}$ (as may be deuced from Theorem 5.3, would admit the truth of FLT and why?

7.1.3 On non-rational Fermat triples

What is the numerical value and significance of the constant $b \in \mathbb{F}$ in the equation $Q_{n-1,a}(y) = \delta(N(y+b,n)), n \in \mathbb{N}$, in those fields $\mathbb{F}$ that *do not* admit the truth of the FLT? For the case of $n = 2$ and $\mathbb{F} = \mathbb{Q}$ we already know, from Remark 3.3(2), that $b := b_{2,\mathbb{Q}} = 20$.

7.2 Correct generalization of $\alpha^2 + \beta^2 = \gamma^2$

The question has always been asked whether FLT was the right question to the generalization of the Babylonian results on the sum of two (integral or rational) squares being written as a (integral or rational) square. It has been posited ([2.]) that the correct analogue to the generalization of $\alpha^2+\beta^2 = \gamma^2$ to cubes is not to consider $\alpha^3 + \beta^3 = \gamma^3$, but to seek non-zero rational solutions to $\alpha^3+\beta^3+\gamma^3 = \delta^3$, while the situation for fourth powers is $\alpha^4+\beta^4+\gamma^4+\delta^4 = \zeta^4, \cdots$.

In short, the conclusion of K. Choi [2] is that if rational solutions of

$$x_1^n + \cdots + x_k^n = z^n$$

are sought, it is necessary to first have that $k \geq n$, though *no* specific way of attacking this observation was suggested by him or by Davis Wilson (See Diophantine Equations on the website of $WolframMathWorld$) other than to state some conjectures and list the following suggestive examples: $3^2+4^2 = 5^2$ (where $k = 2 = n$), $3^2 + 4^2 + 12^2 = 13^2$ (where $k = 3 > 2 = n$), $3^2 + 4^2 + 12^2 + 84^2 = 85^2$ (where $k = 4 > 2 = n$), $3^3 + 4^3 + 5^3 = 6^3$ (where $k = 3 = n$), $4^4+6^4+8^4+9^4+14^4 = 15^4$ (where $k = 5 > 4 = n$), $4^5+5^5+6^5+7^5+9^5+11^5 = 12^5$ (where $k = 6 > 5 = n$), $\cdots$. It is clear that there may be other examples that would escape the above scheme. We believe that the prospect of the case $k \geq n$ above should not preclude the investigation of the existence, or otherwise, of rational solutions of $x_1^n + \cdots + x_k^n = z^n$ for $k < n$, though it may require more than 100 pages if we are to expect a proof of the Wiles-Taylor's magnitude (which was the case $k = 2 < n$) to address *each(!)* of the cases $2 \neq k < n$ and the new cases of $k \geq n$.

We now propose an approach to this study (of both $k \geq n$ and $k < n$) based on an observation already contained in the proofs of Theorems 4.2 and 4.3.

With $k = 2 < n = 3$, we already have the non-existence of rational solutions of $x_1^3 + x_2^3 = z^3$ as Theorem 4.2 above. A second look at the proof of this Theorem (as explained in the paragraph following it) shows that the conclusion of the Theorem stems from "the disparity in the number of terms in $Q_{n-1,a}(x)$ (which is seven) and the number of unknowns in the coefficients of y (which is four)." It was also reported that there was *no way* to match these two numbers in the case $k = 2 < n = 3$, unless we increase the number of cubes being added. That is, unless we increase k beyond 2. Indeed if $k = 3 = n$, then $x_1^3 + x_2^3 + x_3^3 = z^3$ may be recast as $z^3 - x_1^3 - x_2^3 = x_3^3$, which translate (in the context of Binomial triangles) to studying a cubic polynomial $R_{3,a,b}$, given as

$$R_{3,a,b}(y) := f_3(y + a) - f_3(y + b) - f_3(y),$$

for $y, a, b \in \mathbb{Q},\ a \neq 0,\ b \neq 0$. We then seek $y \in \mathbb{Q}$ for which $R_{3,a,b}(y) = \delta(N(y+c, 3))$, $c \in \mathbb{Q}\setminus\{0, a, b\}$, where the *lacuna* noted in the proof of Theorem 4.2 would have been filled due to the inclusion of the *new* term, $f_3(y + b)$, in $R_{3,a,b}(y)$.

It is clear, form this paper, how the above outlined approach for $k = 3 = n$ may be achieved for all $k = 3 \geq n$ and indeed for any $k \geq n$, whenever n is fixed in $\mathbb{N}$. We need only refer to Lemma 4.1 for orientation on the general situation of $k = 2 < n$, which may itself be extended to the most general case of $k < n$.

The present problem, as outlined above, is a strong argument in favour of our methods of handling the FLT and in the complete understanding of the study of Diophantine equations.

7.3 On Fermat metric

We consider here a direct consequence of FLT and fix the positive integer $n \geq 3$. It is already shown that the polynomial, $Q_{n-1,a}(y)$, of Lemma 4.1 is $\neq \delta(N(y+b, n))$ as long as $y \in \mathbb{Q}\setminus\{0, a\}$, but that $Q_{n-1,a}(y) = \delta(N(y+b, n))$, whenever $y \in \mathbb{R}\setminus\{0, a\}$, for any choice of $b \in \mathbb{R}$. A serious question along this line of thought is how the topologies on the two fields of $\mathbb{Q}$ and $\mathbb{R}$ contribute to the above conclusions about $Q_{n-1,a}(y)$ and $\delta(N(y + b, n))$, since we know that, in the *Euclidean metric,* $\overline{\mathbb{Q}} = \mathbb{R}$. However, there are other topologies on $\mathbb{Q}$ in whose metric the completion, $\overline{\mathbb{Q}}$, would not be $\mathbb{R}$. We mention the

well-known $p-$adic completion, $\overline{\mathbb{Q}} = \mathbb{Q}_p$. It is still an open problem, included in §A. above, to find $a \in \mathbb{Q}_p \setminus \{0\}$, for which $Q_{n-1,a}(y) = \delta(N(y+b,n))$, for any $y \in \mathbb{Q}_p \setminus \{0,a\}$. These and many other examples of topologies and metrics on the subsets, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}_p, \cdots$, of $\mathbb{R}$ (or of $\mathbb{C}$) lead to the consideration of the following definition:

Definition 7.1. *Let $(\overline{X}, \rho)$ be the completion of a metric space, (X, ρ). The metric, ρ, is called a fermat metric if whenever FLT holds in (X, ρ) it also holds in $(\overline{X}, \rho)$. We then refer to the pair (X, ρ) as a fermat metric space.*

In other words a *fermat metric* is a metric $\rho : X \times X \to [0, \infty)$ for which $Q_{n-1,a}(y) \neq \alpha^n$, for all $y,\ \alpha \in (\overline{X}, \rho)$. If $X = \mathbb{N},\ \mathbb{Z}$ and $x,\ y \in X$, we set ρ as $\rho(x,y) =\mid x - y \mid$, then (X, ρ) is a *fermat metric space* while $(\mathbb{Q}, \rho)$ is not.

In the general situation of the above definition one would like to know if every metric on a fermat metric space is a fermat metric and which of the topologies on X may be deduced from a fermat metric. Also, for which example of the set, X, (whether finite, discrete, Baire, $\cdots$) is every metric a fermat metric? A description of the open sets, closed sets, accumulation of a set, interior of a set, base of the topology, $\cdots$, in terms of the fermat polynomials, $Q_{n-1,a}(y),\ y \in X$, will contribute richly to our understanding of *polynomial-induced metrics*. An open problem in §A. is to know whether or not the $p-$adic metric is a fermat metric on $\mathbb{Q}$.

7.4 Galois theory of Fermat fields

This section may be seen as an analytic continuation of the exploration in §7(A) above. Let $F_i,\ 1 \leq i \leq r$ be a collection of subfields of $\mathbb{R}$ (or $\mathbb{C}$). We shall call any member of this collection a *fermat field* whenever FLT holds on it.

Definition 7.2. *Let $\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r \subset \mathbb{R}$ (or $\mathbb{C}$) be an increasing collection of fields. We refer to the collection, $F_i,\ 1 \leq i \leq m,\ m \leq r$, as a collection of nested fermat fields of length m whenever (a.) $\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_m \subset \mathbb{R}$ (or $\mathbb{C}$) and (b.) each $\mathbb{F}_i,\ 1 \leq i \leq m$, is a fermat field.*

Some of the important questions on this definition are:

a. How many collection of nested fermat fields are there for each exponent $n \geq 3$?

b. Is there a relationship between the length of a nested fermat fields and each n?

c. In the general case of $\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r \subset \mathbb{R}$ (or $\mathbb{C}$), at what field, $\mathbb{F}_k,\ 1 \leq k \leq r$, does FLT holds for which it fails at $\mathbb{F}_{k+1}$ and what is the relationship of k to n?

d. What are the properties of $\mathbb{F}_k$ and $\mathbb{F}_{k+1}$ in $(c.)$ above and how does the Galois groups, $Gal(\mathbb{F}_{t+1}/\mathbb{F}_t),\ t = 1, 2, 3, \cdots$, of the field extensions, $\mathbb{F}_{t+1}/\mathbb{F}_t$, contribute to these conclusions above?

e. Is $Gal(\mathbb{F}_{t+1}/\mathbb{F}_t)$ in any relationship with $Gal(Q_{n-1,a})$ (which has been computed above to be S_{n-1}) or with $Gal(P_{n,a})$ (with $P_{n,a}$ as in Remarks 4.4(2))?

f. How does an arithmetic group (if non-empty) of any Diophantine curve contributes to all these open problems?

We are hoping to attack some of these open problems in collaboration with others.

Acknowledgement: The author is grateful to Professor Phillip Ogunbona of University of Wollongong, Australia, for his encouragement leading to the revision of preprint [9] and submission of this work.

References

[1] Andreescu, T., Andrica, D. and Cucurezeanu, I., *An introduction to Diophantine equations*, Birkhäuser-Verlag, 2010.

[2] Choi, K., *A note on Fermat's Last Theorem- Was it a right question?*, www.public.iastate.edu/∼kchoi/fermat.html.

[3] Edwards, H. M., *Fermat's Last Theorem*, Graduate Text in Mathematics. Springer-Verlag, **50**, 1984.

[4] Frey, G., The way to the proof of Fermat's Last Theorem,*www.backup.itsoc.org/review/05pl1.pdf*, **17**, (1997), 1-17.

[5] Hall, A., Geneology of Pythagorean triples, *Math. Gaz.*, LIV. XI**15**, (1970), 377-379.

[6] Hindry, M. and Silverman, J.H., *Diophantine geometry, an introduction*, Graduate Text in Mathematics, Springer-Verlag, 2000.

[7] Howie, J. M., *Fields and Galois Theory*, Springer Undergraduate Mathematics Series. Springer-Verlag, 2006.

[8] Mazur, B., Number theory as gadfly, *American Mathematical Monthly*, (August-September, 1991), 593-610.

[9] Oyadare, O.O., On the application of Newtonian triangles to decomposition theorems, Preprint available at *www.scribd.com/mobile/doc/86763873*, (March, 2012).

[10] Page, A., *Algebra*, University of London Press Ltd, First Published 1947, Reprinted, 1950.

[11] Rosen, M., Book Review of Paulo Ribenboim's, Fermat's Last Theorem for Amateurs, *Notices Amer. Math. Soc.*, **47**, (2000), 474-447.

[12] Taylor, R. and Wiles, A.J., Ring theoretic properties of certain Hecke algebras, *Ann. of Math.*, **141**, (1995), 553-572.

[13] Wiles, A.J., Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.*, **141**, (1995), 443-551.