Chapter 3

Algebraic Equations and Fermat's Last Theorem

Abstract

Diophantine equations are known from their comments by Fermat, many concern geometrical assertions, a large part are algebraic equations. Pythagore's equality enables to prove algebraic equations and Fermat's last theorem, with a property of the binomial coefficients. I give simple proofs of these theorems and several generalizations. Fermat's theorems 2.3.3, 3.2.6 and most algebraic equations were unproved.

3.1 Algebraic Equations

The diophantine equations are their origin in Diophant's geometry (250 A.D.), his work has been partly translated and published by Fermat with some proofs, more proofs have been published latter by Euler Legendre and others during the 17–19th centuries. A diophantine equation is an equation on $\mathbb{N}^k$ with integer coefficients, for some $k > 1$. Most equations below are known from Fermat's letters, the proofs are new or simpler than the proofs already published.

Proposition 3.1.1 *The area of a rectangle triangle is not a square in* $\mathbb{N}$.

Proof. From the equality $(a^2+b^2)^2 = (a^2-b^2)^2 + 4a^2b^2$, the edges of the triangle can be choosen as $x = a^2 - b^2$, $y = 2ab$ and the hypotenuse is $z = a^2 + b^2$, with $a \neq b$. Its area is

$$A = ab(a^2 - b^2).$$

We may assume that $\gcd(a^2 - b^2, a^2 + b^2, 2ab) = 1$, then $a^2 \pm b^2$ are odd, one of a and b is even and the other is odd, moreover $\gcd(a, b) = 1$. The existence of a solution for the equation $A = B^2$ requires that $a^2 - b^2$ and ab are squares since they are mutually prime.

Let $a = \alpha^2$ and $b = \beta^2$, the equation $a^2 - b^2 = X^2$ is equivalent to

$$(\alpha^2 - \beta^2)(\alpha^2 + \beta^2) = X^2$$

with X odd. It follows that $\alpha^2 - \beta^2 = c^2$ and $\alpha^2 + \beta^2 = d^2$ where c and d are odd, α is odd and β even

$$2a = c^2 + d^2, \quad 2b = d^2 - c^2.$$

Let k_0 be the largest integer such that $2^{2k_0} \mid b$ and let $b = 2^{2k_0}b_1$ where b_1 is an odd square. The equality $d^2 - c^2 = 2b$ implies $d^2 - c^2$ is multiple of 2^{2k_0+1}. Let $d = 2u + 1$ and $c = 2v + 1$

$$8 \mid (d^2 - c^2) = 4(u^2 + u + v^2 + v)$$

hence

$$2y = 4ab = d^4 - c^4 = 2^{2(k_0+2)}Y^2,$$

where Y is odd. It follows that $2^{2(k_0+1)} \mid b$ which is contradictory. □

The surface of Pythagore's triangles with edges $(x, y,)$ is always an even integer by Theorem 3.2.1. Table (3.1) shows that two different rectangular triangles may have the same surface.

Table 3.1: Surface of rectangular triangles

$(x, y,)$	S
$(3, 4, 5)$	6
$(5, 12, 13)$	30
$(7, 24, 25)$	48
$(8, 15, 17)$	60
$(21, 20, 29)$	60
$(35, 12, 37)$	60

By the same arguments, $a^4 - n^2b^4$ cannot be a square with one of a and nb odd and the other even, in particular the equation $a^4 - b^4 = z^4$ cannot be solved.

Corollary 3.1.2 *The surface of a rectangular triangle in* $\mathbb{Q}^{*3}$ *is even.*

Proof. A solution should satisfy

$$1 = \frac{ak}{bn}\Big(\frac{k^2}{n^2} - \frac{a^2}{b^2}\Big)$$

equivalently $b^3n^3 = ak(b^2k^2 - a^2n^2)$. A rectangular triangle with edges $2xy$ and $x^2 - y^2$, where $x = bk$ and $y = an$, has the area $abkn(b^2k^2 - a^2n^2)$ but it cannot be equal to b^4n^4 by Proposition 3.1.1. □

Proposition 3.1.3 *The equation*

$$x^4 + y^4 = z^2$$

has no solution such that $\gcd(x, y) = 1$ *in* $\mathbb{N}^{*3}$.

Proof. Let $z = a^2 + b^2$ be the hypothenuse of a triangular triangle with edges $x^2 = a^2 - b^2$ and $y^2 = 2ab$ in $\mathbb{N}$, where $\gcd(a^2 - b^2, 2ab) = 1$, one of a and b is even and the other is odd, they are mutually primes, x odd, y even and z is odd. The equations $x^2 = a^2 - b^2$ and $y^2 = 2ab$ imply $a - b$, $a + b$, a and b are squares, let

$$a = \alpha^2, \quad b = \beta^2$$

where a and α are odd, b and β are even. From the equality $y^2 = 8a\beta^2$, $4 \mid y$ and β is even. Let $\beta = 2^c\beta_2$ with β_2 odd, the equation $y^2 = 2ab$ is equivalent to $y^2 = 2^{2c+1}a\beta_2^2$ and y should be a multiple of 2^{c+1} which is contradictory. □

Proposition 3.1.4 *The equation*

$$x^{2n} + y^{2n} = z^2$$

has no solution in $\mathbb{N}^{*3}$.

The proof is similar.

Proposition 3.1.5 *The equation*

$$x^4 - 2y^4 = z^2$$

has no solution in $\mathbb{N}^{*3}$.

Proof. Let $d = \gcd(x, y)$, then $d^2 \mid z^2$ and we have to consider the equation with $\gcd(x, y) = 1$. Solutions of $2y^4 + z^2 = x^4$ should satisfy

$$z = a^2 - b^2, \quad x^2 = a^2 + b^2, y^4 = 2a^2b^2$$

so x and z are odd and y is even, hence a or b should be even. Let $y = 2c$ therofore $8c^4 = a^2b^2$, one of a and b is even and the other one is odd. Let $a = 2^k\alpha$ with α odd, the equation $y^4 = 2a^2b^2$ becomes equivalent to

$$8c^4 = 2^{2k}\alpha^2b^2$$

with $k \geq 2$ and c is even. Let $c = 2^n d$ with d odd, as $2^{4n+3}d^4 \neq 2^{2k}\alpha^2b^2$, there is no solution. □

Proposition 3.1.6 (Fermat) *There exist integers a, b, c and x such that*

$$x^2 = a^4 + b^4 + c^4.$$

For example, the sum $12^4 + 20^4 + 15^4$ is the square of 481.

Proposition 3.1.7 *The equation*

$$x^3 + y^3 = 3z^3$$

has no solution in $\mathbb{N}^{*3}$.

Proof. We may assume without loss of generality that $\gcd(x, y, z) = 1$, this implies $3 \nmid y$ and $3 \nmid x$. Moreover, $z \nmid x$ and $z \nmid y$ for $a^3 + b^3 \neq 3$ in $\mathbb{N}^{*2}$, where $x = az$ and $y = bz$. The equation is equivalent to

$$\begin{aligned} 4(x^3 + y^3) &= (x + y)(2x - y - i\sqrt{3}y)(2x - y + i\sqrt{3}y) \\ &= (x + y)\{(2x - y)^2 + 3y^2\} = 12z^3, \end{aligned} \tag{3.1}$$

$$\tag{3.2}$$

and

$$(x + y)(2x - y)^2 = 3\{4z^3 - y^2(x + y)\} \tag{3.3}$$

these equalities imply $3 \mid (2x - y)$ or $3 \mid (x + y)$.

Let $3 \mid (x + y)$, then $9 \mid \{(x + y)^3 - 3xy(x + y)\} = x^3 + y^3$ this entails $3 \mid z$, then by (3.1), either $3 \mid (2x - y)$ or $3^4 \mid (x + y)$. In the first case, it follows that $3 \mid x$ which is excluded, the second case proves that $3^{4k} \mid (x + y)$ for every k, so x and y are infinite and there is no solution.

Let $3 \mid (2x - y)$, by (3.1)

$$3 \mid (2x - y)^2 + 3y^2 = 4(x^2 - xy + y^2)$$

it follows that $3 \mid x(2x - y) - (x^2 - xy + y^2) = x^2 - y^2$. Since $3 \nmid (x + y)$, $3 \mid (x - y)$ and $3 \mid (2x - y) - (x - y) = x$, which is excluded. □

The proof of Proposition 3.1.7 discusses the divisibility of the prime factors of x^3+y^3 by 3, the same arguments prove that the equation

$$x^3+y^3=3kz^3$$

has no solution in $\mathbb{N}^{*3}$, for every k such that $3 \nmid k$. Legendre (1825) proposed a global and intricated proof of the unsolvability of the equations

$$x^3+y^3=Az^3$$

in $\mathbb{N}^{*3}$, for $A=1,3,5,6,2^k$, $k \geq 1$. The case $A=1$ is a special case of Fermat's last theorem proved in the next section and the above proof for $A=3$ and 6 is much simpler an direct, the other cases are left as exercises.

Proposition 3.1.8 *The equation*

$$x^2+2=y^3 \tag{3.4}$$

has a single integer solution $(x,y)=(5,3)$.

Proof. From the equation, x and y have the same parity and they cannot be even. Let $x=2a+1$ and $y=2b+1$, the equation

$$2(a^2+a)+1=4b^3+3(2b^2+b)$$

implies $b=1$, then $(x,y)=(5,3)$ is the unique solution, or b is odd. If $b>1$, let $y=4c+3$, c is even and $y=8d+3$, with an integer d. Two cases must be considered

1. $x=16k+1$ and d is odd, $y=16m+11$, with m odd and $k=1 \pmod 3$, therefore $x=2 \pmod 3$ and $y=32m'+27$,
2. $x=8k+3$ and d is even, $y=16m+3$, with m even and k odd, therefore $x=16k'+11$ and d is odd, $y=32m'+19$,

but trying to solve the equation under one of these conditions leads to contradictions. □

There exist infinitely many integers k such that the equation

$$x^2+k=y^3$$

has solutions, k being defined from (x, y) in $\mathbb{N}^{\otimes 2}$. The question of Proposition 3.1.8 extends to find integer solutions (x, y) for integers $k > 2$ and to characterize the integers k for which the equation may be solved.

Let k be odd, with x even and y odd, a necessary condition to solve the equation is $\frac{y-1}{2}$ and $\frac{k-1}{2}$ have the same parity. Furthermore, x is odd and y is even if and only if $k = 7 \pmod 8$.

Let k be even, if x and y are even, $\frac{x}{2}$ and $\frac{k}{4}$ have the same parity. If x and y are odd, $\frac{y-1}{2}$ and $\frac{k}{2}$ have the same parity.

Proposition 3.1.9 *The equation*

$$x^2 + 4 = y^3 \tag{3.5}$$

has the unique integer solutions $(x, y) = (2, 2)$ *and* $(11, 5)$.

Proof. Let x and y be even, $x = 2a$ and $y = 2b$ implies $a^2 + 1 = 2b^3$ and a is odd, $(x, y) = (2, 2)$ is a solution. If $a > 1$, let $a = 2\alpha + 1$, the equation $4(\alpha^2 + \alpha) + 2 = 2b^3$ implies b is odd. Denoting $b = 2c + 1$

$$\begin{aligned} 2(\alpha^2 + \alpha) &= (b-1)(b^2 + b + 1) \\ \alpha^2 + \alpha &= c(4c^2 + 6c + 3) \end{aligned}$$

hence $b = 1 \pmod 4$ and $y = 2 \pmod 8 = 2 + 8k$ but

$$\frac{\alpha^2 + \alpha}{2} = k(3 + 12k + 8k^2)$$

and there is no solution. Let $x = 2a + 1$ and $y = 2b + 1$ be odd

$$2(a^2 + a) + 2 = 4b^3 + 3(2b^2 + b)$$

implies b is even and $(11, 5)$ is solution with $b = 2$. If $b > 2$, the equation is impossible modulo 3. □

Proposition 3.1.10 *The equation*

$$x^3 - 2ny^3 = 1 \tag{3.6}$$

does not have integer solutions (x, y, k).

Proof. From (3.6), x is odd. With $x = 2a + 1$

$$4a^3 + 6a^2 + 3a - ny^3 = 0$$

then $a^3 - ny^3 = 0 \pmod 3$ and $a - ny^3 = 0 \pmod 2$, they are contradictory conditions for the parities of a and ny^3. □

Proposition 3.1.11 *Let $m > 1$ in $\mathbb{N}$ such that $2 \nmid z$, the equation*

$$x^3 + y^3 = 2^m z, \tag{3.7}$$

has infinitely many integer solutions.

Proof. The integers x and y have the same parity and we may assume that $z = 2^c\xi$ where ξ is odd and $c \geq 0$. If they are even, $2^\alpha \mid x$ and $2^\beta \mid y$ only if $3(\alpha \wedge \beta) \leq m$. Dividing x and y by $2^{[\frac{m+c}{3}]}$, their ratios have the same parity if $\alpha \wedge \beta > [\frac{m+c}{3}]$, otherwise they are odd, $\xi \mid (x^2 - xy + y^2)$ which is odd and $x + y = 0 \pmod{2^m}$. □

Under the conditions, there is a large number of solutions, the next table presents some of them.

Table 3.2: Solutions of equation (3.7)

m	(x, y, z)
1	(1,3,14), (3,3,27)
2	(1,3,7), (2,4,18)
3	(2,4,9), (4,4,16), (5,3,19)

Proposition 3.1.12 *The equation*

$$x^n + 1 = y^2, \tag{3.8}$$

with $n > 2$, has a single non trivial integer solution $(x, y, n) = (2, \pm 3, 3)$.

Proof. The equation does not have solutions with $x = 1$ or $y = 2$. Let $x > 1$, from the equality $x^n = (y - 1)(y + 1)$, there exist integers h and k between zero and n with

$h+k>0$, $a>1$ and $b>1$ such that $x=ab$, $y-1=a^kb^h$ and $y+1=a^{n-k}b^{n-h}$. It follows that $a^{n-k}b^{n-h}-a^kb^h=2$ and $a^{n-k}b^{n-h}-a^kb^h=2y$. We first consider the equality $a^{n-k}b^{n-h}-a^kb^h=2$, if $k=0$ and $0<h<n$ it become $a^nb^{n-h}-b^h=2$ and there is no solution, the case $h=0$ and $0<k<n$ is similar, if $0<h,k<n$ let H, respectively k, be the minimum of h and $n-h$, respectively k and $n-k$, it is impossible that $a^Kb^H=1$ or 2 and there is no solution. □

The bilinear equations for integers have always infinitely many solutions in $\mathbb{Z}$. For example

$$65x+14y=4$$

where $\gcd(65,14)=1$, has the solutions $(x,y)=(2-14k,65k-9)$, with k in $\mathbb{Z}$, according to Lagrange's method. The equation

$$24x+48y+5z=4$$

has the solutions $(x,y,z)=(-1-2h-3k,1+h-2k,6k-4)$ with m and n in $\mathbb{Z}$. Solving it requires to solve two bilinear equations, $3a+5z=4$ and $8(x+2y)=a$.

Theorem 3.1.13 *Every linear diophantine equation*

$$ax+by=n$$

with variables x and y and constants a, b and n in $\mathbb{Z}$ has infinitely many solutions.

Proof. For every d such that $\gcd(a,b)=d$ and let $n=dm$, the equation is equivalent to $\alpha x+\beta y=m$ with $\gcd(\alpha,\beta)=1$, $\gcd(\alpha,n)=1$ and $\gcd(\beta,n)=1$. Let

$$x=km-\beta h$$

with integers h and k, the equation becomes $m(\alpha k-1)+\beta(y-\alpha h)=0$ where h and k satisfy $\beta \mid (\alpha k-1)$ and $m \mid (y-\alpha h)$, it has infinitely many solutions h and k. □

As a consequence, every linear diophantine equation with k variables can be solved by decreasing progressively its degree. It splits into $k-1$ independent bilinear equations and it has infinitely many solutions.

Bilinear equations with a higher exponent are elliptic equations.

Theorem 3.1.14 *Every elliptic equation*

$$ax^2 + by^2 = n$$

with variables x and y such that $\gcd(x, y) = 1$ and with constants a, b and n in $\mathbb{Z}^*$ such that $\gcd(a, b) = 1$ has solutions and they exists a finite number of values $x_1 \pm x_2$ and $y_1 \pm y_2$.

Proof. There exist solutions such that $\gcd(a, y^2) = n$ or $\gcd(b, x^2) = n$. Let (x_1, y_1) and (x_2, y_2) be solutions, from the equation

$$a(x_1^2 - x_2^2) + b(y_1^2 - y_2^2) = 0 \tag{3.9}$$

we have $a \mid (y_1^2 - y_2^2)$ and $b \mid (x_1^2 - x_2^2)$. Let $bk = x_1 \pm x_2$ and $am = y_1 \pm y_2$, multiplying the first equation by k and the second one by m and adding them to (3.9) entails that k and m are solutions of the equation

$$am^2 + bk^2 \pm 2(kx_2 \pm my_2) = 0.$$

For every k there exist no more than two values of m satisfying this equality and with each values, k is solution of polynomial of degree two. They determine at most two values of $x_1 \pm x_2$ and four values of $y_1 \pm y_2$. □

Example. The elliptic equation $7x^2 - 4y^2 = 31$ has the solutions $(\pm 5, \pm 6)$. Let $(5 + k, 6 + m)$ be another solution, then k even and m satisfies

$$7(k^2 + 10k) = 4(m^2 + 12m)$$

and $(-10, -12)$ is a solution. The case k or m odd is impossible. Let $k = 2a$ and $m = 2b$ such that

$$7(a^2 + 5a) = 4(b^2 + 6b)$$

this implies $a = 2c$ with $7(2c^2 + 5c) = 2(b^2 + 6b)$ hence $c = 2d$ with (b, d) such that $7(4d^2 + 5d) = (b^2 + 6b)$, it has a solution $(b, d) = (-8, -42)$ therefore another solution of the equation is $(x, y) = (-59, -78)$ and it has a finite number of solutions.

The equation of Theorem 3.1.14 has infinitely many solutions if n is variable in $\mathbb{Z}^*$. If the last term is variable with an exponent, the number of solutions may be finite.

Example. The equation $x^2 + y^2 = z^3$ has the solutions $(2, 2, 2)$, $(2, 11, 2)$, $(5, 10, 5)$, $(30, 10, 10)$, $(9, 46, 13)$.

Various methods may be used to solve equations

$$x^4 + ax^3 + bx^2 + cx + d = y^2$$

with unknown integers a, b, c, d and y in $\mathbb{Q}$. Writing the square as

$$y = \Big(x^2 + \frac{ax}{2} - \frac{a^2}{8}\Big),$$

the difference of y^2 and the right side of the equation is zero for

$$x = \frac{64d - a^4}{8(a^3 - 8c)}.$$

The square and the difference may be defined in various forms according to conditions on the integers, such as d is a cube. By the same method, there exist values where a third degree polynomial is a cube, $x^3 + bx^2 + cx + d = y^3$ has the solution

$$x = \frac{27d - b^2}{9(3c - b)}, \quad y = x - \frac{a}{3}.$$

A sixth degree polynomial is a cube

$$x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x + a_6 = y^3$$

at a value x, root of the polynomial

$$\Big(a_3 + \frac{17a_1^3}{27} - 2a_1a_2\Big)x^3 + \Big(a_4 - 3a_2^2 + \frac{5a_1^2a_2}{3} - \frac{2a_1^4}{9}\Big)x^2$$
$$+\Big(a_5 - a_1a_2^2 + \frac{2a_1^3a_2}{3} - \frac{a_1^5}{9}\Big)x + a_6 - \Big(a_2 - \frac{a_1^2}{3}\Big)^3$$

and

$$y = x^2 + \frac{a_1x}{3} + a_2 - \frac{a_1^2}{3}.$$

Other elliptic equations $ax^p + by^q = cz^r$ or with linear combinations of powers of x and y have been studied in extensions of $\mathbb{Z}[i]$, with small exponents such as $p = 2$, $2 \leq q \leq 3$ and $3 \leq q \leq 5$.

3.2 Fermat's Last Theorem

Though Fermat's proof of this theorem has never been found, it is plausible from his letters that he knew the arguments of a proof and that he really proved it. Fabry (1814) published the first almost complete proof of Fermat's last theorem, under the conditions x, y and z are not multiple of the exponent n or only one of them is multiple of n and not of n^2. Heere the proof relies on Pythagore's equality and on a property of the binomial coefficients. For non zero integers, Pythagore's equality

$$x^2 + y^2 = z^2, \tag{3.10}$$

is the equation satisfied by the edges x, y and z of a rectangular triangle, for example $3^2 + 4^2 = 5^2$, $6^2 + 8^2 = 10^2$, $13^2 = 12^2 + 5^2$, $9^2 + 12^2 = 15^2$, $8^2 + 15^2 = 17^2$.

In (3.10), x and y are necessarily strictly smaller than z and they must be distinct since the equation $2x^2 = z^2$ has no integer solution. Assuming arbitrarily that $x < y$, the equation has no solution with $x = 1$ and 2 because the difference between the squares of integers y and z larger than x is always larger than x^2 with these values. It follows that $z = 5$ is the smallest non trivial solution of (3.10). Obviously, there is no solution (x, y, z) of Pythagore's equality with three odd numbers x, y and z. The solutions of (3.10) satisfy the binomial formula for the sum and the difference of two square integers

$$x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2. \tag{3.11}$$

Theorem 3.2.1 *Pythagore's equality (3.10) with x, y and $z > 1$ is equivalent to*

$$(4kl)^2 + (km)^2 = (kn)^2 \tag{3.12}$$

with m and n odd and with l in $\mathbb{N}^*$, for every integer k of $\mathbb{N}^*$.

Proof. It is sufficient to prove that Pythagore's equality (3.10) is equivalent to

$$(4\alpha)^2 + y^2 = z^2$$

when x, y and z have no common factor. Since x, y and z cannot be all odd and satisfy (3.10), we assume without loss of generality that $y > 2$ is odd and only one of x and z is even. A solution with $x = 2a + 1$, $y = 2b + 1$ and $z = 2n$ is impossible for

$4(a^2+a+b^2+b)+2 \neq 4n^2$. Therefore x is even, y and z can be choosen odd, x^2 is multiple of 8 and x is a multiple of 4. □

Lemma 3.2.2 *Let n be an odd prime, for all strictly positive integers y and z*

$$\sum_{i=1}^{n-2}\left\{(-1)^i\binom{n-1}{i}-1\right\}y^{i-1}z^{n-2-i} = 0 \pmod{n}.$$

The lemma is proved by induction from the additive expression of the binomial coefficients

$$\binom{j}{i} = \binom{j-1}{i-1} + \binom{j-1}{i} = \binom{j-2}{i-2} + 2\binom{j-2}{i-1} + \binom{j-2}{i},$$

for $i = 0, \ldots, j$. This formula generalizes to express $\binom{j}{i}$ according to $\binom{j-k}{i-k'}$ for $k = 1, \ldots, i-1$ and $k' = 0, \ldots, i-k$. It applies as k is the difference between two prime number. The sum in Lemma 3.2.2 reduces to 3 with $n = 3$, to $5(y^2 - yz + z^2)$ with $n = 5$, and to $7(y^4 - 2y^3z + 3y^2z^2 - 2yz^3 + z^4)$ with $n = 7$.

Before proving Fermat's last theorem for an arbitrary integer n larger than two, we prove it for $n = 3$ and 5.

Theorem 3.2.3 *The equation*

$$x^3 + y^3 = z^3 \tag{3.13}$$

has no solution with mutually prime integers x, y and z distinct from zero.

Proof. Equation (3.13) is equivalent to $(z-y)(z^2+yz+y^2) = x^3$, its possible solutions satisfy one of the following sets of equations

1. let $x = z - y$ and $x^2 = z^2 + yz + y^2$, then $3yz = 0$ and there are only trivial solutions,
2. let $z - y = 1$ and $z^2 + yz + y^2 = x^3 > 1$ then x is odd for $\gcd(x, y, z) = 1$, and the equality $z^2 - 2yz + y^2 = 1$ implies $3yz = x^3 - 1$ and $3(y+z)^2 = 4x^3 - 1$, where $y = z - 1$ hence $3y^2 + 3y + 1 - x^3 = 0$. By a change of variable, the last equation is equivalent to $3z^2 - 3z + 1 - x^3 = 0$, it follows that $z = -y$ which is impossible,

3. let $x = ab$ with $a > 1$, $a = z - y$ and $z^2 + yz + y^2 = a^2b^3$ then a and b are odd and the equality $z^2 - 2yz + y^2 = a^2$ implies $a^2(b^3 - 1) = 3yz$ but it is impossible that a divide y or z and that 3 divides a with $\gcd(x, y, z) = 1$,

4. let $x = ab$ with $a, b > 1$, $a^2 = z - y$ and $z^2 + yz + y^2 = ab^3$ then x is odd and $a(b^3 - a^3) = 3yz$, since $\gcd(a, y) = \gcd(a, z) = 1$ this entails $a = 3$ therefore $yz = b^3 - a^3$ and $b > a$. It follows $z^2 + y^2 = 2b^3 + a^3$ and $(y + z)^2 = 4b^3 - a^3$. By the equality $y = z - a^2$, y is the unique integer solution of the equation $y^2 + a^2y + a^3 - b^3 = 0$ which is equivalent to $z^2 - a^2z + a^3 - b^3 = 0$ so $z = -y$ which is impossible,

5. let $x = ab$, $b > a > 1$, $a^3 = z - y$ and $z^2 + yz + y^2 = b^3$ which is odd. Then $3yz = b^3 - a^6$ and $3(y + z)^2 = 4b^3 - a^6$. By the equality $y = z - a^3$, y is solution of the equation $3y^2 + 3a^3y + a^6 - b^3 = 0$ which is equivalent to $3z^2 - 3a^3z + a^6 - b^3 = 0$ hence $z = -y$, which is impossible.

□

Theorem 3.2.4 *The equation*

$$x^5 + y^5 = z^5 \tag{3.14}$$

has no solution with mutually prime integers x, y and z distinct from zero.

Proof. Equation (3.14) is equivalent to $(z - y)(z^4 + z^3y + z^2y^2 + zy^3 + y^4) = x^5$ and its solutions satisfy one of the following impossible cases

1. let $x = z - y$ and $x^4 = z^4 + z^3y + z^2y^2 + zy^3 + y^4$ then $z^4 + z^3y + z^2y^2 + zy^3 + y^4 - (z - y)^4 = 0$ and $z^2 - zy + y^2 = 0$, which is equivalent to $x^2 + xy + y^2 = 0$,

2. let $z^4 + z^3y + z^2y^2 + zy^3 + y^4 = x^5$ and $z - y = 1$, then

   $$5yz(z^2 - yz + y^2) = x^5 - 1.$$

   By the change of variable $z - y = 1$, $(z^2 - z)(z^2 - z + 1) = (y^2 + y)(y^2 + y + 1)$ and $z = -y$,

3. let $x = ab$ with $a > 1$, $a^k = z - y$ with k between 1 and 5 and $z^4 + z^3y + z^2y^2 + zy^3 + y^4 = a^{5-k}b^5$ then $5yz(z^2 - yz + y^2) = a^{5-k}b^5 - a^{4k}$. By the previous

arguments, this implies $(z^2-a^kz)(z^2-a^kz+a^{2k})=(y^2+a^ky)(y^2+a^ky+a^{2k})$ and $z=-y$. □

Theorem 3.2.5 *Fermat's equation*

$$x^4+y^4=z^4 \tag{3.15}$$

has no solution (x,y,z) *in* $\mathbb{N}^{*\otimes 3}$ *such that* $\gcd(x,y,z)=1$.

Proof. Let $X=x^2$, $Y=y^2$ and $Z=z^2$, Fermat's equation (3.15) is equivalent to Pythagore's equality $X^2+Y^2=Z^2$ with X even, Y and Z odd, all strictly larger than 2, such that $\gcd(X,Y,Z)=1$ in $\mathbb{N}^*$ and satisfying (3.11)

$$x^2=2ab,\quad y^2=a^2-b^2,\quad z^2=a^2+b^2,$$

equivalently

$$z^2=y^2+2b^2,\quad 2ab=y^2+z^2,\quad x^2=2ab$$

but the equation $2ab=y^2+z^2$ is impossible with odd integers y and z by Pythagore's Theorem 3.2.1. □

Theorem 3.2.6 *For every integer* $n>2$*, Fermat's equation*

$$x^n+y^n=z^n \tag{3.16}$$

has no solution (x,y,z) *in* $\mathbb{N}^{*\otimes 3}$ *such that* $\gcd(x,y,z)=1$.

Proof. Let n be an odd prime integer, (3.16) is written as

$$x^n=(z-y)(z^{n-1}+yz^{n-2}+\cdots+y^{n-2}z+y^{n-1})=(z-y)P_{n-1}(y,z),$$

where the value of $P_{n-1}(y,z)$ is odd. Let $s=z-y$ and $t=P_{n-1}(y,z)$ such that $x^n=st$. By Lemma 3.2.2, we have

$$S_n(y,z)=\sum_{i=1}^{n-2}\left\{(-1)^i\binom{n-1}{i}-1\right\}y^iz^{n-1-i}=s^{n-1}-t,$$

and it is denoted $nyzQ_n(y,z)$ where $Q_n(y,z)$ is a symmetric bilinear integer polynomial of degree $n-3$ having a single term $y^{\frac{n-3}{2}}z^{\frac{n-3}{2}}$. Then (x,y,z) satisfies one of the following impossible cases

1. let $x = s$ and $x^{n-1} = t$ then $Q_n(y, z) = 0$ and by the change of variable, $Q_n(y, y+x) = 0$, this is equivalent to

$$y^{\frac{n-1}{2}} R_n(y, y+x) + (y+x)^{\frac{n-1}{2}} R_n(y+x, y) - C_{n2}\{-y(y+x)\}^{\frac{n-3}{2}} = 0$$

where $C_{n2} = \binom{n-1}{\frac{n-1}{2}}$ and $R_n(y, z)$ is a homogeneous polynomial of degree $\frac{n-5}{2}$ such that $R_n(z, z) = z^{\frac{n-3}{2}} C_{n1}$ and $C_{n1} = \sum_{i=1}^{\frac{n-2}{2}} \left\{1 - (-1)^i \binom{n-1}{i}\right\}$. Expanding the expression of $Q_n(y, y+x)$ leads to a polynomial of y with positive coefficients, which is contradictory,

2. let $t = x^n$ and $z - y = 1$, by a change of variable it follows that $(z^2 - z)Q_n(z - 1, z) = (y^2 + y)Q_n(y, y + 1)$ and $z = -y$ by the symmetry of Q_n,

3. let $x = ab$ such that $1 < a < b$, $a^k = z - y$ with k between 1 and n, (3.16) implies $P_{n-1}(y, z) = a^{n-k}b^n$ then $S_n(y, z) = a^{(n-1)k} - a^{n-k}b^n$. By a change of variable, $(z^2 - a^k z)Q_n(z - a^k, z) = (y^2 + a^k y)Q_n(y, y + a^k)$ which entails $z = -y$ by symmetry of Q_n.

For every integer $n = mp$ with an odd prime factor p, Fermat's equation with exponent p does not have solutions and the equation with exponent n is an equation $X^p + Y^p = Z^p$ with $X = x^m$, $Y = y^m$ and $Z = z^m$, so it does not have any solution. Furthermore, by Theorem 3.2.5, Fermat's equation with exponent 4 does not have solutions in $\mathbb{N}^{*3}$, it follows that (3.16) has no solution for every $n = 2^k$, $k \geq 2$. □

Lagrange proved that the equations

$$x^n + y^n + z^n = 0,\ n = 3, 5$$

cannot be solved in $\mathbb{Z}^{*\otimes 3}$. Let $n = 5$, writing $y^5 + z^5 = (y+z)(z^4 - yz^3 + y^2z^2 - y^3z + y^4)$ and by the same arguments as for Theorem 3.2.4, we have to consider the following impossible cases

1. let $x = -(z + y)$ and $x^4 = z^4 - z^3y + z^2y^2 - zy^3 + y^4$, by Lemma 3.2.2 we have $z^2 + zy + y^2 = 0$ and we may assume $y > 0$ and $z < 0$, the equation becomes equivalent to (3.14) and this case cannot be solved with $x = y - |z|$,

2. let $z^4 - z^3y + z^2y^2 - zy^3 + y^4 = x^5$ and $z - y = 1$, then changing the variable by the second equality leads to $z^4 - 2z^3 + 4z^2 - 3z + 1 = y^4 + 2z^3 + 4z^2 + 3z + 1$ therefore $z = -y$,

3. let $x = ab$ with $a > 1$, $a^k = z - y$ with k between 1 and 5 and $z^4 - z^3y + z^2y^2 - zy^3 + y^4 = a^{5-k}b^5$ then $yz(3z^2 - 5yz + 3y^2) = a^{5-k}b^5 - a^{4k}$ which implies $(z^2 - a^kz)(z^2 - a^kz + 3a^{2k}) = (y^2 + a^ky)(y^2 + a^ky + 3a^{2k})$ and $z = -y$.

Equation (3.16) is equivalent to an equation in $\mathbb{Q}$

$$(x_1y_2z_2)^n + (x_2y_1z_2)^n = (x_2y_2z_1)^n$$

where $x = x_2^{-1}x_1$ with relatively primes integers x_1 and x_2, $y = y_2^{-1}y_1$ with relatively primes integers y_1 and y_2 and $z = z_2^{-1}z_1$ with relatively primes integers z_1 and z_2. Denoting $X = x_1y_2z_2$, $Y = x_2y_1z_2$ and $Z = x_2y_2z_1$, we have an equation similar to (3.16) for (X, Y, Z) but X, Y and Z are not pairwise prime. If $z_2 = 1$, then $\gcd(x_1y_2, x_2y_1) = 1$ and there is no solution of Fermat's equation with rational x and y and with z integer.

We have $\gcd(X, Y) = z_2$. As in the proof of Theorem 3.2.6, it is impossible that $n = 2k$ because Y cannot divide X^k and Z^k. For $n = 3$, the property $X^2 \mid 3YZ$ implies $X = 3ay_2z_2$ with a relatively prime to x_2y_1 but $Y^2 \mid 3XZ = 9ax_2y_2^2z_1z_2$ is impossible. For $n > 3$, Y cannot divide n prime or X and there is no solution. The existence of solutions of (3.16) in $\mathbb{Q}^{*3}$ is therefore impossible.

3.3 Catalan's Equation

Lemma 3.3.1 *Let $m > 1$ and $n > 1$, Catalan's equation*

$$x^m - y^n = 1 \tag{3.17}$$

implies $\gcd(m, n) = 1$.

Proof. Let $d = \gcd(m, n)$, there exist integers a and b such that $m = ad$ and $n = bd$ and the equation is equivalent to $(x^a)^d = (y^b)^d + 1$. By Theorem 3.2.1 and Fermat's last Theorem, this equation does not have non trivial solution for $d \geq 2$. □

Proposition 3.3.2 *In a cyclic field F_p, p odd in $\mathbb{P}$, for every integer $n > 1$ (respectively m) there exists an integer m (respectively n) such that the equation*

$$x^m - y^n = 1$$

has $p-2$ non trivial solutions (x,y) in F_p^2 if m and n are odd, there are $p-1$ non trivial solutions if there are even.

Proof. In F_p, let $x=\theta^a$ and let $y=\theta^b$, by the euclidean division $am=\alpha \pmod{p-1}$ and $bn=\beta \pmod{p-1}$, with $0\leq\alpha<p-1$ and $0\leq\beta<p-1$. If $\alpha=0$, $x^m=1 \pmod{p-1}$ and the equation has a trivial solution $y=0$, in the same way if $\beta=0$, $y^n=1 \pmod{p-1}$ and the equation $\theta^\alpha=2$ has a solution in F_p for a single integer $0<\alpha<p-1$.
Let $\alpha\geq 1$ and let $\beta\geq 1$, by Fermat's first Theorem the equation is equivalent to

$$\theta^\alpha=\theta^\beta+1,$$

for every $\alpha=1,\ldots,p-2$ there exists an unique integer β such that the equation has a solution in $\{1,\ldots,p-2\}$. The solution β is unique if α and β are odd. If they are even, the solutions are the same up to their sign. □

By Lemma 3.3.1, m and n cannot have the same parity. Let $m=2a$ and $n-1=2b$, (3.17) is equivalent to

$$X^2-yY^2=1 \tag{3.18}$$

with $X=x^a$ and $Y=y^b$. For $y=2$, $(x,y)=(\pm 3,2)$ are solutions with exponents $(m,n)=(2,3)$, by Table (1.1). Let $m-1=2a$ and $n=2b$, with the same notations (3.17) is equivalent to (3.18) where the roles of x and y are exchanged.

Lemma 3.3.3 *The unique integer solutions of Eq. (3.17) with $(m,n)=(2,3)$ are $(x,y)=(\pm 3,2)$.*

Proof. The equation

$$(x-1)(x+1)=y^3$$

has no solution with y odd in $\mathbb{P}$ so there exist integers y_1 and y_2 such that $y=zy_1y_2$ with $z=2^\alpha$ and $\gcd(y_1,y_2)=1$, and such that one of the sets of equations holds

$$\begin{aligned} x-1 &= zy_1^3, \quad x+1=z^2y_2^3, \\ x-1 &= z^2y_1^3, \quad x+1=zy_2^3. \end{aligned}$$

In the first case, the solutions of the second order equation $z^2y_2^3 - zy_1^3 - 2 = 0$ are not powers of 2 except with $y_1 = y_2 = 1$ and $\alpha = 1$. In the second case, the equation $z^2y_2^3 - zy_1^3 + 2 = 0$ has a discriminant $\Delta = y_1^6 - 8y_2^3$ which must be a square integer c^2 but $y_1^3 + c$ is strictly negative and z cannot a power of 2. □

Theorem 3.3.4 *The unique integer solutions of Eq. (3.17) are* $(x, y) = (\pm 3, 2)$ *with* $(m, n) = (2, 3)$.

Proof. By Lemma 3.3.1 and a change of variable, a necessary condition for the existence of a solution of (3.17) is the existence of a solution of (3.18) where $m = 2$ and n is odd. Using the same argument as for Lemma 3.3.3, the equation

$$(x - 1)(x + 1) = y^n$$

is equivalent to both equations

$$\begin{aligned} x - 1 &= z^k y_1^n, \\ x + 1 &= z^{n-k} y_2^n \end{aligned}$$

where the integers y_1 and y_2 satisfy $y = zy_1y_2$ and $\gcd(y_1, y_2) = 1$, with $z = 2^\alpha$ and k in $\{1, \ldots, n - 1\}$. These equations are equivalent to

$$z^{2k} y_1^n \pm 2z^k + y_3^n = 0$$

with $y_3 = zy_2$ and the latter one has no solution except with $n = 3$, by Lemma 3.3.3. □
Catalan's equation is equivalent to $x^p - y^q = -1$, for arbitrary p and q. It generalizes to equations $x^p - y^q = k$, for integers k. With $p = 3$ and $q = 2$, the solutions of $x^p - y^2 = 2$ reduce to $(x, y) = (3, \pm 5)$ by Proposition 3.1.8.

Proposition 3.3.5 *The unique integer solutions of the equation*

$$x^p - y^2 = -2$$

with $p \geq 2$ *is* $(x, y) = (-1, \pm 1)$ *with* p *odd.*

Proof. The solutions of this equation are necessarily odd. With p odd, let $y = 2b + 1$ with $b \geq 1$, the equality $x^p + 1 = 4b(b + 1)$ implies $8 \mid x^p + 1$. Let $x = 2^\alpha a + 1$ with

$a \geq 1$ odd and $\alpha \geq 1$

$$\begin{aligned} x^p + 1 &= (x+1)(x^{p-1} + \cdots + 1) \\ &= 2(2^{\alpha-1}a + 1)(x^{p-1} + \cdots + x + 1) \end{aligned}$$

but $(2^{\alpha-1}a + 1)(x^{p-1} + \cdots + 1)$ is odd so there is no solution. Let p be even, denoting $p = 2^c r$ with r odd, the equation $(x^{2^c})^r - y^2 = -2$ has no solution according to the previous case. □

The proof of Proposition 3.3.5 applies to the equation

$$x^p - y^2 = \pm k,\ p \geq 2,$$

now $x^p \mp k - 1$ is multiple of 8 if y is odd. With $k = n^2$, the equation $x^p - y^2 = -n^2$ implies $x^p = (y-n)(y+n)$ and $x \mid 2n$, it follows that for $n \geq 2$ in $\mathbb{P}$, the equations $x^p - y^2 = -n^2$ have no solutions in $\mathbb{Z}^{*2}$ for $p \geq 2$. If $n = 1 \pmod 4$, it is the sum of two squares $n = a^2 + b^2$, by Theorem 2.4.3, and

$$x^p + a^2 = x.\left(x^{\frac{p-1}{2}}\right)^2 + a^2 = y^2 - b^2,$$

the existence of solutions depends on the coherence of this equality.

The equation $x^p - y^2 = -4$ implies $y - 2$ and $y + 2$ are multiple of x hence $x \mid 4$ but there is no solution. Proposition 3.1.9 yields solutions of $x^p - y^2 = 4$.

By Proposition 3.1.11, the equation $x^3 - y^3 = 2^m z$ has infinitely many integer solutions. Catalan's conjecture of the existence of a unique solution up the the sign does not generalize.

3.4 Generalizations of Fermat's Last Theorem

Fermat's equation generalizes to integers x, y and z with different exponents and to linear equations of x^n, y^n and z^n. Let

$$x^n + y^n = pz^n \tag{3.19}$$

where x, y and z are pairwise primes.

With $n = 2$, the equation $x^2 + y^2 = pz^2$ with pairwise primes x, y and z has the solution

$$(x, y, z, p) = (7, 9, 8, 2).$$

It has infinitely many solutions such that x, y and z are not mutually primes.

Theorem 3.4.1 *Let $p > 1$ be integer, the equation*

$$x^3 + y^3 = pz^3 \tag{3.20}$$

with pairwise primes x, y and z strictly larger than 1 in $\mathbb{N}^{*\otimes 3}$ has infinitely many solutions with $p = 1 \pmod 4$ and $p = 3 \pmod 4$ with $p > 3$. It has no solution with pairwise prime integers and with p even.

Proof. The existence of p prime such that

$$pz^3 = (x + y)(x^2 - xy + y^2)$$

implies $p \mid (x^2 - xy + y^2)$ or $(x + y)$. In the first case, $(x + y) \mid z^3$ and there exists an integer $k \geq 1$ such that

$$\begin{aligned} z^3 &= k(x + y), \\ x^3 + y^3 &= pk(x + y) \end{aligned}$$

and $x^2 - xy + y^2 = pk$.

With k and then z even, (3.20) is impossible with x and y odd. With k odd, either z is even if x and y have the same parity, or z is odd if x, respectively y, is even and y, respectively x, is odd. The first case implies $8 \mid x^3 + y^3$ and this is impossible with x and y odd. In the second case, p must be odd and writing (3.20) with $x = 2a$, $y = 2b + 1$ and $z = 2c + 1$, it is equivalent to

$$\begin{aligned} 8(a^3 + b^3) + 12b^2 + 6b &= 8pc^3 + 12pc^2 + 6pc + p - 1 \\ &= 2kp(a + b) + kp - 1, \\ 0 &= 3(pc - b) + \frac{p - 1}{2} \pmod 2, \\ 0 &= 1 - b + \frac{p - 1}{2} \pmod 2, \end{aligned}$$

then $p = 1 \pmod 4$ and

$$x^3 + y^3 = z^3 \pmod 4$$

or $p = 3 \pmod 4$ and

$$x^3 + y^3 = z^3 \pmod 2.$$

There exist solutions in both cases, for example $(2, 7, 3)$ with $p = 13$ and $(4, 5, 3)$ with $p = 7$.

In the second case, let $y + x = mp$ with p prime and an integer $m \geq 1$. With $p = 2$, (3.20) is impossible unless x, y and z are odd then $4 \mid (x + y - 2)$ and $x^3 + y^3$ differs from $2z^3$.

Let $p > 3$ in $\mathbb{P}$, x and y both even or odd implies $2 \mid pz^n$ which is contrary to the assumptions so let $x = 2a$ with $y = 2b + 1$ and $z = 2c + 1$. The equality $x^3 + y^3 = pz^3$ implies

$$\begin{aligned} 4(a^3 + b^3 - pc^3) &= \frac{p-1}{2} + 6(pc^2 - b^2) + 3(pc - b), \\ 0 &= \frac{p-1}{2} + 3(pc - b) \pmod 2. \end{aligned} \tag{3.21}$$

If $p = 3 \pmod 4$, there exist a solution for $p = 7$. Assuming that $p = 1 \pmod 4$, b and c have the same parity, $2 \mid (b^3 - pc^3)$, $4 \mid (pc^2 - b^2)$, $2 \mid (pc - b)$ and

$$\frac{p-1}{4} + \frac{3(pc - b)}{2} = \frac{p-1}{4} + \frac{c-b}{2} = 0 \pmod 2.$$

If $p = 1 \pmod 8$, $c = b \pmod 4$, there exist infinitely many solutions with $x = 2y$ and $z = y$ which are not mutually primes, $(1, 6, 4)$ is solution with $p = 17$. If $p = 5 \pmod 8$

$$\frac{p-1}{4} = 1 \pmod 2$$

and $c = b + 2 \pmod 4$ then (3.21) implies $b = 0 \pmod 4$, b and c must be even but (3.21) is then impossible for $a^3 = 33b + 38 \pmod 8$ is divided by 2 but not by 8.

If p is not prime, let $p = p_1 m_1$ where p_1 is prime with an exponent $\alpha_1 \neq 0 \pmod 3$ in the factorisation of p for the prime divisors of p with a cubic exponent cannot be distinguished from those of z. By the same arguments as for p prime, p_1 does not divide $x^2 - xy + y^2$ therefore it should divide $x + y$. With $p_1 = 2$, (3.20) with x or y even would imply the three variables are even so x and y must be odd. Let $x + y = 2a$

$$8a^3 = x^3 + y^3 + 6axy = 2m_1 z3 + 6axy$$

implies a and m_1 even, $a = 2b$ and $m_1 = 2m_2$ but $2^6b^3 = 4m_2z3 + 12bxy$ implies b and m_2 even and, by induction α_1 should be infinite.
With $p_1 = 3$, (3.20) with x even, y and z odd implies that m_1 and therefore p are odd, but 3 does not divide $x + y$ as proved above (cf. Proposition 3.1.7). With $p_1 > 3$, $p > 3$ and the proof with p prime applies. □

Example. The following triples are solutions of (3.20), there is no solution with $p = 3, 5$ and there exist other solutions for larger values of p

1. $(x, y, z) = (4, 5, 3)$ with $p = 7$,
2. $(x, y, z) = (2, 7, 3)$ with $p = 13$,
3. $(x, y, z) = (3, 5, 2)$ and $(x, y, z) = (1, 6, 4)$ with $p = 17$,
4. $(x, y, z) = (2, 3, 1)$ with $p = 33$,
5. $(x, y, z) = (1, 7, 4)$ with $p = 41$.

Removing the condition $\gcd(x, y, z) = 1$, other solutions of (3.20) are all multiples of the previous ones. With $p = 2$, (3.20) is satisfied by $x = y = z$ in $\mathbb{N}^*$. Legendre (1830) proved that the next equations have no integer solutions

1. $x^3 - y^3 = z^3$, equivalent to $x^3 = y^3 + z^3$ has no solution by Fermat's last theorem,
2. $x^4 + 2y^4 = z^4$,
3. $x^4 + 8y^4 = z^2$,
4. $x^4 - y^4 = z^4$, equivalent to $x^4 = y^4 + z^4$, has no solution by Fermat's last theorem.

Theorem 3.4.2 (Dirichlet) *For all integers $n \neq 0, 2$ and A not divisible by 2, 5 and all integers $10k \pm 1$, the equation*

$$x^5 \pm y^5 = 5^n Az^5$$

has no pairwise prime solutions (x, y, z).

Proof. Let $f_{xy} = x^4 - x^3y + x^2y^2 - xy^3 + y^4$, $x^5 + y^5 = (x+y)f_{xy}$ and the common prime factors of $x + y$ and f_{xy} are prime factors of $(x + y)^5 - f_{xy}$ they are therefore 5 or 3 by Lemma 3.2.2, otherwise they are mutually prime. We assume without loss of generality that $x = 2a$ and $y = 2b + 1$ and the prime factors of $x + y$ and f_{xy} are odd. With the common prime factor 5, we get $n = 2$ and with 3, $x^5 + y^5$ cannot be multiple of 3^{4c}, $c > 0$, the constant $A = 1 \pmod{10}$ being not allowed. Let $x + y = 3k$, then $x^5 + y^5 = 243k^5 \pmod 5$ and $n = 0$. Let $x + y = 5k$, then $x^5 + y^5$ is multiple of 5^2k with $k \neq 0 \pmod 5$ since $\gcd(x, y) = 1$, and there is no solution.

Assuming that $x + y = 7k$

$$x^5 + y^5 = 2k^5 + k^4y + 3k^3y^2 + k^2y^3 + 2ky^4 \pmod 5$$

with $y = -k$, this polynomial equals $5k^5$ and k multiple of 5 implies $n = 7$ but $\gcd(x, y) > 1$ so there is no solution. □

The proof is the similar for the equation $x^5 - y^5 = 5^n Az^5$, replacing f_{xy} with $g_{xy} = x^4+x^3y+x^2y^2+xy^3+y^4$. The equation $x^5+y^5 = 5^n Az^5$ has many solutions with $z = 1$ and $x + y$ multiple of 5 such as $2^5 + 3^5 = 5^2.11$, $7^5 + 8^5 = 5^2.1983$, $22^5 + 3^5 = 5^3A_1$ and $6^5 + 19^5 = 5^3A_2$ with $A_j = 1 \pmod{10}$. If $x + y$ is multiple of 3, n is generally zero.

Theorem 3.4.3 *The equation*

$$x^5 \pm y^5 = pz^5 \tag{3.22}$$

with pairwise primes x, y and z in $\mathbb{N}^*$ *has no solution with* $p = 2$, $p = 5 \pmod 8$, $p = 3 \pmod 4$ *or with z even.*

Proof. The equality

$$x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4)$$

implies $p \mid (x^4 - x^3y + x^2y^2 - xy^3 + y^4)$ or $p \mid x + y$. In the first case, there exists an odd integer $k \geq 1$ such that

$$x^4 - x^3y + x^2y^2 - xy^3 + y^4 = pk \tag{3.23}$$

therefore $z^5 = k(x+y)$ and $x^4+y^4 = pk + xy(x^2+y^2-xy)$. In the second case, there exists an integer $k \geq 1$ such that $x+y = pk$.

If x and y had the same parity they are odd, z must be even. Because p does not divide the left side of (3.23), it should divide $x+y = pk$ which divides z^5 and

$$\begin{aligned} pz^5 &= (x^5+y^5) = (x+y)^5 - 5xy(x^3+y^3) - 10x^2y^2(x+y) \\ &= (pk)^5 - 5xy(x^3+y^3) - 20kx^2y^2 \\ &= (pk)^5 - 5xy(x+y)\{(x+y)^2 - 3xy\} - 20kx^2y^2, \\ z^5 &= \frac{x+y}{2}(xy)^2 \pmod 2 \end{aligned}$$

the equation does not have solutions with z even, nor with z odd since $x+y = pk$ does not divide z^5. The argument is similar for $x^5 - y^5 = pz^5$, x and y having the same parity. Let x be even and let y and z be odd. Denoting $x = 2a$, $y = 2b+1$ and $z = 2c+1$, the equation is equivalent to

$$2^5(a^5+b^5-pc^5) + 5.2^4(b^4-pc^4+b^3-pc^3) + 5.2^3(b^2-pc^2) + 5.2(b-pc) = p-1.$$

With $p = 1 \pmod 4$, the equation implies $y^5 - z^5 = 0 \pmod 4$ hence b and c have the same parity but the equation has no solution such that $8k \nmid (p-1)$. With $p = 3 \pmod 4$, it implies $y^5 + z^5 = 0 \pmod 4$, b and c have again the same parity so the left side of the equation is divisible by 4 but $4 \nmid (p-1)$. □

We now consider the question of finding exponents solutions of (4.11) for triples of integers (x, y, z).

Proposition 3.4.4 *The equation*

$$3^n + 4^r = 5^s \tag{3.24}$$

has no solution with integers n, r, s strictly larger than 2.

Proof. With $n = 2k+1$, the equation is written as $3.9^k + 4^r = 5^s$, it has no solution fr $-1 \neq 1 \pmod 4$.

With $n = 2k$, the equation $9^k + 4^r = 5^s$ implies $(-1)^k + (-1)^r = 0 \pmod 5$ hence k and r do not have the same parity. With $n = 4m$ the equation $81^m + 4^r = 5^s$ or $0 = 1 \pmod 4$ has no solution. With $n = 4m+2$ and $r = 2h$, $9.81^m + 16^h = 5^s$ implies $(-2)^h = (-4)^r \pmod 9$ and this is still impossible. □

Proposition 3.4.5 *The equation*

$$5^n + 12^r = 13^s \tag{3.25}$$

has no solution with integers n, r, s strictly larger than 2 in $\mathbb{N}^*$.

Proof. Let $n = 2k + 1$ with $k \geq 1$, (3.25) implies $5.25^k = 5 = 1 \pmod{12}$, so n must be even. Let $n = 2k > 2$, assuming $r = 2l + 1$ and $s = 2h + 1$ with l and $h \geq 1$, $25^k + 12.144^l = 13^s$ implies $2.(-1)^l = 3.(-1)^h \pmod 5$ then l and h cannot have the same parity. Let $r = 4l_2 + 1$ and $s = 2h + 1$ with odd integers l_2 and $h \geq 1$ then $25^k + 12.20736^{l_2} = 13.169^h$ implies $(-1)^{l_2} - 1 = 0 \pmod{13}$, therefore l_2 should be even and $25^k + 12^{8l_3+1} = 13^s$ is equivalent to $2 = 3.(-1)^h \pmod 5$, h should be even which is contradictory to the assumption.
Consider now $r = 2l + 1$ and $s = 4h_2 + 1$ with l odd, the equation is written as $25^k + 12.144^l = 13^{4h_2+1}$, it implies $(-1)^k - 1 = 0 \pmod{13}$, therefore k is even, then let $n = 4k_2+1$, $r = 2l+1$ and $s = 4h_2+1$ $5.625^{k_2}+12.144^l = 13^{4h_2+1}$ implies $5+12 = 0 \pmod{13}$ which is not true.
With r even and s odd the equation would become $25^k + 144^l = 13.169^h$ and this is impossible modulo 5, with r odd and s even the equation is still false. □

Proposition 3.4.6 *The equation*

$$8^n + 15^r = 17^s \tag{3.26}$$

has no solution with integers n, r, s strictly larger than 2 in $\mathbb{N}^*$.

Proof. Let $n = 2k+1$, with $k \geq 1$, the equation $8.64^k+15^r = 17^s$ implies $(-1)^r = 1 \pmod 4$ so r should be even, then let $r = 2l$, $l \geq 1$, the equation becomes $8.64^k + 225^l = 17^s$ hence $8.(-4)^k + 4^l = 0 \pmod{17}$ and this is impossible.
Let $n = 2k$, $k \geq 1$, the equation $64^k + 15^r = 17^s$ modulo 4 still requires r even, let $r = 2l$, $l \geq 1$, the equation becomes $64^k + 225^l = 17^s$ entails $(-1)^k = 2 = 2^s \pmod 5$ which wis impossible. □

Proposition 3.4.7 *The equations*

$$x^2 + y^3 = z^2, \tag{3.27}$$

$$x^2 + y^3 = z^3 \tag{3.28}$$

have solutions in $\mathbb{N}^*$.

The solution of (3.27) is not unique and the parity of the integers may be arbitrary

$$(x, y, z) = (1, 2, 3), (3, 3, 6), (6, 4, 10).$$

Equation (3.28) has the solution $(x, y, z) = (13, 7, 8)$. In F_3 and if $\gcd(x, 3) = 1$, the equation is equivalent to $y + 1 = z$ and therefore to $(x - 1)(x + 1) = 3y(y + 1)$ hence 3 divides $x - 1$ or $x + 1$.

Proposition 3.4.8 *The equation*

$$x^2 + y^3 = a^2 + b^3 \tag{3.29}$$

has solutions in $\mathbb{N}^*$.

There exist many solutions of (3.29), for example

$$\begin{aligned}(x, y, a, b) \quad = \quad & (1, 4, 8, 1), (2, 5, 11, 2), (3, 2, 4, 1), (5, 4, 9, 2), (9, 3, 10, 2), \\ & (9, 4, 12, 1), (9, 6, 17, 2), (10, 6, 17, 3), (11, 17, 20, 4), \text{ etc.}\end{aligned}$$

The problem posed by Fermat was to find three distinct pairs of integers satisfying the same equality, it is not solved.

3.5 Exercises

Exercise 3.1. Find all rectangular triangles in $\mathbb{N}^*$ such that their area is a square.
Exercise 3.2. [Euler] Solve the equation $x^3 + y^3 + z^3 = t^3$ in $\mathbb{N}^{*4}$.
Exercise 3.3. Solve the equation $x^5 + y^5 + z^5 = t^5$ in $\mathbb{N}^{*4}$.
Exercise 3.4. Prove that the equation $x^3 + y^3 = 5z^3$ has no solution in $\mathbb{N}^{*3}$.
Exercise 3.5. Prove that the equation $x^3 + y^3 = 2^k z^3$ has no solution in $\mathbb{N}^{*3}$.
Exercise 3.6. [Legendre] Prove that the equations $x^4 + 2y^4 = z^4$ and $x^4 + 8y^4 = z^2$ have no solutions in $\mathbb{N}^{*3}$.
Exercise 3.7. Find the solutions of the equation $x^2 + y^2 = z^4$.
Exercise 3.8. Prove that the equations $x^{2k} - y^{2k} = z^{2n}$ do not have non trivial integer solutions.