Chapter 1

Introduction

Abstract

We introduce elementary results on the prime numbers and the first criteria to determine them, the representations of integers as sums of squares and the conjectures about representations with higher powers of integers. The factorization of integer polynomials and quadratic bilinear forms are presented, they are related to the units of the quadratic fields.

A group $(G, *)$ is provided with an asssociative law $*$ with a unit element e, $e * x = x * e = x$ for every x in G, and each element x in G has an unique symmetric x' in G, $x' * x = x * x' = e$. An Abelian group is a commutative group. Then $(x * y)' = x' * y'$ for all x and y of G and the quotients $x * y' = y' * x$ and $x' * y = y * x'$ belong to G. A subgroup F is stable for the law and the inverse of every element of F belongs to F.

A homomorphism h between groups $(G, *_G)$ and $(G', *_{G'})$ is a mapping from G to G' that preserves the laws of the groups,

$$h(x *_G y) = h(x) *_{G'} h(y),$$

hence the unit element of G' is $e_{G'} = h(e_G)$ and the inverse in G' is $h'(x)$, x in G. An isomorphism is a bijective homomorphism and an endomorphisms h maps G into G. The kernel of a homomorphism is

$$\ker h = \{x \in G : h(x) = e_{G'}\},$$

it reduces to $\{e_G\}$ if h is injective.

Let H be a subgroup of G, the quotient group of G and H is

$$G/H = \{\bar{x} = x *_G H = H *_G x, x \in G\}.$$

With an homomorphisme $h : G \mapsto G'$, $h(G)$ is isomorph to $G/\ker h$.

A ring $(A, +, .)$ provided with additive and multiplicative laws is a commutative group for the addition such that the multiplication is associative and distributive with respect to the addition, $(a+b).c = a.c+b.c$. If $(A, .)$ is commutative, A is a commutative ring. The kernel of f defined on A is sub-rings of A and the image $f(A)$ of A by f is a sub-rings of A'.

An ideal I is a sub-group of a ring $(A, +, .)$ such that the relation $x - y$ belongs to I is compatible with the addition and the multiplication of A, for all x in I and a in A, $a + x$ and ax belong to I. Equivalently, there exists a homomorphism $h : A \mapsto B$ such that $\ker h = I$. An ideal aA generated by a single element a of A is a principal ideal. A principal ring $(A, +, .)$ is a ring with a unit element for the multiplication and such that every ideal of A is principal.

A field is a ring with a unit element for the multiplication and such that every non zero element has an inverse. A commutative and unitary ring A is a field if and only if its ideals reduce to $\{0\}$ and A.

A homomorphism h between commutative rings $(A,+,.)$ and $(A',+,.)$ preserves the additive law

$$f(x+y)=f(x)+f(y)$$

this equality implies

$$f\Big(\frac{kx}{n})\Big)=\frac{k}{n}f(x)$$

and $f(n)=nf(1)$. If $(A,+,.)$ is a field, every element of A' has a symmetric

$$1=f(x).f(x'),\quad f(x.x')=f(1).$$

If f preserves the multiplicative law

$$f(x.y)=f(x).f(y)$$

and this implies $f(1)=1$.

1.1 Factorization of the Integers

For every p of $\mathbb{Z}\setminus\{0,1\}$, the set $p\mathbb{Z}=\{kp,k\in\mathbb{Z}\}$ is an ideal of $\mathbb{Z}$ generated by the integers divided by p. It is a proper ideal if p is prime. The quotient space $F_p=\mathbb{Z}/p\mathbb{Z}=\{0,1,\ldots,p-1\}$ is the finite ring of the elements of $\mathbb{Z}$ modulo p and $p\mathbb{Z}$ is the kernel of $f(k)=kp$ on $\mathbb{Z}$. If p is prime, F_p is a field.

Let $\mathbb{P}$ be the set of the prime numbers of $\mathbb{N}$, they can be divided only by the unit number 1 and themselves. A prime number p satisfies Euclid's property

$$p\mid ab\quad\text{implies}\quad p\mid a\quad\text{or}\quad p\mid b. \tag{1.1}$$

where the notation $n\mid p$ means n divides p in $\mathbb{N}$.

Every integer n has a unique factorization according to prime integers $p_1,\ldots,p_{I_n}$

$$n=\prod_{i=1}^{I_n}p_i^{\alpha_i} \tag{1.2}$$

where $\alpha_i \geq 1$ is the highest exponent of p_i such that $p_i^{\alpha_i} | n$. The unicity of this factorization is a consequence of Euclid's property. Fermat proposed methods for the factorization of large numbers. If an odd integer n is not prime, there exists a divisor of n, $p \geq q + 1$ where $q = \left[\sqrt{n}\right]$.

Large tables of the prime numbers and their cardinal have been calculated very early. Erastothene sieves to find them consists in removing all multiples of an integer, starting from 2 (300 A.D.). It is known from Pythagore that the cardinal of $\mathbb{P}$ is infinite. Several approximations and expressions of the cardinal $\pi(n)$ of the prime numbers lower than a value n have been formulated since the 18th century by Euler, Legendre, Riemann and Dirichlet.

Integers a and b are relatively primes if their greatest common divisor $\gcd(a, b)$ is 1. Euclid's division provides an algorithm to determine the greatest common divisor of two numbers a and b. Let $q_0, q_1, \ldots, q_n$ and $r_1, \ldots, r_{n+1}$ be integer sequences such that $0 < r_{k+1} < r_k$ and

$$\begin{aligned} a &= q_0 b + r_1, \\ b &= q_1 r_1 + r_2, \\ r_k &= q_{k+1} r_{k+1} + r_{k+2},\ k = 1, \ldots, n-1, \\ r_{n+1} &= 0, \end{aligned}$$

then $\gcd(a, b) = r_n$.

Integers a and b are relatively primes if and only if there exists x and y in $\mathbb{Z}$ such that

$$ax + by = 1. \tag{1.3}$$

Theorem 1.1.1 (Euler) *For all intergers a and b, there exist x and y in $\mathbb{Z}$ such that $ax + by = \gcd(a, b)$.*

Proof. Let $d = \gcd(a, b)$, the highest interger that divides a and b, $a = \alpha d$ and $b = \beta d$ with $\gcd(\alpha, \beta) = 1$. Then d divides every linear combination a and b, $ax + by = d(\alpha x + \beta y)$. The smallest positive linear combination of a and b is equal to d. □

Theorem 1.1.2 (Dirichlet) *Let a and b be relatively primes then the sequence $(a + nb)_{n \in \mathbb{N}}$ contains infinitely many primes to a.*

In this sequence all numbers in the form $a + kb$ are relatively prime to a if a and k are relatively primes. There are infinitely many primes in a linear form $4n + 1$, $4n + 3$, $6n + 1$, $6n + 5$ or $8n + 5$ they are special cases of Dirichlet's theorem.

Patterns of the distribution of $\mathbb{P}$ in $\mathbb{N}$ and functions generating prime numbers has been search. Sun and Sun (1992) studied the divisors of Fibonacci's numbers

$$F_n = F_{n-1} + F_{n-2}$$

with $F_0 = 0$ and $F_1 = 1$, and Lucas's numbers $L_n = L_{n-1} + L_{n-2}$, with $L_0 = 2$ and $L_1 = 1$.

Mersenne's numbers are defined with p prime as

$$M_p = 2^p - 1.$$

Let $p_1 < p_2$ in $\mathbb{P}$ such that $p_2 = rp_1 + q$ with $0 < q < p_1$

$$M_{p_2} = 2^q(M_{p_1} + 1)^r - 1 = 2^q - 1 \pmod{M_{p_1}}$$

which implies M_{p_1} and M_{p_2} are mutually prime and all Mersenne's numbers are mutually prime but many of them are not primes. If q is a prime factor of M_p, $2^p = 1 \pmod{q}$ and $2^{q-1} = 1 \pmod{q}$ by Fermat first theorem (Theorem 2.1.1), therefore $p \mid q - 1$.

Fermat's numbers are defined as

$$F_n = 2^{2^n} + 1,\ n \geq 0.$$

For all n and $k = 0, \ldots, n - 1$, they satisfy

$$F_n = (F_{n-1} - 1)^2 + 1 = (F_{n-k} - 1)^{2^k} + 1,$$

they are all mutually primes with

$$F_n = 2 \pmod{F_{n-k}}.$$

The first ones are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ and they are primes. Lucas (1878) proved that

$$F_5 = 2^{32} + 1 = 641 \times 6700417$$

and $114689 \mid F_{12}$. If q is a prime factor of F_n, $2^{2^n} = -1 \pmod q$ and $2^{2^{n+1}} = 1 \pmod q$. Let k be the smallest integer such that $2^k = 1 \pmod q$, then $k \leq q - 1$ by Fermat first theorem and $k \leq 2^{n+1}$ for $q \mid F_n$. It follows that

$$q \mid (2^{2^{n+1}} - 2^k) = 2^k(2^{2^{n+1}-k} - 1)$$

hence $2^{2^{n+1}-k} = 1 \pmod q$ and $k < 2^n$, similarly $q \mid 2^k(2^{q-1-k} - 1)$ implies $2k + 1 \leq q$. Let $2^n = ak + b$ with $0 \leq b < k$, then $2^{2^n} = (2^k)^a.2^b = 2^b \pmod q$ and $q \mid 2^b + 1$. Fermat's numbers are mutually primes, b is not a power of 2, and $b > 0$ since q is odd.

Many prime numbers have a linear form and the graph of every linear function covers infinitely many prime numbers however they do not generate prime numbers, for example there are 161 primes lower than 1000, among them there are 25 numbers such that $p_1 = 18n + 5$ and 28 numbers such that $p_2 = 18n + 11$

$$\begin{aligned} P_1 &= \{23, 41, 59, 113, 131, 149, 167, 239, 257, 293, 311, 347, 383, 419, 491, \\ &\quad 509, 563, 599, 617, 653, 743, 761, 797, 887, 941\}, \\ P_2 &= \{29, 47, 83, 101, 137, 173, 191, 227, 263, 281, 317, 353, 389, 443, 461, \\ &\quad 479, 569, 587, 641, 659, 677, 821, 839, 857, 911, 929, 947, 983\}. \end{aligned}$$

Fermat and Legendre determined the most important criteria to determine whether a large number belongs to $\mathbb{P}$ and large tables of prime numbers have been published. If n has two possible divisors p_1 and p_2, the search of the smallest of p_1 and p_2 may be performed up to the largest integer smaller or equal to $\sqrt{n}$, the other factor being then larger than this value.

The rules for an integer to be divided by a prime are simple for 2, 3 or 5. To write an integer modulo p, let

$$n = \sum_{i=0}^{k} x_i.\ 10^k,$$

then $n = x_0 \pmod 2$ and $2 \mid n$ if and only if $2 \mid x_0$. For the division by 3, $n = \sum_{i=0}^{k} x_i \pmod 3$ and $3 \mid n$ if and only if $3 \mid \sum_{i=0}^{k} x_i$. In the same way, $n = x_0 + 2\sum_{i=1}^{k} x_i \pmod 4$, $n = x_0 \pmod 5$

$$\begin{aligned}
n &= \sum_{i=0}^{k}\{x_{6i} - x_{6i+3} + 3(x_{6i+1} - x_{6i+4}) + 2(x_{6i+2} - x_{6i+5})\}, \pmod 7,\\
n &= x_0 + \sum_{i=1}^{k}(-1)^i x_i \pmod{11},\\
n &= \sum_{i=0}^{k}\{3(x_{6i+4} - x_{6i+1}) + 4(x_{6i+5} - x_{6i+2}) + x_{6i} - x_{6i+3}\}, \pmod{13},\\
n &= \sum_{i=0}^{k}(x_{5i} + 6x_{5i+1} - 2x_{5i+2} - 3x_{5i+3} + 4x_{5i+4}) \pmod{17}.
\end{aligned}$$

This rules applies to all integers. Other rules may be faster for the search of prime divisors.

Let n be two digit odd number

$$7 \mid n \text{ if and only if } 100 - n = 2 \pmod 7$$

if n is a three digit odd number

$$7 \mid n \text{ if and only if } 1000 - n = 6 \pmod 7.$$

The following equivalences are satisfied modulo 7, $10^{i+1} \equiv -10^{i-1} \equiv 10^{i-3}$, for a large odd number n with k digits $7 \mid n$ if and only if $7 \mid 10^{k+1} - n$.
Applying the same principle to the following primes and since $13 \mid 1001$, for a three digit odd number

$$13 \mid n \text{ if and only if } 13|(1001 - n).$$

For a large number n, $k \times 1001 - n$ is multiple of 13 where k is an integer such that $(k-1) \times 1001 \leq n < k \times 1001$ and so on.

Other rules of factorization are well known.

1. Every integer n divides exactly one of n consecutive integers $k, k+1, \ldots, k+n$, with k arbitrary.

2. An integer in the form $n^4 + 4m^4$ is not prime since

$$\begin{aligned} n^4 + 4m^4 &= (n^2 + 2m^2)^2 - 4n^2m^2 \\ &= (n^2 + 2nm + 2m^2)(n^2 - 2nm + 2m^2). \end{aligned}$$

3. The radical of an integer is the product of the prime numbers that divide it. Let a and b in $\mathbb{P}$ and let $c = a + b$, the radical of their product is

$$Rad(abc) = abRad(c) > \max(a, b, c).$$

If a and b are not prime, the inequality $Rad(abc) > \max(a, b, c)$ is not necessarily satisfied.

Proposition 1.1.3 *Let n be a product of prime numbers, the number $\phi(n)$ of integers prime to n and smaller than n is the product of the numbers of integers prime to its prime factors.*

Euler's function $\phi(n)$ is the cardinal of the numbers smaller than n and relatively prime to n, it is also the number of generators of the cyclic group F_n. From the factorization (1.2) of n, it is defined as

$$\phi(n) = n \prod_{i=1}^{I_n} \Big(1 - \frac{1}{p_i}\Big) = \prod_{i=1}^{I_n} p_i^{\alpha_i - 1}(p_i - 1) \tag{1.4}$$

and the number of the divisors of n

$$\tau(n) = \prod_{i=1}^{I_n} (\alpha_i + 1),$$

they are $1, p_i, \ldots, p_i^{\alpha_i}$, $i = 1, \ldots, I_n$. An integer n is a square if and only if $\tau(n)$ is odd.

Let k such that $\phi(n + k) = 2\phi(n)$. If n is even and $2^\alpha | n$, the equation is equivalent to $2^{\alpha+1} | n + k$ and $k = n$, in that case $\phi(2n) = 2\phi(n)$. If $2 | \phi(n + k)$ with n odd and $3 | n + k$ but not n, $k = 2n$ and $\phi(3n) = 2\phi(n)$.

Replacing 2 with an arbitrary prime p such that $p | n + k$ and n, the equation entails $n + k = np$ and $k = (n - 1)p$, $\phi(np) = p\phi(n)$. Otherwise $p | \phi(n + k)$ but not $\phi(n)$, then $k = np$ and $\phi(n(p + 1)) = p\phi(n)$.

Proposition 1.1.4 (Euler) *Every integer n is written as*

$$n = \sum_{k=1}^{\tau(n)} \phi(k), \quad \sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \left[\frac{n}{k}\right].$$

Proof. Let $A_k = \{a \in \{1, \ldots, n-1\} : \gcd(n, a) = d_k^{-1} n\}$ for every divisor d_k of n, they are disjoint sets which cover $\{1, \ldots, n\}$ and their cardinals are $\#A_k = p_k - 1$ if d_k is prime, $\#A_k = p_k^{\alpha_k - 1}(p_k - 1)$ if $d_k = p_k^{\alpha_k}$ with $1 \leq \alpha_k \leq m_k$. For a product $p_i^{\alpha_i} p_j^{\alpha_j}$, the cardinal is $\#A_{ij} = p_i^{\alpha_i - 1}(p_i - 1) p_j^{\alpha_j - 1}(p_j - 1)$.

The second assertion is deduced from the equality

$$\#\{k \leq n : p | k\} = \left[\frac{n}{p}\right]$$

for every n and p in $\mathbb{N}^*$. □

The sum of the divisors of an integer $n \geq 1$ factorized as (1.2) is $1 + p_i + p_i^2 + \ldots, + p_i^{\alpha_i}$ for $i = 1, \ldots, I_n$ and the function $\sigma(n)$ is their product

$$\begin{aligned} \sigma(n) &= \prod_{i=1}^{I_n} \{1 + p_i + p_i^2 + \ldots, + p_i^{\alpha_i}\} \\ &= \prod_{i=1}^{I_n} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}. \end{aligned}$$

Conjectures about the representation of numbers as sum of functions of primes are not completely proved.

Goldbach's conjecture. Every even $n \geq 6$ is sum of two odd primes and every odd $n \geq 9$ is sum of three primes.

Levy's conjecture. For every odd $n \geq 5$, there exist p, q in $\mathbb{P}$ such that $n = p + 2q$.

Waring-Goldbach conjecture. For $k \geq 2$ and for every sufficiently large n, there exist $n_1, \ldots, n_{s(k)}$ in $\mathbb{N}$ such that

$$n = n_1^k + \cdots + n_{s(k)}^k$$

where $s(k)$ does not depend on n. It is obvious that $s(k) \geq 2^k$ for every k, we have $s(3) \leq 9$ if $n \leq 100$ and $s(5) \leq 38$ if $n \leq 250$, asymptotic upper bounds have been established for large values of k.

Table 1.1: Integers n sums of two cubes

2	9	16	28	35	54	65	72	91
126	133	152	189	217	224	243	250	280
341	344	351	370	407	432	468	513	520
539	559	576	637	686	728	730	737	756
793	854	855	945	1001	1008	1024	1027	1064

By Fermat's last theorem, the sum of two cubes cannot be cubic. The conjectures about the number of terms necessary for the representation of an integer as a sum of cubes are not proved. Table (1.1) shows that the representation of integers as sums or differences of two cubes is restrictive. Let n be such that

$$x^3 \pm y^3 = n$$

if n is prime, by the factorization $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$ it is necessary that $x = y + 1$, the equation has many solutions such as

$$(n, x, y) = (19, 3, 2), (27, 4, 3).$$

The solutions (x, y) of the equations $n = x^3 + y^3$ are not always unique

$$\begin{aligned} 1729 &= 1 + 12^3 = 9^3 + 10^3, \\ 4104 &= 2^3 + 16^3 = 9^3 + 15^3 \end{aligned}$$

The length δ_k of the interval between x^k and $(x - 1)^k$ has bounds

$$kx^{k-1} < \delta_k < 2^k x^{k-1},$$

the interval of length δ_k contains n_{x-1} multiples of $(x - 1)^k$, the sub-interval of length δ_{k-1} between $(n_{x-1} + 1)(x - 1)^k$ and $(x - 1)^k$ contains n_{x-2} multiples of $(x - 2)^k$ and so on. An upper bound of $s(k)$ is

$$N_k = \sum_{i=2}^{x-1} n_i < 2^k \sum_{m=2}^{x-1} m^{k-1}(m - 1)^{-k}.$$

Euler's conjecture. For $k \geq 2$ and for every integer n, there exist integers $n_1, \ldots, n_{s(k)} \neq n$ such that

$$n^k = n_1^k + \cdots + n_{s(k)}^k$$

where $s(k)$ does not depend on n and $s(k) \geq k$ for every $k \geq 2$, with $s(2) = 2$. It extends Fermat's last theorem, where $s(k) > 2$, for every $k \geq 2$ (Section 3.2). For example, the equation $x^3 + y^3 = z^3$ cannot be solved by pairwise prime integers except by trivial solutions with a null component. The equation with rational cubes is equivalent to an equation $(x_1y_2z_2)^3 + (x_2y_1z_2)^3 = (x_2y_2z_1)^3$.

There exist integers n sums of a few powers $n^4 = n_1^4 + n_2^4$, $n^4 = n_1^4 + n_2^4 + n_3^4$ or $n^5 = n_1^5 + \cdots + n_3^5$ (Lander and Parkin, 1966), they are special cases rather than counter-examples of the conjecture.

Birch Swinnerton-Dyer conjecture. The square-free integers N congruent to $4, 6, 7, 8 \pmod 9$ are written as a sum of two cubes of $\mathbb{Q}$.

Let $\gcd(a, b) = 1$, $\gcd(k, n) = 1$, $\gcd(a, k) = 1$ and $\gcd(b, n) = d$, the equation

$$N = \frac{a^3}{b^3} + \frac{k^3}{n^3}$$

or

$$A = d^3N = \frac{a^3}{c^3} + \frac{k^3}{m^3}$$

with $\gcd(c, m) = 1$, is equivalent to

$$(cm)^3A = (am)^3 + (ck)^3 = (am + ck)(a^2m^2 + amk + c^2k^2)$$

where $\gcd(am + ck, cm) = 1$ therefore $cm \mid (a^2m^2 + ackm + c^2k^2)$ but a and m are not multiples of $c > 1$, c and k are not multiples of $m > 1$. It follows that $c = m = 1$ and a necessary condition for the existence of solutions is $b = n$.
The equation is then equivalent to

$$d^3N = a^3 + k^3 = (a + k)(a^2 - ak + k^2).$$

Because $\gcd(a, k) = 1$, the prime factors of d and N cannot divide both $a + k$ and $a^2 - ak + k^2d$ therefore there exist integers $s, t, u, v \geq 1$ relatively prime to a and k, such that $d = st$ and $N = uv$, with

$$a + k = s^3u, \quad a^2 - ak + k^2 = t^3v.$$

The conjecture leads to characterize the prime integers that divide $\gcd(N, a + k)$ and $\gcd(N, a^2 - ak + k^2)$.

1.2 Polygonal Numbers

The polygonal numbers are written as

$$p_{\alpha+2,n} = n + \alpha\frac{n(n-1)}{2},\ n \geq 1,\ \alpha \geq 1,$$

the ratio $p_{\alpha+2,n}p_{\alpha+2,n}^{-1}$ tends to 1 as n tends to infinity. They may be even or odd, they are triangular numbers with $\alpha = 1$, squares with $\alpha = 2$, pentagons with $\alpha = 3$, hexagons, etc. The triangular numbers satisfy the recurrence formula $p_{3,n} = p_{3,n-1} + n$ it follows that every integer $k = p_{3,m} + n$ is written as a sum

$$k = p_{3,m} + p_{3,n} - p_{3,n-1}$$

and every $k = n - p_{3,m}$ is the sum

$$k = p_{3,m} + p_{3,n} + p_{3,n-1},$$

n and therefore k being arbitrary, every integer is sum of three triangular numbers.

Table 1.2: Triangular numbers

1	3	6	10	15	21	28	3
45	55	66	78	91	105	120	136
153	171	190	210	231	253	276	300
325	351	378	406	435	465	496	528
561	595	630	666	703	741	780	820
861	903	946	990	1035	1081	1128	

The squares satisfy the recurrence

$$p_{4,n} = n^2 = p_{4,n-1} + 2n - 1,$$

they are obtained by adding the consecutive odd integers $1, 1+3, 4+5, 9+7, 16+9$ and so on. There exist consecutive triangular numbers which are not separated by squares, for example the interval $[231, 253]$ does not contain any square. There are two triangular numbers in some square intervals such as $[64, 81]$ or $[100, 121]$ and only one in other square intervals such as $[81, 100]$.

For the pentagonal numbers

$$p_{5,n} = p_{5,n-1} + 3(n-1) + 1$$

and $p_{5,n} < 2n^2$, Table (1.3) presents their first values.

Table 1.3: Pentagonal numbers

1	5	12	22	35	51	70	92
117	145	176	210	247	287	330	376
425	477	532	590	651	715	782	852
925	1001	1080	1162	1247	1335	1426	1520
1617	1717	1820	1926	2035	2147	2262	2380
2501	2625	2752	2882	3015	3151	3290	

If $n = 2a$, $p_{5,n}$ has the same parity as a, if $n = 2a + 1$, the parity of $p_{5,n}$ is the opposite of the parity of a.

The hexagonal numbers are

$$p_{6,n} = p_{6,n-1} + 4(n-1) + 1$$

all hexagonal numbers are triangular with

Table 1.4: Hexagonal number

1	6	15	28	45	66	91	120
153	190	231	276	325	378	435	496
561	630	703	780	861	946	1035	1128
1225	1326	1431	1540	1653	1770	2016	2145
2278	2415	2556	2701	2850	3003	3160	3321
3486	3655	3828	4005	4186	4371	4560	

$$p_{3,2n+1} = p_{6,n+1}$$

and $2p_{6,n} + 1 = (2n-1)^2$.
The heptagonal numbers are $p_{7,n} = p_{7,n-1} + 5(n-1) + 1$ A triangular number can be a

Table 1.5: Heptagonal numbers

1	7	18	34	55	81	112	148
189	235	286	342	403	469	540	616
697	783	874	970	1071	1177	1288	1404
1525	1651	1782	1918	2059	2205	2356	2512
2673	2839	3010	3186	3367	3553	3744	3940
4141	4347	4558	4774	4995	5221	5452	

square such as 1, $p_{3,8} = 36$, $p_{3,288} = 41616$ and every square $a = mk$ such that $n = k^2$ and $n + 1 = 2m^2$ or $n = 2k^2$ and $n + 1 = m^2$, with $\gcd(m, k) = 1$, it follows

$$k^2 - 2m^2 = -1 \quad \text{or} \quad m^2 - 2k^2 = 1.$$

A triangular number can be heptagonal such as 1 and 55. A square cannot be heptagonal except 1, 225 and all $p_{7,n}$ with integers n such that $\gcd(n, 5n - 3) = 1$ and

$$5n = 10k^2 = m^2 + 3 \quad \text{or} \quad 5n = 5k^2 = 2m^2 + 3.$$

In a regular polygon with n edges with angles $2\pi n^{-1}$, the vertex a_k in $\mathbb{C}$ satisfy $\|a_{k+1} - a_k\| = \|a_k - a_{k-1}\|$ hence

$$\frac{a_{k+1} - a_k}{a_k - a_{k-1}} = \frac{2\pi}{n},\ k = 2, \ldots, n - 1$$

and this property is specific for every n. For the pentagonal integers

$$\begin{aligned}
\frac{p_{3,n+1} - p_{3,n}}{p_{3,n} - p_{3,n-1}} &= \frac{n}{n-1}, \\
\frac{p_{4,n+1} - p_{4,n}}{p_{4,n} - p_{4,n-1}} &= \frac{2n+1}{2n-1}, \\
\frac{p_{5,n+1} - p_{5,n}}{p_{5,n} - p_{5,n-1}} &= \frac{3(2n+1)-1}{3(2n-1)-1},
\end{aligned}$$

for every α, this ratio depends on n and it is always strictly larger than 1.

For all $n > 1$ and $\alpha > 3$, the nth order $(\alpha + 1)$-polygonal numbers is the sum of the triangular number of the previous order and of the α-polygonal number of the same order

$$p_{\alpha+2,n} + p_{3,n-1} = p_{\alpha+3,n}.$$

From Plutarch (100 A.D.), for every $n \geq 1$

$$8p_{3,n} = (2n+1)^2 - 1.$$

For the squares $4n^2 = (2n)^2$ and for every $\alpha \geq 3$

$$2\alpha p_{\alpha+2,n} = (\alpha n + 1)^2 - (\alpha^2 + 1).$$

If α is even, let $\alpha = 2a$, this equality is written as a difference of two squares

$$2\alpha p_{\alpha+2,n} = (\alpha n + 1 - a)^2 - (a-1)^2.$$

Theorem 1.2.1 (Fermat) *Every integer is the sum of $k \leq 3$ triangular numbers, the sum of $k \leq 4$ squares, the sum of $k \leq (\alpha+2)$ α-polygons for every $\alpha \geq 3$.*

The decomposition of an integer n as a sum of polygons is not always unique. This theorem can be proved or verified numerically for small α but its algebraic proof has been the origin of controverses. The sum may be reduced to two triangular numbers, e.g. $36 = 15 + 31$.

The decomposition of an integer n as a sum of four squares does not necessarily include the largest integer q_n, integer part of $n^{\frac{1}{2}}$.
Example. Let $n = 419 = 3 \pmod 4$ with $q_n = 20$, then $n - q_n^2 = 4$, a sum of 4 squares, and

$$n - (q_n - 1)^2 = 58 = 7^2 + 3^3$$

hence $n = 3$. Moreover n is sum of three triangular numbers and no more than four pentagons and five hexagons

$$\begin{aligned} n &= p_{3,28} + p_{3,4} + p_{3,2}, \\ n &= p_{5,15} + p_{5,9} + p_{5,5} + p_{5,2}, \\ n &= p_{6,16} + p_{6,4} + 2p_{6,2} + p_{6,1}. \end{aligned}$$

Example. Let $n = 2027651281 = 1 \pmod 4$, it is not prime as proved by Fermat and $q_n = 45029$, then $n = (q_n - 1)^2 + r$ with $r = 130497$, $r = 361^2 + 176$ which proves

$$n = (q_n - 1)^2 + 359^2 + 40^2 + 4^2 = 4.$$

Its decomposition as a sum of pentagonal numbers does not exceeds 5 pentagons since

$$n = 2027589751 + 60501 + 925 + 92 + 12.$$

It is also the sum of no more than 5 hexagonal numbers,

$$n = 2027539360 + 107416 + 4371 + 91 + 43.$$

Fermat's Theorem does not apply to the triangular numbers, for instance 1055 is a sum of five triangular numbers $1055 = 1035 + 15 + 3 + 1 + 1$.

Lagrange improved Fermat's Theorem by reducing to a constant number the number of polygons of the sums, independently of their degree $\alpha + 2 > 3$.

Theorem 1.2.2 (Lagrange) *If $\alpha > 1$ is odd, every integer $n > 28\alpha^3$ is the sum of 4 polygons $p_{\alpha+2}$. If α is even, every odd integer $n > 7\alpha^3$ is the sum of 4 polygons $p_{\alpha+2}$ and every odd integer $n > 7\alpha^3 - 1$ is the sum of 1 and 4 polygons $p_{\alpha+2}$.*

Let $\alpha = 0 \pmod 4$, every even integer $n > 28\alpha^3$ is the sum of 4 polygons $p_{\alpha+2}$, under conditions concerning the parity of $\frac{\alpha}{2}$ and n.

Legendre (1810) proved several results about the decomposition of an integer n as a sum of three triangular numbers. Let us assume that there exist integers n, x, y, z such that $2n = a + b$ with

$$\begin{aligned} a &= x^2 + y^2 + z^2, \\ b &= x + y + z, \end{aligned}$$

a and b having the same parity, it follows that a cannot be equal to $2^\alpha(8k + 7)$ and $a^{\frac{1}{2}} \leq b \leq (3a)^{\frac{1}{2}}$. One of x, y and z has the same parity as a, for instance x. Denoting $2p = y + z$ and $2q = y - z$, $a = (b - 2p)^2 + (p + q)^2 + (p - q)^2$ and

$$u = \frac{3a - b^2}{2} = (3p - b)^2 + 3q^2$$

that is possible if u has simple divisors of the form $6n + 1$, and 3 if $3 \mid b$, 4 if $a = 8n + 3$ or if $4^k \mid a$ and $2^k \mid b$. Then the equation can be solved. This is not a general case, other

restrictions are necessary for the decomposition of an integer n as a sum of four triangular numbers so that $2n = a + b$ with

$$\begin{aligned} a &= u^2 + x^2 + y^2 + z^2, \\ b &= u + x + y + z, \end{aligned}$$

a and b having the same parity.

Theorem 1.2.3 (Fermat) *Every $n > 2$ of $\mathbb{P}$ has a unique decomposition as a difference of two squares*

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2.$$

The representation of an integer as a sum of two squares is not unique

$$\begin{aligned} 50 &= 1 + 7^2 = 5^2 + 5^2, \\ 65 &= 1 + 8^2 = 4^2 + 7^2, \\ 130 &= 3^2 + 11^2 = 7^2 + 9^2, \\ 265 &= 3^2 + 16^2 = 11^2 + 12^2, \\ 338 &= 7^2 + 17^2 = 13^2 + 13^2. \end{aligned}$$

Lagrange has established that the product of two sums of two squares is a sum of two squares

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{1.5}$$

and the following decompositions.

Necessary conditions for a prime number n to be a sum of two squares are $n = 1 \pmod 4$ or $n = 2$. A sufficient condition for a prime number n to be a sum of 3 or 4 squares is $n = 3 \pmod 4$, then it is the sum of the squares of three odd numbers or the sum of the squares of an even numbers and three odd numbers. This is not a necessary condition for $n = 1 \pmod 4$ may be the sum of the squares of two even numbers and an odd number.

The decomposition of a prime number as a sum or a difference of squares depends on its value modulo 4 or 8. For every odd integer $a > 0$, $a^2 = 1 \pmod 4$ and $a^2 + a$ is even, this entails

1. $n = 0 \pmod 4$ if it is the square of an even integer,
2. $n = 1 \pmod 8$ if $n = (2a+1)^2$ with $a > 0$, or $n = (2a+1)^2 + 2b^2$, $a, b > 0$ and b even,
3. $n = 1 \pmod 4$ if it is the sum of the squares of two odd integers $n = (2a+1)^2 + (2b+1)^2$, $a, b > 0$,
4. $n = 3 \pmod 8$ if it is the sum of the squares of three odd integers $n = (2a+1)^2 + (2b+1)^2 + (2c+1)^2$, $a, b, c > 0$,
5. $n = 5 \pmod 8$ if it is the sum of the squares $n = \{2(2a+1)\}^2 + (4b+1)^2$, $a, b > 0$,
6. $n = 7 \pmod 8$ if it is a sum of four squares $n = \{2(2a+1)\}^2 + (2b+1)^2 + (2c+1)^2 + (2d+1)^2$ with $a, b, c, d > 0$.

More results on the decomposition of integers are due to Fermat or have been proved using his first theorem by Euler, Lagrange and Legendre (Section 2.2).

Theorem 1.2.4 (Lagrange) *For every prime number $p > 2$, there exist integers x and y such that $1 + x^2 + y^2 = 0 \pmod p$, with $1 \leq m < p$ in $\mathbb{N}$ satisfying one of the equalities*

1. $x^2 + y^2 = 1 \pmod 4$ *if m is even,*
2. $x^2 + 2y^2 = 3 \pmod 8$ *if m is odd,*
3. $x^2 - 2y^2 = 7 \pmod 8$ *if m is odd.*

Example. $x^2 + 3y^2 = 1 \pmod 6$ for all x and y having different parities and such that $3 \nmid x$.

Proposition 1.2.5 *Let n be odd in $\mathbb{P}$, necessary conditions for the equality $n = x^2 + 2y^2$ are $n = 1 \pmod 8$ or $3 \pmod 8$. Necessary conditions for $n = x^2 - 2y^2$ are $n = 1 \pmod 8$ or $7 \pmod 8$.*

According to Proposition 1.2.5, $x^2 + 2y^2$ cannot be written as 5 or $7 \pmod 8$ and $x^2 - 2y^2$ is always different from 3 or $5 \pmod 8$.

Proposition 1.2.6 *Let n be odd in $\mathbb{P}$ and let A be odd in $\mathbb{N}$, n satisfies*

$$n = x^2 \pm Ay^2$$

only if $n = 1 \pmod 4$ *or* $n = 1 \pm A \pmod 8$ *or* $n = A \pmod 4$.

The proof relies on the parity of x and y. The next theorem proved by Legendre extends to quadratic equations.

Theorem 1.2.7 (Legendre) *Let x and y in $\mathbb{N}$ such that $\gcd(x, y) = 1$, every prime factor of an integer $x^2 + y^2$ is the sum of two squared integers. Every prime factor of $x^2 - y^2$ is the difference of two squared integers.*

By the same argument, every prime number dividing a sum of 4 squares is the sum of 4 squares.

Theorem 1.2.8 *Let x and y in $\mathbb{N}$ such that $\gcd(x, y) = 1$, every prime factor of an integer $x^2 \pm 2y^2$ is written as $a^2 \pm 2b^2$.*

Proof. Let $N \mid x^2 + 2y^2$, for all a and b of $\mathbb{N}$ such that $x' = x - aN$ and $y' = y - bN$ satisfy $|x'| < \frac{N}{2}$, $|y'| < \frac{N}{2}$ and $N \mid x'^2 + 2y'^2$ so there exists $N' \mid x'^2 + 2y'^2$ in $\mathbb{N}$ such that

$$NN' = x'^2 + 2y'^2 < \frac{3N^2}{4}.$$

If $N' = 1$, $N = x'^2 + 2y'^2$ and the proposition is proved, otherwise there exist N'', α and β in $\mathbb{N}$ such that $|x' - \alpha N''|$ and $|y' - \beta N''| < \frac{N'}{2}$, $N' \mid (x' - \alpha N')^2 + 2(y - \beta N')^2$ and

$$\begin{aligned} N'N'' &= (x' - \alpha N')^2 + 2(y' - \beta N')^2 < \frac{3N'^2}{4}, \\ NN'^2N'' &= (x'^2 + 2y'^2)\{(x' - \alpha N')^2 + 2(y' - \beta N')^2\} \\ &= (x'^2 + 2y'^2 - \alpha x'N' - 2\beta y'N')^2 + 2(\alpha y'N' - \beta x'N')^2 \\ &= (NN' - \alpha x'N' - 2\beta y'N')^2 + 2(\alpha y'N' - \beta x'N')^2, \end{aligned}$$

dividing by N'^2 implies

$$NN'' = (N - \alpha x' - 2\beta y')^2 + 2(\alpha y' - \beta x')^2 = x''^2 + 2y''^2$$

with $x'' = N - \alpha x' - 2\beta y'$ and $y'' = \alpha x' - \beta y'$. If $N'' = 1$, there exists a finite sequence $(N^{(k)}, \alpha^{(k-2)}, \beta^{(k)})_{k=1,\ldots,K}$ satisfying the same property and the last integer $N^{(k)}$ is one.

The proof is similar for the prime factors of $x^2 - 2y^2$. □

Theorem 1.2.9 *Let x, y and a in $\mathbb{N}$ such that $\gcd(x, y) = 1$, every prime factor of $x^2 \pm ay^2$ is written as $s^2 \pm at^2$, every prime factor of $x^4 - a^2y^4$ is written as $s^4 - a^2t^4$.*

The proof is the same as in Theorem 1.2.8 where $a = 2$. The prime factors of a quadratic number $x^2 + bxy + cy^2 = (x \pm ay)^2$, with $b = \pm 2a$ in $\mathbb{Z}$ and $c = a^2$ in $\mathbb{N}_+$, are deduced.

The solutions of an equation

$$x^2 + a = 0 \pmod{n}$$

with an integer n are deduced from Theorem 1.2.9. All prime divisors of n have the form $y^2 + a$, with integers y. The product of two divisors of n solutions of the equation is

$$(s^2 + a)(t^2 + a) = (st + a)^2 + a(s - t)^2,$$

it is solution of an equation $x^2 + ay^2 = 0 \pmod{n}$.

In the same way, the product of two prime factors $p_1 = s_1^2 + at_1^2$ and $p_2 = s_2^2 + at_2^2$ of $x^2 + ay^2$ has the same form $(s_1s_2 + at_1t_2)^2 + a(s_1t_2 + at_1s_2)^2$.

1.3 Quadratic Fields

Let d in $\mathbb{Z}$ be without square factor (sqare-free), $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field with $[K : \mathbb{Q}] = 2$, where $[K : \mathbb{Q}]$ is the dimension of K as a vector space on $\mathbb{Q}$. Gauss's integer ring is

$$\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\},$$

every element of $\mathbb{Z}[i]$ is root of a normed equation of second degree with coefficients in $\mathbb{Z}$. The equation $x^2 + 1 = 0$ has the solutions $x = \pm i$ in $\mathbb{Z}[i]$, the equation $x^3 +$

$1 = (x+1)(x^2-x+1) = 0$ has the solutions $x = -1$ and $x = \frac{1}{2}(1 \pm \sqrt{3}i)$ in $\mathbb{Q}[\sqrt{3}i]$. The equation $x^4 + 1 = 0$ has the solutions $x^2 = \pm i$ in $\mathbb{Z}[i]$, the roots of $x^5+1 = (x+1)(x^4-x^3+x^2-x+1) = 0$ are $x = -1$ or such that $x^4-x^3+x^2-x+1 = 0$.

The units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$ and p in $\mathbb{Z}$ is prime in $\mathbb{Z}[i]$ if it is divisible only by a unit or by itself. If p is prime in $\mathbb{Z}$ and p is sum of two squares, it is not prime in $\mathbb{Z}[i]$ since $a^2 + b^2 = (a + bi)(a - bi)$.

Theorem 1.3.1 *For every p in $\mathbb{Z}[i]$, p is prime if and only if $p = a + ib$ with a and b in $\mathbb{Z}^*$ and $N(p) = a^2 + b^2$ is prime or p is prime in $\mathbb{Z}$ and p is not a sum of two squares.*

The first condition is a consequence of the equivalence of $z_1 z_2 \mid p$ and the same property for the complex norms $|z_1|.|z_2| \mid |p|$.
Example. $n = 2$ factorizes as $n = (1 + i)(1 - i) = i(1 - i)^2$, where $\gcd(i, 1 - i) = 1, 2$ is not prime in $\mathbb{Z}[i]$.
Example. For every $p = 1 \pmod 4$, $2^{\frac{p-1}{2}} = 1 \pmod p$ and $2^{2k} - 1 = x^2 + i^2 = 0 \pmod p$ hence $p \mid x + i$ or $p \mid x - i$ with $x = 2^k$. Let $p = 3 \pmod 4$, then $2^{\frac{p-1}{2}} = -1 \pmod p$ and $p \mid 2^{2k+1} + 1$ therefore p is prime in $\mathbb{Z}[i]$ if it is prime in $\mathbb{Z}$.

Euclid's division is defined in $\mathbb{Z}[i]$ with a condition for the norms, for all a and $b \neq 0$ in $\mathbb{Z}[i]$ there exist q and r in $\mathbb{Z}[i]$ such that

$$a = qb + r, \ N(r) < N(b).$$

Euclid's property (1.1) still holds if p is prime in $\mathbb{Z}[i]$

$$p \mid ab \quad \text{implies} \quad p \mid a \quad \text{or} \quad p \mid b.$$

In the euclidean division of $y = a + ib$ by $y_1 = a_1 + ib_1$ in $\mathbb{Z}[i]$, there exist $z = s + it$ and $y_2 = a_2 + ib_2$ in $\mathbb{Z}[i]$ such that

$$y = zy_1 + y_2, \quad 0 \leq N(y_2) < N(y_1).$$

A common divisor of y and y_1 in $\mathbb{Z}[i]$ is determined by a sequence of the euclidean divisions starting from $y = zy_1 + y_2$ and, for $k = 1, \ldots, n-1$, the division of y_k by y_{k+1} such that $0 \leq N(y_{k+1}) < N(y_k)$, until $y_{n+1} = 0$. The elements of $\mathbb{Z}[i]$ are not ordered

and the sequence $(y_k)_{k=1,n+1}$ is not necessarily unique, it defines y_n as a common divisor of y and y_1 but this is not necessarily the greatest. An algebraic integer x of a field K on $\mathbb{Z}$ is a root of a polynomial with integer coefficients, it solution in K of an algebraic equation

$$P(x) = a_0x^n + a_1x^{n-1} + \cdot + a_n = 0$$

with $a_1, \ldots, a_n$ in $\mathbb{Z}$. The algebraic numbers are therefore countable in $\mathbb{R}$. A polynomial of degree n, $P(x) = x^n + a_1x^{n-1} + \cdot + a_n = 0$ on $\mathbb{Z}$ is primitive if $\gcd(a_0, a_1, \ldots, a_n) = 1$. Let d in $\mathbb{N}^*$, it is square-free if $a^{-2}d$ is not an integer for every a in $\mathbb{N}^*$. Let d a square-free integer, a quadratic field $\mathbb{Q}(\sqrt{d})$ is generated by a root of a quadratic algebraic equation. Let d in $\mathbb{N}^*$ such that $a^{-3}d$ is not an integer for integer every a, the cubic root $\alpha = d^{\frac{1}{3}}$ and α^2 are generators of the field $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha, \alpha^2)$.

Theorem 1.3.2 *Let $x = a + b\sqrt{d}$ with d a square-free in $\mathbb{N}^*$, a and b in $\mathbb{Q}$, then x is an algebraic integer of $\mathbb{Q}(\sqrt{d})$ if it is root of the quadratic polynomial*

$$(X - a)^2 - db^2 = 0,$$

with the necessary and sufficient conditions that its trace

$$Tr(x) = 2a$$

and its squared norm

$$N(x) = a^2 - db^2$$

belong to $\mathbb{Z}$.

For $\alpha = a + b\sqrt{d}$ in $\mathbb{Q}(\sqrt{d})$, the multiplicative endorphism $m_\alpha : x \mapsto \alpha.x$ is linear, it is expressed in the basis $(1, \sqrt{d})$ as the vector

$$m_\alpha(s + t\sqrt{d}) = M(\alpha)\begin{pmatrix} s \\ t \end{pmatrix},$$

with the matrice

$$M(\alpha) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}.$$

The trace and the determinant of $M(\alpha)$ are $Tr(x)$ and, repectively, $N(x)$ and

$$m_\alpha(\alpha) = \begin{pmatrix} N(\alpha) \\ bTr(\alpha) \end{pmatrix}.$$

The addition and the multiplication of matrices $M(\alpha)$ and $M(\beta)$ generate a matrix field $M_2(\mathbb{Q})$ with the properties $m_\alpha + m_\beta = m_{\alpha+\beta}$ and $m_\alpha \circ m_\beta = m_{\alpha\beta}$. In $M_2(\mathbb{Q})$, each element has an inverse $m_{\alpha^{-1}}$ associated to the matrix M_α^{-1}, for the multiplication. The properties of m_α imply $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$, $Tr(\alpha.\beta) = \alpha Tr(\beta)$ and $N(\alpha.\beta) = N(\alpha).N(\beta)$ for all α and β in $\mathbb{Q}[\sqrt{d}]$

In a field $\mathbb{Z}[\sqrt{d}]$, with d square-free, the norm N of a product is equal to the product of the norms which entails a generalization of Theorem 1.3.1.

Theorem 1.3.3 *For every p in $\mathbb{Z}[\sqrt{d}]$, p is prime if and only if $p = a + \sqrt{d}b$ with a and b in $\mathbb{Z}^*$ and $N(p)$ is prime or p is prime in $\mathbb{Z}$ and p is not a sum $a^2 - db^2$.*

The last condition is a consequence the factorization of $a^2 - db^2$ in $\mathbb{Z}[\sqrt{d}]$. The first condition comes from the property of the norm. Euclid's division and property (1.1) are still true if p is prime in $\mathbb{Z}[\sqrt{d}]$, furthermore every element of $\mathbb{Z}[i]$ has a factorization (1.2) according to its prime divisors in $\mathbb{Z}[i]$.

Theorem 1.3.4 *Let d be square-free in $\mathbb{N}^*$, if $d = 1 \pmod 4$*

$$\mathbb{Q}(\sqrt{d}) = \Big\{a + \frac{b(1+\sqrt{d})}{2}; a, b \in \mathbb{Z}\Big\} = \mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big],$$

if $d = 2$ or $3 \pmod 4$

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d}; a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}].$$

Proof. The conditions of Theorem 1.3.3 are fulfilled for the fields $\mathbb{Q}(\sqrt{d})$ in both cases.

To prove the equality, let $x = a + b\sqrt{d}$ be an integer of $\mathbb{Q}(\sqrt{d})$, $u = 2a$ and

$$N(a) = \frac{u^2}{4} - db^2$$

belong to $\mathbb{Z}$. If $d = 1 \pmod 4$ and u is odd, $2b$ must belong to $\mathbb{Z}$, otherwise a and b must belong to $\mathbb{Z}$ and $a^2 - db^2 = 0$ which is excluded for d is not a square.

If $d = 2$, the condition $N(a)$ belongs to $\mathbb{Z}$ implies

$$\frac{u^2}{4} - 2b^2 - 4kb^2 \in \mathbb{Z}$$

where k belongs to $\mathbb{Z}$, then if u must be even for $\frac{1}{4} - 2b^2 - 4kb^2$ does not belong to $\mathbb{Z}$. In the same way, if $d = 2$ or $3 \pmod 4$, the condition

$$\frac{u^2}{4} - 3b^2 - 4kb^2 \in \mathbb{Z}$$

with k in $\mathbb{Z}$ implies that u is even. □

If $d = 1 \pmod 4$, $y = \frac{a \pm b\sqrt{d}}{2}$ in $\mathbb{Q}(\sqrt{d})$ is a root of the equation

$$y^2 - ay + N(y) = 0$$

if $d = 2$ or $3 \pmod 4$, $y = a \pm b\sqrt{d}$ in $\mathbb{Q}(\sqrt{d})$ is a root of the equation

$$y^2 - 2ay + N(y) = 0.$$

The group of the units U of a quadratic field $\mathbb{Q}[\sqrt{d}]$ is the set of the elements having an inverse with norm ± 1. Every u in U hs an inverse u' in U such that $uu' = \pm 1$ and for all x in $\mathbb{Q}[\sqrt{d}]$ and u in U, $ux = \pm x(u')^{-1}$ where $\pm(u')^{-1}$ belongs to U.

Lemma 1.3.5 *Let d be square-free in $\mathbb{N}^*$, if $\mathbb{Q}[\sqrt{d}]$ has units, the set of its units larger than 1 has a smallest unit $\omega > 1$.*

Proof. For every unit $w = a + b\sqrt{d} > 1$, with a and b in $\mathbb{N}$, has the inverse $w^{-1} = \pm (a - b\sqrt{d})$ such that $w - w^{-1} = 2a > 1$ or $2b\sqrt{d} > 1$, hence

$$w^2 - w - 1 = \Big(w - \frac{1+\sqrt{5}}{2}\Big)\Big(w - \frac{1-\sqrt{5}}{2}\Big) > 0$$

therefore $w > \frac{1+\sqrt{5}}{2}$, the largest root of $w^2 - w - 1 = 0$. □

Theorem 1.3.6 *Let d be square-free in $\mathbb{N}^*$, if $\mathbb{Q}[\sqrt{d}]$ has a unit group U with a smallest element ω larger than one, then $U = \{w^n, n \in \mathbb{Z}\}$ where ω is the smallest element of U larger than one.*

Proof. If a unit u larger than one were different from w^n, for every n in $\mathbb{N}$, there exists n such that $w^n < u < w^{n+1}$ therefore $1 < uw^{-n} < w$ which is impossible for uw^{-n} is a unit. □

Example. In $\mathbb{Z}[\sqrt{2}]$, the equation $X^2 - 2X - 1 = 0$ has the roots $\omega = 1 + \sqrt{2}$ and

$-\omega^{-1}$, where $\omega^{-1} = -1 + \sqrt{2}$, then $\pm\omega^n$ and $\pm\omega^{-n}$ belong to U. Their norms are $N(\pm\omega^{2k+1}) = -1$ and $N(\pm\omega^{2k}) = 1$.
The group of the units of $K = \mathbb{Q}(\sqrt{d})$ in $\mathbb{Z}$ is therefore the set

$$U = \{x \in \mathbb{Q}(\sqrt{d}) : N(x) = \pm 1\}.$$

Let w be the smallest element of U larger than 1, the units of

$$U_+ = \{\pm w^{2n}, n \in \mathbb{N}\}$$

have the norm 1 and the units of

$$U_- = \{\pm w^{2n+1}, n \in \mathbb{N}\}$$

have the norm -1.

1.4 Quadratic Equations

Pell's equation

$$x^2 - dy^2 = 1 \tag{1.6}$$

is the equation for the units $u = x + y\sqrt{d}$ of $\mathbb{Q}(\sqrt{d})$ having the norm one.

Let w is the smallest unity larger than 1 of $\mathbb{Z}(\sqrt{d})$, it is written as

$$\begin{aligned} w &= a + b\sqrt{d}, \\ N(w) &= a^2 - db^2 = \pm 1 \end{aligned}$$

and the solutions of (1.6) are (x, y) such that $x = \pm 1 \pmod{d}$ and

$$x + y\sqrt{d} = w^{2n},\ n \geq 1.$$

Fermat stated that for every integer d, there exist infinitely many squares such that adding 1 to their product with d is a square, with the example $3.16 + 1 = 49$. Pythagore's equality provides a method to prove the existence of rational units of $K = \mathbb{Q}(\sqrt{d})$. Let y be an arbitrary integer, the equality $4dy^2 + (y^2 - d)^2 = (y^2 + d)^2$ is equivalent to

$$\frac{2y^2}{x^2}\, d + 1 = \frac{(y^2 + d)^2}{x^2},$$

with $x = \pm(y^2 - d)$. An integer $d = y^2 \pm 1$ provides integer units of $K = \mathbb{Z}(\sqrt{d})$ with norm 1. If $y = r^{-1}s$ is rational, the above equality is written as

$$(s^2 + dr^2)^2 - (2sr)^2\, d = (s^2 - dr^2)^2.$$

Example. Let $A = 2, 5, 10, 17, 26, 37, 65$, there exists a square such that $y^2 - A = 1$ and

$$(y^2 + A)^2 - (2y^2)^2 A = 1.$$

Let $A = 3, 15, 35, 63, 80, 99$, there exists a square such that $A - 1 = a^2 d$ with $a = 1$ or $a > 1$ and with the free-square integers $d = 2, 3, 5, 7, 11, 15$, the equation becomes

$$(y^2 + A)^2 - (2ay^2)^2 d = 1.$$

There are infinitely many integers A or d such that the equation $N(a + b\sqrt{d}) = 1$ has solutions and all squares y^2 such that $y^2 \pm 1$ is free-square are convenient.
The question is whether this procedure goes through all free-square integers, Wallis (1657) proposed the following algorithm to answer it. Let d a free-square integer, $d = c^2 - b$ where c^2 is the least square larger than d, for every integer a

$$da^2 = (ac)^2 - ba^2.$$

Writting this equation until there exists k such that $(ac)^2 + 1 = ba^2 + k^2$ yields a solution (a, k) of $k^2 - da^2 = 1$. For example, the equation $5a^2 = (3a)^2 - 4a^2$ becomes $80 = 5a^2 = 9^2 - 1$ with $a = 4$ and it provides $u = 9 + 2\sqrt{5}$ with norm 1.

Theorem 1.4.1 *If Pell's equation (1.6) has a solution in $\mathbb{Q}[\sqrt{d}]$ for a square-free integer d, it has infinitely many solutions.*

Let (a, b) be the minimal solution of the equation, then

$$x + y\sqrt{d} = (a + b\sqrt{d})^n$$

is solution for every $n \geq 2$ because the norm is associative. Euler proposed the solution

$$\begin{aligned} x &= \frac{1}{2}\Big\{(a + \sqrt{d}b)^2 + (a - \sqrt{d}b)^2\Big\}, \\ y &= \frac{\sqrt{d}}{2d}\Big\{(a + \sqrt{d}b)^2 - (a - \sqrt{d}b)^2\Big\} \end{aligned}$$

Table 1.6: Integer solutions of Pell's equation

d	(y, x)
2	$(2,3),(12,17),(70,99)$
3	$(1,2),(4,7),(15,26),(56,97)$
5	$(4,9),(70,171)$
6	$(2,5),(20,49)$
7	$(3,8),(48,17)$
8	$(1,3),(6,17)$
10	$(6,19)$
11	$(10,3)$
12	$(7,2)$

for an equation $x^2 - dy^2 = (a^2 - db^2)^2$. More generally, Section 4.2 develops the method of continuous fractions to solve the equations $N(a + b\sqrt{d}) = \pm k$ on $\mathbb{Z}$.

Let $d < 0$ in $\mathbb{Z}$, we consider the complex quadratic fields generated by $i\sqrt{-d}$. Let $d' = -d$, if $d' = 1 \pmod 4$ then $d = 3 \pmod 4$ and if $d' = 2$ or $3 \pmod 4$ then $d = 2$ or $1 \pmod 4$ and Theorem 1.3.4 applies to d'.

Theorem 1.4.2 *If* $d = 3 \pmod 4$

$$\mathbb{Q}(i\sqrt{d}) = \Big\{a + \frac{b(1 + i\sqrt{d})}{2}; a, b \in \mathbb{Z}\Big\} = \mathbb{Z}\Big[\frac{1 + i\sqrt{d}}{2}\Big],$$

if $d = 1$ *or* $2 \pmod 4$

$$\mathbb{Q}(\sqrt{d}) = \{a + bi\sqrt{d}; a, b \in \mathbb{Z}\} = \mathbb{Z}[i\sqrt{d}].$$

Algebraic equations of higher degrees have been studied in $\mathbb{Z}[i]$, Euler proved that $(8, 9)$ is the unique solution in $\mathbb{Z} \times \mathbb{Z}$ of $x^3 - y^2 = -1$ and Lebesgue proved that the equation

$$x^p - y^2 = 1,\ p \geq 2$$

cannot be solved in $\mathbb{Z}^* \times \mathbb{Z}^*$. In the latter cases x must be odd and the equation

$$x^p = y^2 + 1 = (y + i)(y - i)$$

implies $d = \gcd(y+i, y-i)$ divides x, $d \mid 2i$ and $d \mid 2y$ hence $d = \pm 1, \pm i$ therefore $y+i = d(a \pm ib)^p$ and $y-i = d(a' \mp ib')^p$ where $a \pm ib$ and $a' \mp ib'$ are relatively primes

$$\begin{aligned} 2y &= d\{(a \pm ib)^p + (a' \mp ib')^p\}, \\ 2i &= d\{(a \pm ib)^p - (a' \mp ib')^p\}. \end{aligned}$$

Expanding the right side of these expressions implies $b = \pm 1$ and $b' = \pm 1$, this leads to contradictions. Quadratic diophantine equations are solved by factorization in $\mathbb{Z}[i\sqrt{d}]$. The equation $x^2 + 2 = z^3$ has the unique solution $(x, z) = (5, 3)$ where z is an integer dividing $x^2 + 2$ in $\mathbb{Z}[i\sqrt{d}]$. The equation

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

has infinitely many solutions such as $(x, y, z) = (10, 9, 7)$. They are defined by integers p and q such that $p \pm i\sqrt{3}q$ divide z and

$$x = p(p^2 - 9q^2), \quad y = \pm 3q(p^2 - q^2).$$

For every integer a, the equation

$$x^2 + ay^2 = z^3$$

has infinitely many solutions

$$x = p(p^2 - 3aq^2), \quad y = \pm q(3p^2 - aq^2), \quad z = p^2 + aq^2$$

such that $p \pm i\sqrt{a}q$ divide z, with arbitrary p and q. **Catalan's conjecture**. The equation $x^p - y^q = 1$, with $xy > 0$, $u > 1$ and $v > 1$, has the unique solution $x^p = (\pm 3)^2$, $y^q = 2^3$.

Catalan's conjecture restricted to even exponents q is proved by Lebesgue's result who studied the case $x^p - y^2 = 1$. The proof for $p = 2$ and $q > 3$ odd is similar, writting

$$y^q = x^2 - 1 = (x-1)(x+1),$$

$d = \gcd(x+1, x-1)$ divides 2 so $d = \pm 1, \pm 2$. Let $x + 1 = du^q$ and $x - 1 = dv^q$ with $u > v$ in $\mathbb{Z}$, u and v having the same sign and such that $uv = y$, this entails

$$2 = d(u^q - v^q) = d(u - v)(u^{q-1} + u^{q-2}v + \cdots + v^{q-1})$$

which is impossible. For odd exponents p and q, it remains to prove the conjecture that $y^q = x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$ cannot be solved with $x \neq 1$ and $y \neq -1$ in $\mathbb{Z}^*$.

The irrational numbers are limits of rational fractions, they are expressed as infinite continued fractions such as (4.7). The rational and irrational numbers are algebraic, the non algebraic numbers are transcendental, they are predominant in $\mathbb{R}$ where they are limits of sequences of rational or irrational numbers issued from Taylor expansions of functions and they converges faster than the sequences defining the irrational numbers. There existence is proved by Liouville's theorem, Section 4.4. Hermite proved that π is transcendental, Hilbert, Weierstrasse and Lindemann proved it for e, the same arguments apply to prove that e^x, $\sin x$ and $\cos x$ are transcendental for every x algebraic. Let $a > 0$ and $b > 0$ be algebraic numbers such such b is not a square, $\sqrt{b}$ is algebraic, $\log a$ and the exponential $a^{\sqrt{b}}$ are transcendental.

1.5 Exercises

Exercise 1.1. Let a and b be relatively prime integers. Prove

1. the equalities $au + bv = 1$ and $au' + bv' = 1$ imply $u = u' + kb$ and $v' = v - ka$ in $\mathbb{Z}$, with k in $\mathbb{N}$,
2. there exist unique integers u and v such that $|u| < \frac{b}{2}$ and $|v| < \frac{a}{2}$.

Exercise 1.2. Determine x such that $x = y \pmod{p}$ and $x = z \pmod{q}$ where p and q are relatively prime.
Exercise 1.3. Prove $n^5 + 5 = k^2$ has no integer solution.
Exercise 1.4. Find a, b, c pairwise relatively primes such that

$$a^2 - ab + b^2 = c^2.$$

Exercise 1.5. Solve the equation $x^n + y^n = 1$.
Exercise 1.6. Find the units of $\mathbb{Q}[\sqrt{5}]$ and $\mathbb{Q}[i\sqrt{5}]$.