Chapter 4

Prime Numbers and Irrational Numbers

Abstract

The question of the existence of prime numbers in intervals is treated using the approximation of cardinal of the primes $\pi(x)$ given by Lagrange.

Legendre's theory to find explicitly the roots of quadratic algebraic polynomials is related to the search of the unit ring of the groups F_p, we present the method with applications and its generalization to higher degrees.

4.1 Cardinal of the Primes in Intervals

Let $\pi(n)$ be the cardinal of the set of the prime numbers lower than a prime integer n and let $u(n)$ be the function defined on $\mathbb{P}$ as the sum of the inverse of the prime numbers lower than n

$$u(n) = \sum_{k \in \mathbb{P}, k \leq n} \frac{1}{k}. \tag{4.1}$$

Legendre (1830) have proposed an approximation of the function $\pi(n)$ from the variations of the function $u(n)$, as n is large

$$\pi(n) = \frac{n}{\log n - A}\{1 + o(1)\} \tag{4.2}$$

with a constant $A = 1.08366$. His numerical comparaison to the existing tables prove that the relative approximation error of $\pi(n)$ is decreasing and smaller than 10^{-4} for n larger than $5.\,10^4$. Chebyshev's approximation

$$\pi(n) \sim Li(x) = \int_2^n \frac{dx}{\log x}$$

has always a much larger error, its bounds

$$.89\, Li(x) \leq \pi(n) \leq 1.11\, Li(x)$$

are not sharp and the true value of $\pi(n)$ is closer than the lower bound than to $Li(x)$.

Bounds for an approximation of $\pi(n)$ by $n(\log n)^{-1}$ are unprecise, from (4.2)

$$\pi(n) \sim n(\log n)^{-1} \sum_{k \geq 0} A^k (\log n)^{-k}$$

as n tends to infinity so there exists a constant a such that

$$\frac{n}{\log n} < \pi(n) < \frac{an}{\log n}.$$

According to Bertrand's postulate (1845), for every n of $\mathbb{N}^*$ there exists a prime number p such that

$$n < p \leq 2n.$$

He proved this inequality on the interval $[2, 4001]$. In this section, it is extended to infinity using Legendre's approximation (4.2) and other open questions on the existence of primes in smaller intervals at infinity are proved.

Theorem 4.1.1 *For all n and k of $\mathbb{N}^*$, the number of primes in the interval $]kn, (k+1)n]$ has the order $\pi(n)$ and*

$$\pi(n+m) - \pi(m) \leq \pi(n)$$

as m and n tend to infinity.

Proof. As n tends to infinity, the cardinal of the prime numbers between kn and $(k+1)n$ has the order $\pi(k+1)n) - \pi(kn)$ and it is approximated by

$$\begin{aligned}\pi_k(n) &= \frac{(k+1)n}{\log n + \log(k+1)} - \frac{kn}{\log n + \log k} \\ &\quad + A\Big[\frac{(k+1)n}{\{\log n + \log(k+1)\}^2} - \frac{kn}{(\log n + \log k)^2}\Big]\{1 + o(1)\} \\ &= \frac{n}{\log n} - o\Big(\frac{n}{\log^2 n}\Big)\end{aligned}$$

where the second term is neglectable with respect to the first one. The last equality proves that $\pi_k(n) \leq \pi(n)$ as m and n tend to infinity. □

The inequality $\pi(n+m) - \pi(m) \leq \pi(n)$ is known as Hardy-Littlewood conjecture and it was not proved for large numbers.

Legendre conjectured the existence of a prime number in the intervals

$$]n^2, (n+1)^2].$$

It can checked for small values of n such as $]4, 9]$, $]9, 16]$, $]16, 25]$, $]25, 36]$, $]36, 49]$, etc. but it was not proved for large n and Legendre's approximation of $\pi(n)$ enables to approximate the order of the cardinal of $\mathbb{P}$ in such intervals.

Theorem 4.1.2 *For all n and $k \geq 2$ of $\mathbb{N}^*$, the number of primes in the interval $]n^k, (n+1)^k]$ has the order*

$$\pi_k(n) = \frac{n^{k-1}}{\log n}$$

as n tends to infinity.

Proof. As n tends to infinity, the number of primes in the interval has the order $\pi(n+1)^k) - \pi(n^k)$ which is expanded as

$$\begin{aligned}\pi_k(n) &= \frac{(n+1)^k}{k\log(n+1)} - \frac{n^k}{k\log n} \\ &\quad + A\Big\{\frac{(n+1)^k}{k^2\log^2(n+1)} - \frac{n^k}{k^2\log^2 n}\Big\}\{1+o(1)\} \\ &= \frac{n^k}{k\log n}\Big\{\Big(1+\frac{1}{n}\Big)^k \frac{\log n}{\log n + \log\Big(1+\frac{1}{n}\Big)} - 1\Big\} + O\Big(\frac{n^k}{\log^2 n}\Big) \\ &= \frac{n^{k-1}}{\log n} + O\Big(\frac{n^{k-1}}{\log^2 n}\Big)\end{aligned}$$

so it tend vers infinity avec n. □

Proposition 4.1.3 *There exist infinitely many intervals* $]n^k, (n+1)^k]$ *that contain Mersenne numbers* $M_m = 2^m - 1$.

Proof. Let m, k and n be integers such that $n^k \leq M_m \leq (n+1)^k$ then

$$\frac{k\log n}{\log 2} < m < \frac{k\log(n+2)}{\log 2} \tag{4.3}$$

since $2^m \leq (n+1)^k + 1 \leq (n+2)^k$ for all n and k in $\mathbb{N}$. There exists k_0 in $\mathbb{N}$ such that for every $k \geq k_0$, there exist integers m and n satisfying (4.3). Since there are infinitely many intervals $]n^k, (n+1)^k]$, there exist infinitely many m satisfying (4.3). □

Proposition 4.1.4 *There are infinitely many intervals* $]n^k, (n+1)^k]$ *that contain Fermat numbers* $F_p = 2^{2^p} - 1$.

Proof. Let p, k and n be integers such that $n^k \leq F_p \leq (n+1)^k$ and for $m = 2^p$

$$\frac{k\log(n-1)}{\log 2} < m < \frac{k\log(n+1)}{\log 2}. \tag{4.4}$$

Furthermore, there exists k_0 such that for all $k \geq k_0$, there exist n and p such that 2^p belongs to the interval defined by (4.4). □

Let $(x_n)_{n\geq 1}$ be an integer sequence tending to infinity with n, Another problem is to determine the order of the smallest integer a_n such that the intervals $]x_n, x_n + a_n]$, $n \geq 2$, do not contain prime number.

Theorem 4.1.5 *Let $a_n = o(x_n)$, n tends to infinity the cardinal of the prime numbers in the interval $]x_n, x_n + a_n]$ has the order*

$$\pi(x_n, a_n) = \frac{a_n}{\log x_n}.$$

Proof. As n tends to infinity, thee cardinal of the prime numbers between x_n and $x_n + a_n$ has the expansion

$$\begin{aligned}
\pi(x_n, a_n) &= \frac{x_n + a_n}{\log(x_n + a_n)} - \frac{x_n}{\log x_n} \\
&\quad + A\Big\{\frac{x_n + a_n}{\log^2(x_n + a_n)^2} - \frac{x_n}{\log^2 x_n}\Big\}\{1 + o(1)\} \\
&= \frac{x_n}{\log x_n}\Big\{\Big(1 + \frac{a_n}{x_n}\Big)\frac{\log x_n}{\log x_n + \log\Big(1 + \frac{a_n}{x_n}\Big)} - 1\Big\} \\
&\quad + \frac{Ax_n}{\log^2 x_n}\Big[\Big(1 + \frac{a_n}{x_n}\Big)\frac{\log x_n}{\Big\{\log x_n + \log\Big(1 + \frac{a_n}{x_n}\Big)\Big\}^2} - 1\Big] \\
&= \frac{a_n}{\log x_n}\Big\{1 + \frac{A-1}{\log x_n}(1 + o(1))\Big\}
\end{aligned}$$

its limit as n tends to infinity is deduced. □

At infinity, an interval $]x_n, x_n + a_n]$ defined by $a_n = x_n^{\frac{1}{2}}$ or $a_n = \log^2 x_n$ contains prime numbers but an interval with length $a_n = \log x_n$ is generally not large enough for small values of n though primes may occur for large x_n, for example in the interval $]4001, 4008]$, with $x_n = n$. If $a_n = o(\log x_n)$, $\pi(n)$ tend to zero as n tends to infinity and there are no primes in the interval $]x_n, x_n + a_n]$.

Legendre stated several results about the multiples of prime number in an arithmetic series. Let A and C be relatively primes, for all n in $\mathbb{N}^*$ and $\theta \leq n$ in $\mathbb{P}$ such that $\theta \nmid A$, there exists α in $\mathbb{N}^*$ such that in the sequence of n terms

$$A - C, 2A - C, 3A - C, \ldots, nA - C, \tag{4.5}$$

$\theta \mid A\alpha - C$, then

$$A\alpha - C, A(\alpha + \theta) - C, A(\alpha + 2\theta) - C, \ldots$$

is an integer sequence of multiples of θ. With two primes θ and $\lambda > 2$ that do not divide A, there exist only two consecutive multiples of θ and, respectively, λ. With three primes

$3, \theta, \lambda$, there exist four consecutive multiples of $3, \theta, \lambda, 3$. With five primes $3, 5, \theta, \lambda, \mu$, there exist a maximum of $M = 6$ consecutive multiples of $5, 3, \theta, \mu, 3, 5$. More generally, with a sequence of k primes including two unknown numbers, the maximum number of consecutive multiples of the k primes is

$$M = \pi^{(k-1)} - 1$$

where $\pi^{(k-1)}$ is the $(k-1)$th term of the sequence of the odd prime integers.

Theorem 4.1.6 (Legendre) *Let $\theta_1, \ldots, \theta_k$ be k prime numbers. In every sequence of $\pi^{(k-1)}$ consecutive terms of (4.5), there exists at least one prime number which is not divided by $\theta_1, \ldots, \theta_k$.*

As a consequence, every arithmetic series having a first term and a progression relatively prime, contains infinitely many prime numbers.

4.2 Legendre's Quadratic Equations

The equation

$$p^2 - Aq^2 = \pm k, \tag{4.6}$$

with an integer k, has been explicitly solved using an expansion of $\sqrt{A}$ in a series of fractions. Let a be the larger integer such that $a^2 \leq A$ and let $A = a^2 + b$ with $b < a^2$

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

where $a^{(1)}$ is the larger integer before $x^{(1)}$, $x^{(1)} > 0$ and $x^{(2)} > 0$ satisfies

$$\begin{aligned} x^{(2)} &= \frac{b}{\sqrt{A} + a - a^{(1)}b} = \frac{\sqrt{A} - (a - a^{(1)}b}{1 + 2aa^{(1)} - a^{(1)2}b} \\ &= a^{(2)} + \frac{1}{x^{(3)}}, \end{aligned}$$

where $a^{(2)}$ is the larger integer before $x^{(2)}$ and $x^{(3)} > 0$. Continuing this expansion, for every $k > 1$, there exist $M > 0$ and $D > 0$, $a^{(k)}$, the larger integer before $x^{(k)}$, and

$x^{(k+1)} > 0$ such that

$$\begin{aligned} x^{(k)} &= \frac{\sqrt{A}+M}{D} = a^{(k)} + \frac{1}{x^{(k+1)}}, \\ x^{(k+1)} &= \frac{D}{\sqrt{A}+M-Da^{(k)}} = \frac{\sqrt{A}+M'}{D'}, \\ M' &= Da^{(k)} - M, \\ D' &= \frac{(\sqrt{A}+M)(\sqrt{A}+M')}{D} - a^{(k)}(\sqrt{A}+M'). \end{aligned}$$

The continued fraction

$$\sqrt{A} = a + \cfrac{1}{a^{(1)} + \cfrac{1}{a^{(2)} + \cfrac{1}{a^{(3)} + \ldots}}} \tag{4.7}$$

where all $a^{(k)}$ are integers, converges to $\sqrt{A}$.

The properties of the continued fractions enable to solve quadratic integer equations. Let us consider a continued fraction x defined by (4.7) with integers $a^{(k)}$, its first terms are

$$a, \frac{aa^{(1)}+1}{a^{(1)}} \quad , \frac{aa^{(1)}a^{(2)}+a+a^{(2)}}{a^{(1)}a^{(2)}+1}.$$

A classical representation of the ith convergent of a continued fractions is the equality of its numerator p_i and the determinant of the matrix

$$\begin{pmatrix} a_0 & 1 & 0 & & \cdots & & 0 \\ -1 & a_1 & 1 & 0 & & \cdots & 0 \\ 0 & -1 & a_2 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & -1 & a_{i-2} & 1 & 0 \\ 0 & & \cdots & 0 & -1 & a_{i-1} & 1 \\ 0 & & & \cdots & 0 & -1 & a_i \end{pmatrix}$$

and its denominator is similar to the numerator p_{i-1} calculated for $(a_1, \ldots, a_{i-1})$.

Let $p^0 q^{0-1}$ and pq^{-1} be two consecutive fractions of (4.7) with arbitrary orders k and $k+1$, the $k+2$th fraction is deduced from the previous equation as

$$\frac{p'}{q'} = \frac{p\mu + p^0}{q\mu + q^0}$$

where $p' > q'$ so they are defined by

$$\begin{aligned} p' &= p\mu + p^0, \\ q' &= q\mu + q^0. \end{aligned} \tag{4.8}$$

Theorem 4.2.1 *The consecutive finite fractions p^0q^{0-1} and pq^{-1} of (4.7) satisfy*

$$pq^0 - p^0q = \pm 1$$

with the value 1 if pq^{-1} has an even order, and -1 if pq^{-1} has an odd order.

Proof. Considering 4 consecutive fractions p^0q^{0-1}, pq^{-1}, $p'q'^{-1}$ and $p''q''^{-1}$

$$pq' - p'q = -(pq^0 - p^0q) = -(p'q'' - p''q')$$

furthermore, the first fractions are a and $(aa^{(1)} + 1)/a^{(1)}$ for which $pq^0 - p^0q = 1$ and the result follows. □

By construction, the finite continued fractions of x in (4.7) are alternatively larger and smaller than x, with $a^{(k)} > 0$ and $x^{(k)} > 0$. The even fractions are larger than x and the odd fractions are smaller. By induction, for a continued fraction with ith term $p_iq_i^{-1}$ and initial term a_0, we have

$$\begin{aligned} p_iq_{i-1} - p_{i-1}q_i &= \pm(-1)^i, \\ p_iq_{i-2} - p_{i-2}q_i &= \pm(-1)^i a_i, \\ p_iq_{i-3} - p_{i-3}q_i &= \pm(-1)^i(a_ia_{i-1} + 1), \\ p_iq_{i-4} - p_{i-4}q_i &= \pm(-1)^i(a_ia_{i-1}a_{i-2} + a_i + a_{i-2}), \text{ etc.} \end{aligned}$$

Corollary 4.2.2 *For every non square integer d, there exists a sequence $(p_nq_n^{-1})_{n\geq 0}$ converging to $\sqrt{d}$ and such that*

$$\left|\sqrt{d} - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2}.$$

Proof. From Theorem 4.2.1

$$\left|\frac{p}{q} - \frac{p^0}{q^0}\right| = \frac{|pq^0 - p^0q|}{q^0q} = \frac{1}{q^0q}.$$

□

Choosing the mean of two consecutive terms of the continued fraction gives a better approximation of $\sqrt{d}$, for n large enough.

Example. The integer part of $\sqrt{31}$ is 25 and the square root of 31 is the continued fraction

$$\begin{aligned}
\sqrt{31} &= 5+\frac{1}{x},\\
x &= \frac{1}{\sqrt{31}-5}=\frac{\sqrt{31}+5}{6}=1+\frac{\sqrt{31}-1}{6},\\
x^{(1)} &= \frac{\sqrt{31}+1}{5}=1+\frac{\sqrt{31}-4}{5},\\
x^{(2)} &= \frac{\sqrt{31}+4}{3}=3+\frac{\sqrt{31}-5}{3},\\
x^{(3)} &= \frac{\sqrt{31}+5}{2}=5+\frac{\sqrt{31}-5}{2},\\
x^{(4)} &= \frac{\sqrt{31}+5}{3}=3+\frac{\sqrt{31}-4}{3},\\
x^{(5)} &= \frac{\sqrt{31}+4}{5}=1+\frac{\sqrt{31}-1}{5},\\
x^{(6)} &= \frac{\sqrt{31}+1}{6}=1+\frac{\sqrt{31}-5}{6},\\
x^{(7)} &= 5+\sqrt{31}.
\end{aligned}$$

The cycle of fractions restarts infinitely many often at $x^{(7)}=10+x^{-1}=2a+x^{-1}$, using $\sqrt{31}=5+x^{-1}$. The first integer of the period is $\alpha=1$ due to x and the last one is $2a$. The integers of a cycle are $1,1,3,5,3,1,1,10$, the sequence of the first seven terms is symmetric with respect to 5 and the denominator 1 of $x^{(7)}$ leads to replace $a=5$ by $2a$ at the end of the cycle. The partial quotients after a are

$$1,\ \frac{1}{2},\ \frac{4}{5},\ \frac{21}{37},\ \frac{51}{118},\ \frac{88}{155},\ \frac{155}{273},\ \text{etc.},$$

they have alternative orders

$$\frac{1}{2}<\frac{4}{7},\quad \frac{4}{7}>\frac{21}{37},\quad \text{etc.}$$

One can prove the same properties for every irrational number with a cycle $a^{(i)}$, $a^{(i+1)}$, …, $a^{(i+s)}$ and the partial fractions have alternating orders.

Proposition 4.2.3 (Legendre) *In the expansion of $\sqrt{A}$ as a cyclic continued fraction, the cycle $a^{(i)}, a^{(i+1)}, \ldots, a^{(j)}$ is symmetric.*

Proof. Let pq^{-1} be a finite fraction with integer part μ in the expansion of $\sqrt{A}$, there exists $z = x^{(j)}$ corresponding to the end of the period such that

$$x^{-1} = z - \mu = \sqrt{A} - a.$$

Let $p^0 q^{0-1}$ be the finite fraction preceeding pq^{-1}, then

$$\begin{aligned} \sqrt{A} &= \frac{pz + p^0}{qz + q^0} = \frac{p\sqrt{A} + p(\mu - a) + p^0}{q\sqrt{A} + q(\mu - a) + q^0}, \\ Aq &= p(\mu - a) + p^0, \\ p &= q(\mu - a) + q^0 \end{aligned}$$

from the last equation, $pq^{-1} = (\mu - a) + q^0 q^{-1}$ where $\mu - a$ is the integer part of pq^{-1}, it follows that $\mu = 2a$. Moreover $q^0 = p - aq$ therefore the integer part of $p^0 q^{0-1}$ is a, it is symmetric to the first term.

Let $D^{0-1}(A^0 + I^0)$, $D^{-1}(A + I)$ and $D'^{-1}(A' + I')$ be the consecutive quotients in the continued fraction of $\sqrt{A}$, $I = aD^0 - I^0$ and $I' = \mu D - I$, $A - I^2 = D^0 D$ and $A' - I'^2 = DD'$, it follows that

$$D' = D^0 + \mu(I - I').$$

The reverse equations are similar, $I^0 = aD^0 - I$ and $D^0 = D' + \mu(I - I')$ which proves the symmetry of the series of integer parts in the continued fraction of $\sqrt{A}$. □

Example. The continued fraction of $\sqrt{271}$ begins with $a = 16$ and it has the symmetric cycle

$$2, 6, 10, 1, 4, 1, 1, 2, 1, 2, 1, 15, 1, 2, 1, 2, 1, 1, 4, 1, 10, 6, 2, 32.$$

The integer solutions of (p, q) of Pell's equation (4.6), with constants A integer such that $\sqrt{A}$ is irrational and k in $\mathbb{Z}$, can be found in the series of the partial continued fractions pq^{-1} of $\sqrt{A}$, if the equation has solutions.

Example. The first term in the continued fraction of $\sqrt{31}$ is pq^{-1} determined by $(p, q) = (11, 2)$ such that $p^2 - 31q^2 = -3$.

Theorem 4.2.4 *If $\sqrt{A}$ has a cyclic continued fraction, the equation $p^2 - Aq^2 = \pm 1$ has infinitely many solutions (p, q) and $p^2 - Aq^2 = 1$ if and only if $p - \sqrt{A}q > 0$.*

It is not proved that the equations $p^2 - Aq^2 = k$ have solutions for all A and k. For every partial continued fraction pq^{-1} of $\sqrt{A}$ irrational, there exists a constant k such that (p, q) is solution of an equation (4.6) with the constant k in $\mathbb{Z}$. The values of k are small due to the oscillations of the consecutive values of pq^{-1} (Theorem 4.2.1).

The following cases present solutions of (4.6) where A is not a square number. The square root of A is defined by a and the series $(a^{(j)}_{j=1,\ldots,J})$. The continued fractions of $\sqrt{A}$ are defined as follows

$\sqrt{2}$ has the series $1, 2, 2, 2, \ldots$,

$\sqrt{3}$ has the cycle $(1, 2)$ with $a = 1$,

$\sqrt{5}$ has the series $2, 4, 4, 4, \ldots$,

$\sqrt{6}$ has the cycle $(2, 4)$ with $a = 2$,

$\sqrt{7}$ has the series $(1, 1, 1, 2)$ with $a = 2$,

$\sqrt{11}$ has the cycle $(3, 6)$,

$\sqrt{13}$ has the series $(1, 1, 2)$ with $a = 3$,

$\sqrt{15}$ has the cycle $(1, 6)$ with $a = 3$,

$\sqrt{17}$ has the series $4, 8, 8, 8, \ldots$,

$\sqrt{19}$ has the cycle $(2, 1, 3, 1, 2, 8)$ with $a = 4$,

$\sqrt{21}$ has the cycle $(1, 1, 2, 1, 1, 8)$ with $a = 4$,

$\sqrt{23}$ has the cycle $(1, 3, 1, 8)$ with $a = 4$,

$\sqrt{27}$ has the cycle $(5, 10)$ with $a = 5$,

$\sqrt{29}$ has the cycle $(2, 1, 1, 2, 10)$ with $a = 5$.

The length of the cycles is $s = 1$ for the series defining $\sqrt{2}$, $\sqrt{5}$, $\sqrt{17}$, for these numbers $\sqrt{A} = a + x^{-1}$ where x satisfies $(x-k)^2 = k^2 + 1$ for an integer k. The symmetry of the continued fractions is not specific to the integers, the fraction of the transcendental number π is cyclic with $a = 1$ and the cycle $(1, 1, 2)$. The partial quotients up to $(a^{(j)}_{j=1,\ldots,J})$ of $\sqrt{A}$ are solutions of equations $p^2 - Aq^2 = k$ with varying k, they are given in the following tables for $A = 1 \pmod 4$, $A = 3 \pmod 4$ and $A = 7 \pmod 8$. The group of the units of $\mathbb{Q}(\sqrt{2})$ is $\{(1+\sqrt{2})^n, n \geq 1\}$.

Proposition 4.2.5 (Legendre) *Let $A = 1 \pmod 4$ such that $\sqrt{A}$ is irrational and let (p, q) be the smallest solution of the equation $p^2 - Aq^2 = 1$ with $q > 1$, then there exists a solution (g, h) of $p^2 - Aq^2 = -1$ and such that (g, h) is smaller than (p, q).*

Its proof relies on a factorization of q and on the fact that p and q do not have the same parity. It applies to $A = 5$ and $A = 17$, then $Z[\sqrt{5}]$ and $Z[\sqrt{17}]$ have infinitely many roots of the unit and their smallest roots with q larger than 1 are respectively

$$\begin{aligned} w_5 &= 9 + 4\sqrt{5}, \\ w_{17} &= 33 + 8\sqrt{17}, \end{aligned}$$

and the roots of the unit for $A = 5$ are $2 + \sqrt{5}, (2+\sqrt{5})^2, (2+\sqrt{5})^3, (2+\sqrt{5})^4$. The fields $Z[\sqrt{13}]$ and $Z[\sqrt{29}]$ have infinitely many roots of the unit w^n where

$$\begin{aligned} w_{13} &= 29 + 8\sqrt{13}, \\ w_{29} &= 70 + 13\sqrt{29}. \end{aligned}$$

For these numbers, Pell's equations with $k = 1$ has the solutions $(p, q) = (649, 180)$ for $A = 13$ and $(p, q) = (9801, 1820)$ for $A = 29$.

Proposition 4.2.6 (Legendre) *Let $A = 3 \pmod 4$ be prime and let (p, q) be the smallest solution of the equation $p^2 - Aq^2 = 1$ with $q > 1$, then*

1. *if $A = 3 \pmod 8$, the equation $x^2 - Ay^2 = -2$ has a solution smaller than (p, q),*
2. *if $A = 7 \pmod 8$, the equation $x^2 - Ay^2 = 2$ has a solution smaller than (p, q).*

Table 4.1: Solutions of equations (4.6) with $A = 1 \pmod 4$

	A					
(p, q)	5	$(2, 1)$	$(9, 4)$	$(38, 17)$	$(161, 72)$	$(682, 305)$
k		-1	1	-1	1	-1
(p, q)	13	$(4, 1)$	$(7, 2)$	$(11, 3)$	$(18, 5)$	$(44, 13)$
k		3	-3	4	-1	9
(p, q)	17	$(4, 1)$	$(33, 8)$	$(268, 65)$		
k		-1	1	-1		
(p, q)	21	$(5, 1)$	$(9, 2)$	$(23, 5)$	$(32, 7)$	
k		4	-3	4	-5	
(p, q)	29	$(5, 1)$	$(11, 2)$	$(27, 5)$	$(70, 13)$	$(727, 135)$
k		-4	5	4	-1	4

Examples are presented in Table (4.2) for the first case with $A = 3, 11, 27$ and in Table (4.3) for the second case with $A = 7$ and 23, the proposition does not apply to $A = 15$ which is not prime.

The groups of units of $Z[\sqrt{3}]$, $Z[\sqrt{11}]$, $Z[\sqrt{19}]$ and $Z[\sqrt{27}]$ have infinitely many elements and their smallest units larger than 1 are respectively

$$\begin{aligned} w_3 &= 2 + \sqrt{3}, \\ w_{11} &= 10 + 3\sqrt{11}, \\ w_{19} &= 170 + 39\sqrt{19}, \\ w_{27} &= 26 + 5\sqrt{27}. \end{aligned}$$

Theorem 4.2.7 (Legendre) *If the equation*

$$p^2 - Aq^2 = -1 \tag{4.9}$$

has solutions, then A is a sum of two squares.

Equation (4.9) cannot be satisfied if $A = 3 \pmod 4$ which cannot be sum of two squares, it requires $A = 1 \pmod 4$.

Table 4.2: Solutions of equations (4.6) with $A = 3 \pmod 8$

	A					
(p, q)	3	$(1, 1)$	$(2, 1)$	$(5, 3)$	$(7, 4)$	$(19, 11)$
k		-2	1	-2	1	-2
(p, q)	11	$(3, 1)$	$(10, 3)$	$(63, 19)$	$(199, 60)$	
k		-2	1	-2	1	
(p, q)	19	$(4, 1)$	$(9, 2)$	$(13, 3)$	$(48, 11)$	$(61, 14)$
k		-3	5	-2	5	-3
(p, q)	27	$(5, 1)$	$(26, 5)$	$(265, 51)$	$(1351, 260)$	
k		-2	1	-2	1	

Table 4.3: Solutions of equations (4.6) with $A = 7 \pmod 8$

	A					
(p, q)	7	$(3, 1)$	$(5, 2)$	$(8, 3)$	$(13, 5)$	$(21, 8)$
k		2	-3	1	-6	-7
(p, q)	15	$(4, 1)$	$(27, 7)$	$(31, 8)$	$(213, 55)$	
k		1	6	1	-6	
(p, q)	23	$(5, 1)$	$(19, 4)$	$(24, 5)$	$(211, 44)$	
k		2	-7	1	-7	
(p, q)	31	$(6, 1)$	$(11, 2)$	$(39, 7)$	$(206, 37)$	$(1520, 273)$
k		5	-3	2	-3	1

Necessary conditions for (4.9) with $A = 1 \pmod 4$ are q odd and p even since q even would imply $x^2 = -1 \pmod 4$ and this is impossible. Let $A = 1 \pmod 4$, with $q = 1$, the equation is equivalent to $A = p^2 + 1$. Otherwise, let

$$\frac{\sqrt{A} + I^0}{D^0}, \quad \frac{\sqrt{A} + I}{D}$$

be the continued fractions with integer parts μ at the middle of the cycle, then $D^0 = D$ and $A = D^2 + I^2$. For example $29 = 5^2 + 2^2$.

Kaplan and Williams (1986) noted that the equation (4.9) has solutions if and only if the continued fraction of $\sqrt{A}$ has a cycle with an odd length. Moreover if A has a prime factor equal to $-1 \pmod 4$, this equation and the equation $p^2 - Aq^2 = -4$ have no

solutions. If the equation $p^2 - Aq^2 = -4$ has solutions, either $A = 5 \pmod 8$ or $A = 0 \pmod 4$ and $p^2 - Aq^2 = -4$ is equivalent to p even and to the equation $x^2 - aq^2 = -1$ for $2x = p$ and $4a = A$, then the length of the cycle of $\sqrt{\frac{m}{4}}$ is odd.

For $A \neq 1 \pmod 4$ such that $\sqrt{A}$ has a continued fraction with a cycle of length $s > 1$, Pell's equation has a solution (p, q) such that pq^{-1} is the partial continued fraction of order $s - 1$ after the integer part of $\sqrt{A}$.

According to Dedekind's proof of the existence of a non trivial solution of Pell's equation for every A, such solutions would be deduced from solutions (x, y) and (x', y') of an equation $x^2 - Ay^2 = k$ having several solutions, this equation is supposed to imply the equalities $xx' - Ayy' = x^2 - Ay^2 = 0 \pmod k$ and $xy' - yx' = 0 \pmod k$ which entail

$$\begin{aligned} \xi^2 - A - \eta^2 &= 1, \\ (x - \sqrt{A}y)(x' + \sqrt{A}y') &= k(\xi + \eta\sqrt{A}), \\ (x + \sqrt{A}y)(x' - \sqrt{A}y') &= k(\xi - \eta\sqrt{A}). \end{aligned}$$

Numbers 19 and 21 proves that this argument fails, the equation $x^2 - 21y^2 = 4$ has several solutions $(5, 1)$, $(23, 5)$ and $(110, 24)$. With the values $(x, y) = (5, 1)$ and $(x', y') = (23, 5)$, we have $xx' - Ayy' = 2 \pmod k$ and $xy' - yx' = 2 \pmod k$ then

$$\begin{aligned} (x - \sqrt{A}y)(x' + \sqrt{A}y') &= 2(1 + \sqrt{A})) + 4(\xi + \eta\sqrt{A}), \\ (x + \sqrt{A}y)(x' - \sqrt{A}y') &= 2(1 - \sqrt{A})) + 4(\xi - \eta\sqrt{A}), \\ (x^2 - 21y^2)(x'^2 - 21y'^2) &= 4(1 - A) + 16(\xi^2 - A\eta^2) + 16(\xi - \sqrt{A}\eta), \\ (\xi^2 - A\eta^2) + (\xi - \sqrt{A}\eta) &= 6 \end{aligned}$$

and $\eta = 0$. Therefore the existence of several solutions of an equation with $k \neq 1$ does not imply the existence of a solution for $k = 1$. The third solution of $x^2 - 21y^2 = 4$ is $x'' = 110, y'' = 24$, this implies $(55, 12)$ is solution of $x^2 - 21y^2 = 1$. For $A = 19$, the equations $x^2 - 19y^2 = k$ with $k = -3$ and 5 have several solutions and they do not provide solutions for the equation with $k = 1$.

If A is not prime, the equations can be simplified if A, k and p have a least common factor larger than 1. For $A = 15$ and with the solution $(p, q) = (27, 7)$, the equation $p^2 - 15q^2 = 6$ is identical to $3m^2 - 5n^2 = 2$, with $m = 7$. For $A = 21$ and with

$(p, q) = (9, 2)$, the equation $p^2 - 21q^2 = -3$ is identical to $3m^2 - 7q^2 = -1$, with $m = 3$.

Proposition 4.2.8 *Let $A = NC$ be square-free and let k be such that $C \mid k$, the equation $p^2 - Aq^2 = k$ has solutions such that $C \mid p$ if and only if the equation*

$$Mm^2 - Nn^2 = k'$$

has solutions, where $CM = m$ and $Ck' = k$.

Let $A = 1 \pmod 4$ be a square-free integer, the equation $p^2 - Aq^2 = k$ has solutions if there exist integers a and b such that $p^2 = a^2 + b^2 + k$. Necessary conditions to solve the equation $p^2 - Aq^2 = k$ are

1. $k = 1 \pmod 4$, p is odd and q is even,
2. $k = 3 \pmod 4$, p is even and q is odd,
3. $k = 0 \pmod 4$, p and q are odd,

Let $A = 3 \pmod 4$, necessary conditions to solve the equation $p^2 - Aq^2 = k$ are

1. $k = 1 \pmod 4$, p and q do not have the same parity,
2. $k = 1 - A \pmod 8$, p and q are odd,
3. $k = 0 \pmod 4$, p and q are even,

then the equation $p^2 - Aq^2 = k$ is equivalent to $p^2 + q^2 = k \pmod 4$ and it has no solution with $k = 3 \pmod 4$.

Theorem 4.2.9 (Legendre) *For all M and N prime and equal to $1 \pmod 4$, one of the equations*

$$Mp^2 - Nq^2 = \pm 1, \qquad p^2 - MNq^2 = 1$$

has solutions. For all M and N prime and equal to $3 \pmod 4$, the equation

$$Mp^2 - Nq^2 = \pm 1$$

has solutions.

4.3 Complex Quadratic Rings

A quadratic equation $x^2 + x + p = 0$ with p in $\mathbb{P}$ generates a quadratic ring

$$k_p = \mathbb{Z}[\omega_p] = \{a + \omega_p b, a, b \in \mathbb{Z}\}$$

where ω_p is a complex roots of the equation. Let z in k, its norm is a quadratic form

$$N(z) = \left(a - \frac{b}{2}\right)^2 + \frac{b^2}{4}(4p - 1) = (a^2 - ab + pb^2).$$

The units of k_p satisfy $N(z) = \pm 1$, the primes of k_p belong to $\mathbb{P}$ or their norm belongs to $\mathbb{P}$. For the units, the integers $2a - b$ and b are solutions of the equation

$$x^2 + Ay^2 = \pm 4, \quad A = 4p - 1 > 0, \tag{4.10}$$

where A cannot be a square since $A = 3 \pmod 4$, equivalently

$$a^2 - ab + pb^2 = \pm 1.$$

The norm of the units belonging to $\mathbb{Z}$ is positive and the units are ± 1. Then k_p is an unitary principal ideal on $\mathbb{Z}$. In the field of the fractions of k_p, every element z has a symmetric $\pm \bar{z} N^{-1}(z)$, according to the unit.

The primes of k_p belong to $\mathbb{P}$ or their norm belongs to $\mathbb{P}$, in the latter case $b = 2b'$ and the integers $a - b'$ and b' are solutions of the equation

$$x^2 + Ay^2 = \pi$$

where π belongs to $\mathbb{P}$. The complex roots $\omega_p = \frac{1}{2}(-1 + i\sqrt{A})$ and $\bar{\omega}_p$ of the equation $x^2 + x + p = 0$ are primes in k_p, they have the norm p. The factorization of the integers $n = N(z)$, with z in k_p, as $n = z\bar{z}$ is unique up to the sign of the prime factors and for every z of k_p there exist $z_1, \ldots, z_m$ primes in k_p such that $z = \prod_{i=1}^{m} z_i^{\alpha_i}$ with positive integers exponents.

Let π in $\mathbb{P}$, if there exists B in $\mathbb{Z}$ such that $B^2 = (4\pi - 1)A^{-1}$, then

$$\frac{-1 \pm iB\sqrt{A}}{2}$$

are complex primes in k_p with the norm π and B is solution of the equation

$$1 + Az^2 = 4\pi.$$

Example. Let $B = 3$ with $(\pi, p) = (61, 7), (367, 41)$ and $(421, 47)$ and $B = 5$ with $(\pi, p) = (54, 5)$ and $(421, 17)$ provide primes of k_p.

For the complex primes of k_p, the equation entails $\pi > p$ and $\gcd(x, y, \pi) = 1$ in $\mathbb{Z}$, and for every prime factor n of A, $x^2 = \pi \pmod n$ hence $\left(\frac{\pi}{n}\right) = 1$.
Example. Let $p = 3$, $A = 11$ is prime and $x^2 = \pi \pmod{11}$, there exist solutions (x, y, π) such as

$$(\pm 6, \pm 1, 47),\ (\pm 3, \pm 2, 53),\ (\pm 2, \pm 3, 103),\ (\pm 8, \pm 3, 163),$$

they yield the primes

$$7 + 2\omega_p,\ 5 + 4\omega_p,\ 5 + 206\omega_p,\ 11 + 326\omega_p$$

as $x > 0$ and $y > 0$, and those with negative components. They are not ordered though their norms are and one cannot prove that there are infinitely many prime norms for elements of k_p as expected.

The equation $x^2 - x + p = 0$ with p in $\mathbb{P}$ generates a quadratic ring

$$K_p = \{a + \theta_p b, a, b \in \mathbb{Z}\}$$

where $\theta_p = \frac{1}{2}(1 + i\sqrt{A})$ is a complex roots of the equation. Let z in K_p, its norm is a quadratic form

$$N(z) = a^2 + ab + pb^2.$$

The units of K_p are defined by integers $2a + b$ and b are solutions of the equation $N(z) = \pm 1$, they are ± 1. The primes of K_p are defined by integers $a - b'$ and b' solutions of the equation

$$x^2 + Ay^2 = \pi$$

where $b = 2b'$ and πbelongs to $\mathbb{P}$, they are deduced from the primes of K_p. The complex roots θ_p and $\bar{\theta}_p$, $1 - \theta_p$ and $1 - \bar{\theta}_p$ are primes of K_p with the norm p. If p is not prime, the same properties are still valid for the units and the primes.

An equation $x^2 + sx + t = 0$, with p and q in $\mathbb{Z}$, generates a real or complex irrational ring I according to the sign of A. Let θ be a complex roots of the equation, with $A = 4t - s^2 > 0$, its norm is $N(\theta) = t$. Let $z = a + b\theta$ in I, its norm is a quadratic form

$$N(z) = a^2 - abs + tb^2.$$

The units are ± 1 and $z = a + b\theta$ where the integers a and b satisfy the equation $a^2 - abs + tb^2 = \pm 1$.
Example. With $s = 4$, the equation is equivalent to Pell's equation

$$(a - 2b)^2 - (4 - t)b^2 = \pm 1$$

and it has solutions with $t = 3$.

The primes of K_p are defined by integers a and b such that $a - \frac{b}{2}$ and $\frac{b}{2}$, with b even, are solutions of the equation

$$x^2 - Ay^2 = \pi, \quad A = s^2 - 4t > 0,$$

where π belongs to $\mathbb{P}$. If t is prime, θ and $\bar{\theta}$, $s + \theta$ and $s + \bar{\theta}$ are prime in I, with the norm t. Tables for the Pell equations provide the values of s and t for which the ring I generated by the equation has a prime with norm π. The question is solved by the same arguments if x^2 has an integer coefficient.

4.4 Algebraic Numbers of Degree n

An algebraic number with degree $n > 1$ is the root of an irreductible polynomial with degree n.

Theorem 4.4.1 (Liouville) *For every algebraic number with degree $n > 2$, there exists a constant $c > 0$ such that for all rationals pq^{-1}*

$$\left| \sqrt{d} - \frac{p}{q} \right| > \frac{c}{q^n}.$$

The prime factors of $x^n \pm 1$ are characterized by the following theorems (Legendre, 1808).

Theorem 4.4.2 *Every p prime such that $p \mid (x^n + 1)$ has the form $p = 1 \pmod{2n}$ or $p \mid (x^\omega + 1)$ where ω is the quotient of n divided by an odd integer.*

Proof. If p is even (respectively odd), x is odd (respectively even) and prime to p. By assumption, we have

$$x^n = -1 \pmod{p}$$

and n is odd. From the euclidean division of p by $2n$, $p = 2na + k$, with a and k in $\mathbb{N}$, $k < 2n$ and from Fermat's first theorem

$$x^{p-1} = x^{k-1} = 1 \pmod{p}.$$

This is always true with $k = 1$, let $k > 1$ and let $\omega = \gcd(n, k-1)$. By Euler's theorem, there exist π and ρ such that $\pi n - \rho(k-1) = \omega$, and $\pi n' - \rho k' = 1$ where $n = \omega n'$ and $k - 1 = \omega k'$, this implies

$$x^{\omega} = (-1)^{\pi} \pmod{p}$$

where ω and π are odd. □

Theorem 4.4.3 *Every p prime such that $p \mid (x^n - 1)$ has the form $p = 1 \pmod{n}$ or $p \mid (x^{\omega} - 1)$ where $\omega \mid n$.*

The proof is similar with the euclidean division of p by n. These methods have been used previously by Fermat to find large prime integers and to determine whether integers $x^n \pm 1$ larger than 2.10^6 are primes.

Theorem 4.4.4 *The equation $x^n = b \pmod{a}$ with a in $\mathbb{P}$ such that $\gcd(a, b) = 1$ and $\gcd(n, a-1) = \omega$, has solutions only if*

$$b^{\frac{a-1}{\omega}} = 1 \pmod{a},$$

then x is solution of the equation

$$x^{\omega} - b^m = 0 \pmod{a},$$

where $mn + \rho(a-1) = \omega$.

The existence of integers m and ρ is due to Euler's theorem 1.1.1. The equation $x^n = b \pmod{a}$ has n solutions $\theta, \theta^2, \ldots, \theta^n \pmod{a}$. Under the conditions of Theorem 4.4.4, let $n = \omega n'$ and $a = 1 + \omega a'$

$$x^n = (x^{\omega})^{n'} = (b^m)^{\frac{n}{\omega}} = b(b^{\frac{a-1}{\omega}})^{-\rho} = b \pmod{a}.$$

As a special case, the n solutions of the equation $x^n = 1 \pmod{a}$, with a in $\mathbb{P}$ and $\gcd(n, a-1) = \omega$, are solutions of $x^{\omega} = 1 \pmod{a}$.

Theorem 4.4.5 (Lagrange) *The equation $x^n = b \pmod a$, with a in $\mathbb{P}$ and b prime to a, has a solution if*

$$b^m = \pm 1 \pmod a,$$

where m divides $\frac{a-1}{n}$. Let $\omega = \gcd(m, n)$ and let π and σ be such that

$$\pi n - \omega\sigma m = \omega$$

1. *if $\omega = 1$, a solution is $x = b^\pi y$ where $y^n = (\pm 1)^\sigma \pmod a$,*
2. *if $\omega \neq 1$, a solution x satisfies $x^\omega = b^\pi y$ where $y^{\frac{n}{\omega}} = (\pm 1)\sigma \pmod a$.*

Under the conditions and denoting $n = \omega n'$

$$x^n = x^{\omega n'} = b^{\pi n'} y^{n'} = b^{1+\sigma m} y^{\frac{n}{\omega}} = b \pmod a.$$

By Theorem 1.1.1, for every b prime to a, the equation $x^n = b \pmod a$, with a in $\mathbb{P}$ such that n and $a - 1$ are relatively primes, has the solution $x = b^\pi$ where π is the smallest integer such that $n\pi + (a - 1)\rho = 1$.

For every n, $(x - 1) \mid (x^n - 1)$ and the ratio

$$P(x) = (x^n - 1)(x - 1)^{-1}$$

is an algebraic polynomial. These polynomials $P(x)$ have a unique factorization as a product of irreductible polynomials

1. $x^3 - 1 = (x - 1)P_2(x)$ where

   $$P_2(x) = x^2 + x + 1$$

   has the complex roots $(-1 \pm i\sqrt{3})/2$,
2. $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$ has the complex roots $\pm i$,
3. $x^5 - 1 = (x - 1)P_4(x)$ where

   $$P_4(x) = x^4 + x^3 + x^2 + x + 1$$

   is an irreductible algebraic polynomial with 4 complex roots,

4. $x^6 - 1 = (x-1)(x+1)P_1(x)P_2(x)$, where

$$P_1(x) = x^2 - x + 1$$

has the complex roots $(1 \pm i\sqrt{3})/2$,

5. $x^7 - 1 = (x+1)P_6(x)$ where

$$P_6(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

has 6 complex roots,

6. $x^8 - 1 = (x-1)(x^2+1)(x^4+1)$,

7. $x^9 - 1 = (x-1)(x^3+1)P_2(x)$,

8. $x^{10} - 1 = (x-1)(x+1)P_3(x)P_6(x)$, where

$$P_3(x) = x^4 - x^3 + x^2 - x + 1$$

is an irreductible algebraic polynomial with 4 complex roots,

9. $x^{12} - 1 = (x-1)(x+1)(x^2+1)P_1(x)P_2(x)P_3(x)$.

If n is an odd prime, $P(x)$ is irreductible by Theorem 4.4.3. The polynomials $x^{2^k} + 1$, $k \geq 1$, are symmetric and irreductible in $\mathbb{R}$ and $x^{2n+1} + 1$ is a multiple of $x + 1$ for every $n \geq 1$.

Let $n > 2$, the polynomials $x^n + 1$ factorize according to the factorization of n, by Theorem 4.4.2

1. $x^3 + 1 = (x+1)P_1(x)$,

2. $x^5 + 1 = (x+1)P_3(x)$,

3. $x^6 + 1 = (x^2+1)P_1(x^2)$ where $P_1(x^2) = x^4 - x^2 + 1$ has 4 complex roots $(\pm\sqrt{3} \pm i)/2$, square roots of the complex roots of $P_1(x)$,

4. $x^7 + 1 = (x+1)P_5(x)$ where

$$P_5(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1,$$

5. $x^9+1=(x+1)P_1(x)P_1(x^3)$ where $P_1(x^3)=x^6-x^3+1$ is an irreductible algebraic polynomial with 6 complex roots, cubic roots of the roots of $P_1(x)$,
6. $x^{10}+1=(x^2+1)P_3(x^2)$,
7. $x^{11}+1=(x+1)P_9(x)$ where
$$P_9(x)=x^{10}-x^9+x^8-x^7+x^6-x^5+x^4-x^3+x^2-x+1,$$
8. $x^{12}+1=(x^4+1)P_1(x^4)$.

The polynomials $P_5(x)$ and $P_9(x)$ also have complex roots.

Proposition 4.4.6 *Let k be odd in $\mathbb{P}$, there is equivalence between $k \mid n$ and each following property*

1. $(x^k-1) \mid (x^n-1)$
2. $(x^k+1) \mid (x^n+1)$.

Proof. Let $n=ka$ and let $y=x^k$ then $(y-1) \mid (y^a-1)$ and $(y+1) \mid (y^a+1)$ (cf the above cases). Reversely, let $n=ka+b$, a and $b<k$ in $\mathbb{N}$, and assume that $(x^k-1) \mid (x^n-1)$ then $x^n-1=x^{ka}x^b-1$ and $(x^k-1) \mid (x^{ka}-1)$. It follows that
$$x^n-1=x^b(x^k-1)P(x)+x^b-1$$
with $P(x)$ a polynomial with coefficients in $\mathbb{Z}$, but this is contradictory to the assumption with $b<k$. The proof is the same for x^n+1. □

The polynomials $P_1, P_3, P_5, P_9, \ldots, P_{p-2}$ are irreductible algebraic polynomials, prime factors of x^p+1, for p of $\mathbb{P}$. These cases provide the rules for the factorization of all polynomials x^n-1 and x^n+1 according to the factorization of n.
Example. The polynomial $x^{15}+1$ is divided by x^3+1 and x^5+1
$$\begin{aligned} x^{15}+1 &= (x^3+1)P_3(x^3)=(x^5+1)P_1(x^5) \\ &= (x+1)(x^2-x+1)P_3(x^3) \\ &= (x+1)(x^4-x^3+x^2-x+1)P_1(x^5) \\ &= (x+1)(x^2-x+1)(x^4-x^3+x^2-x+1)\,Q(x), \\ Q(x) &= x^8+x^7-x^5-x^4-x^3+x+1. \end{aligned}$$

The polynomial $x^{12}-1$ is divided by x^2-1, x^3-1, x^4-1 and x^6-1, where $Q_6(x) = x^6-1 = Q_3(x^2) = Q_3(x)Q_3(-x)$, with $Q_3(x) = x^3-1$.

4.5 Equations with Several Variables

An equation $ax^2+by^2=1$ with a and b in $\mathbb{Z}$ has integer solutions (x,y) if and only if $\gcd(a,b)=1$ and $\gcd(x,y)=1$ in $\mathbb{Z}$, by (1.3). Lagrange (1770) proved that every equation

$$A = a_0t^n + a_1t^{n-1}y + \cdots + a_ny^n$$

where A is prime to y is equivalent to an equation

$$1 = b_0t^n + b_1t^{n-1}x + \cdots + b_nx^n$$

if there exists θ such that $a_0\theta^n + a_1\theta^{n-1} + \cdots + a_n$ is multiple of A. In that case, $\gcd(b_0,\ldots,b_n)=1$ and solutions (x,t) satisfy $\gcd(x,t)=1$. Lagrange solved explicitly the equations of the first and second degrees of this form.

The equation $ax^2+by^2=cz^2$ is the equation of an ellipse with parameters depending on z. Fermat's used geometry of elliptic curves to solve 3rd degree equations such as $x^3+y^3=pz^3$ also studied by Lagrange and in Theorem 3.4.1. Here we consider some higher degrees algebraic equations. The super-Fermat equations form a class of equations

$$ax^n + by^r = cz^s \tag{4.11}$$

with integers n,r,s larger than 2 and with integers a,b,c. They are classified according to the value of

$$\chi = \frac{1}{n} + \frac{1}{r} + \frac{1}{s},$$

the hyperbolic equations are characterized by $\chi<1$, the elliptic equations by $\chi>1$ and the euclidean equations $\chi=1$. Many hyperbolic and elliptic equations have solutions, several of them were studied in Section 2.5. In the euclidean equations, the exponents reduce to $(4,4,2)$, $(3,3,3)$, $(3,6,2)$ and their permutations. With the constants $a=b=c=1$, the euclidean cases $(3,3,3)$, $(4,4,2)$ and its permutations have no solutions. The equation

$$x^3 + y^6 = z^2$$

has solutions which are those of the equation $x^3 + y^3 = z^2$, where $y = 1$ and $(x, z) = (2, \pm 3)$ by Proposition 3.1.12.

The equation

$$x^2 + y^6 = z^3$$

has no solution with $x = 1$ by Theorem 3.3.4 about Catalan's equation. The equation $x^2 + y^3 = z^3$ has the unique solutions $(x, y, z) = (\pm 13, 7, 8)$ but 7 is not a square and the equation with exponents $(2, 6, 3)$ has no solution. These examples show that the curves are not algebraically equivalent under a permutation of the exponents.

The elliptic equations have the sets of exponents $(2, 2, k)$ with $k \geq 2$ or $(2, 3, k)$ with $k = (3, 4, 5)$.

Proposition 4.5.1 *The equation*

$$x^2 + y^2 = z^5$$

has the solution $(x, y, z) = (\pm 4, \pm 4, 2)$ *and infinitely many solutions in* $\mathbb{Z}^{*3}$ *with* z *odd with prime divisors* $p_i = 1 \pmod 4$.

Proof. If z is even, x and y are necessarily even and $(x, y, z) = (\pm 4, \pm 4, 2)$ is solution. Assuming there exist another solution, z is odd and x and y do not have the same parity. Every prime p_i is sum of two squares by Legendre's Theorem 1.2.7, their product is sum of two squares by Equation (1.5) and every z product of prime $p_i = 1 \pmod 4$ is sum of two squares. □

Proposition 4.5.2 *The equation*

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

with $k \geq 2$ *has infinitely many solutions in* $\mathbb{Z}^{*3}$ *with* z *odd with prime divisors* $p_i = 1 \pmod 4$.

The existence of solutions of the equations where x and y have even exponents depends on the value of k. The equation

$$x^2 + y^4 = z^3$$

has the even solutions $(x, y, z) = (\pm 16, \pm 4, 8)$.

Proposition 4.5.3 *Let n, p, q, k in $\mathbb{N}$ such that $np + 1 = ak$ and $np = bq$, the equation*

$$x^p + y^q = z^k$$

has the even solution $(x, y, z) = (2^n, 2^b, 2^a)$.

It applies to determine the even solutions of the equations with an odd exponents k such as $(x, y, z) = (\pm 4, \pm 2, 2)$ for the equation $x^2 + y^4 = z^5$, $(x, y, z) = (8, 8, 4)$ for the equation $x^3 + y^3 = z^5$, and $(x, y, z) = (\pm 2^5, 4, 2)$ is solution of the equation $x^2 + y^5 = z^{11}$. Obviously, $\gcd(x, y) > 1$ and they are the smallest integers solutions of these equations.

Proposition 4.5.4 *The equation*

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

has infinitely many solutions in $\mathbb{Z}^{*3}$.

Proof. Assuming that $\gcd(x, z) = 1$, $\gcd(x - z, x + z) = 1$ by the equality $y^3 = (z + x)(z - x)$, hence $x - z$ and $x + z$ are relatively prime cubes, x, z are their sum or difference. All sums or difference of cubes provide a solution (x, y, z) and there exist infinitely many solutions. □

The solutions of Proposition 4.5.4 with $\gcd(x, z) = 1$ such as $(1, 2, 3)$ or $(13, 3, 14)$ are not the unique solutions, for example we have the triples of solutions $(3, 3, 6)$, $(6, 4, 10)$, $(13, 3, 14)$, $(3, 6, 15)$, they cannot be reduced by division by a common factor of the coordinates for the equation is not homogeneous.

Proposition 4.5.5 *The equation*

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

has solutions (x, y, z) in $\mathbb{Z}^{*3}$ such that $\gcd(x, y, z) = 1$, x and z are odd, and y is even, in particular $(\pm 13, 7, 8)$ is solution.

Proof. The equation is equivalent to $x^2 = (z - y)(y^2 + yz + z^2)$ therefore $z - y$ divides x. Denoting $y = u + v$ and $z = u - v$, $y + z = 2u$ and $y - z = 2v < 0$, the equation becomes $x^2 + 2v(v^2 + 3u^2) = 0$ where $v^2 + 3u^2$ is odd because $\gcd(y - z, y^2 + yz + z^2) = 1$ in

that case. Let $x = 2a$, $2a^2 + v(v^2 + 3u^2) = 0$ which implies $v = \pm 2$ due to the parity of v^2+3u^2 but the equation $a^2 = \pm(4+3u^2)$ has an integer solution if $3u^2 = (a-2)(a+2)$. Let $d = \gcd(a-2, a+2)$, it follows that $d = \pm 2, \pm 4, \pm a$ and there is no solutions such that y and z have the same parity which allows only x and z odd and y even.

Furthermore $\gcd(x, y, z) = 1$, let $d = \gcd(z - y, y^2 + yz + z^2)$ with $z - y > 0$ then $d \mid 3yz$ and $d \mid 3(y^2 + z^2)$ therefore $d = 1$ or 3, otherwise $d \mid y$ or z and $d \mid (y^2 + z^2)$ which is contradictory to $\gcd(x, y, z) = 1$. With $d = 3$, $x = 3a$, $z - y = 3b$ and the equation becomes

$$a^2 = b(y^2 + 3yb + 3b^2)$$

where $b \mid a$ and $b \mid (y^2 + 3yb + 3b^2)$, equivalently $b \mid y$ and this is contradictory to $\gcd(x, y, z) = 1$. It follows that

$$\gcd(z - y, y^2 + yz + z^2) = 1,$$

$z - y = n^2$ and $y^2 + yz + z^2 = k^2$, with odd integers n and k such that $\gcd(k, n) = 1$ and $x = kn$. We obtain $y + z = 2y + n^2$, $yz = y^2 - yn^2$ and

$$k^2 = (y + z)^2 - yz = 3y^2 + 3yn^2 + n^4,$$

where $n \nmid 3y$ if $n > 1$. With $n = 1$, the equation reduces to $3y^2 + 3y + 1 = x^2$ and we obtain a solution with $y = 7$, $x^2 = 169$. □

Proposition 4.5.6 *The equation*

$$x^2 + y^3 = z^4$$

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

Proof. The equation with $y = 1$ has no solution, from the solutions of Catalan's equation. otherwise

$$y^3 = (z - \sqrt{x})(z + \sqrt{x})(z - i\sqrt{x})(z + i\sqrt{x})$$

the roots are distinct and the polynomials $z \pm x$ and $z \pm ix$ are irreductible in the field they generate, their product cannot be a cube. □

Propositions 3.1.7, 3.4.3, 3.1.10 and Dirichlet's Theorem are cases where (4.11) do not have non trivial integer solutions, Proposition 3.1.11 provides an example of equation

having infinitely many integer solutions. Let us assume the condition $a = b = c = 1$ in (4.11). For every integer n, the equation with $\chi > 1$ and $x = 1$ is equivalent to $z^s - y^r = 1$ and there exist solutions such as $1 + 2^3 = 3^2$ and, with $s = 1$, $1 + 2^2 = 5$ and every prime p such that $1 + 2^r = p$. Equation (4.11) with all exponents strictly larger than 2 has no solution if one of n, r and s divides the other exponents. Let $n \mid r, s$, (4.11) is equivalent to

$$x^n + (y^k)^n = (z^l)^n,$$

by Fermat's last theorem it has no solution. The equation $x^2 + y^3 = z^3$ has solutions and $x^2 + y^3 = z^4$ has no solution. More equations are studied in the last chapter.

Equation (4.11) has no solution with relatively prime x, y, z in $\mathbb{N}^*$ satisfying $x^m = a \pmod y$, $z^l = b \pmod y$ where $m \mid n$ and $l \mid s$, a and b in N^* and such that $a^{k_1} \neq b^{k_2} \pmod y$ for every $k_1, k_2 > 1$. For every triple (x, y, z) such that $\gcd(x, y, z) = 1$, the least integers $a > 1$, $b > 1$, k_1 and $k_2 > 1$ can be computed but they may be large.

Bruin (1999) established that the hyperbolic equations (4.11) without constants and with $\gcd(x, y, z) = 1$ has no solution for $(n, r, s) = (2, 4, 6)$ and its permutations and he found the unique solution of the equation for $(n, r, s) = (2, 8, 3)$. The hyperbolic equation

$$x^2 + y^4 = z^3 \tag{4.12}$$

has the solution $(x, y, z) = (\pm 16, 4, \pm 8)$ in $\mathbb{Z}^{*3}$.

Weierstrass's equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is the is reparametrized as $y^2 = b_0x^3 + b_1x^2 + b_2x + b_3$ on $\mathbb{Q}$ and it amounts to an equation $Y^2 = X^3 + c_1X + c_2$ with rational coefficients

$$\begin{aligned} c_1 &= a_4 + \frac{a_1a_3}{2} - \frac{1}{3}\Big(a_2 + \frac{a_1^2}{4}\Big), \\ c_2 &= a_6 + \frac{a_3^2}{4} - \frac{1}{3}\Big(a_2 + \frac{a_1^2}{4}\Big)\Big(a_4 + \frac{a_1a_3}{2}\Big) \end{aligned}$$

and the variables

$$X = x - \frac{b_1}{3}, \quad Y = y + \frac{a_1x}{2} + \frac{a_3}{2}.$$

The solution as a real function $Y = f(X)$ or $X = g(Y)$ is explictly known and its projection on $\mathbb{Z}$ or $\mathbb{Q}$ is often empty. At $y = x$, the equation is the intersection of a parabolic and a hyperbolic curve. There exists a single intersection point in $\mathbb{R}$, it lies on the positive axis $Y > 0$ if $c_1 + c_2 < 0$, and on the negative axis if $c_1 + c_2 > 0$.

Solving an equation

$$x^2 + ay^2 + bz^2 + cxy = n$$

depends on the representation of n as sums of squares. By Theorem 2.4.3, if $n = 1 \pmod 4$ in $\mathbb{P}$ has the form $n = n_1^2 + n_2^2$, the equation becomes $ay^2 + bz^2 + cn_1y = n_2^2$ with $x = n_1$ and it can be solved as previously. If n is a sum $n = n_1^2 + \cdots + n_4^2$, the equation becomes $ay^2 + bz^2 + cn_1y = m$ where $m = n_2^2 + \cdots + n_4^2$.

A conic is determined by an homogeneous quadratic form in $\mathbb{R}^3$

$$f(x, y, z) = a_1x^2 + b_1y^2 + c_1z^2 + 2a_2yz + 2b_2xz + 2c_2xy.$$

Cauchy studied a third degree homogeneous equation

$$ax^3 + by^3 + cz^3 = 3dxyz$$

by differential calculus. Hermite, Serret, Dirichlet proposed several method to solve algebraic equation with a prime degree, in particular methods of substitutions to deduce several solutions from a first one. Reparametrizations have also been used for the resolution of the equations.

4.6 Twin-primes

The twin-primes are the sets of numbers $p_1 < p_2$ in $\mathbb{P}$ such that p_1 and p_2 have the same distance d. With an odd distance, one of p_1 and p_2 is odd and the other one is even, so they reduce to $(2, 5)$ for $d = 3$, $(2, 7)$ for $d = 5$, $(2, 11)$ for $d = 9$, etc. With the even distances $d = 2, 4, 6, 8, 10$, the twin-primes lower than 100 are given in the next Table.

For every integer n, the prime factors of n and $n + 1$ are different since their parities differ. Let p in $\mathbb{P}$ be such that $p \mid n$ and $(p + 1) \mid (n + 1)$, for example $2 \mid 14$ and $3 \mid 15$,

Table 4.4: Twin-primes

$d = 2$	(3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73),
$d = 4$	(3,7), (7,11), (13, 17), (19, 23), (43,47), (67,71), (79,83),
$d = 6$	(5,11), (7,13), (11, 17), (13, 19), (17,23), (23,29), (31,37), (41,47),(53, 59),(67,73),(83, 89),
$d = 8$	(3,11), (5,13), (11,19),(23,31), (29,37), (53,61), (59,67), (89,97),
$d = 10$	(3,13), (13, 23), (19, 29), (31, 41), (37,47), (43,53), (61,71), (73,83) , (79,89).

$3 \mid 15$ and $4 \mid 16$, $4 \mid 24$ and $5 \mid 25$, $5 \mid 35$ and $6 \mid 36$. There exist infinitely such numbers and

$$\begin{aligned} \frac{n+1}{p+1} &= 1 \pmod p, \\ \frac{n-p}{p+1} &= 0 \pmod p. \end{aligned}$$

Let p in $\mathbb{P}$ such that $p \mid n$ and $(p+2) \mid (n+2)$, for example $2 \mid 6$ and $4 \mid 8$, $2 \mid 14$ and $4 \mid 16$, $3 \mid 33$ and $5 \mid 35$, then

$$\frac{2(n-p)}{p+2} = 0 \pmod p.$$

All integers p prime and n such that $p \mid n$ and there exists k satisfying $(p+k) \mid (n+k)$ has similar properties with the equivalence

$$\frac{k(n-p)}{p+k} = 0 \pmod p.$$

In the above examples, p and $p+k$ are twin-primes but it is not proved that for each k the properties of their prime factors occur for infinitely many n and p.

Bertrand's postulate extends to twin-primes with small values of d.

Proposition 4.6.1 *For all d and sufficiently large n, there exist twin primes p and $p+d$ in $\mathbb{P}$ in every interval $[kn, (k+1)n]$, for n sufficiently large.*

This is a consequence of Theorems 4.1.1 and 4.1.2. This is generally not true for the first pair of twin-primes. This implies the existence of infinitely many twin-primes, for every integer d.

Hardy and Littlewood' conjecture about the number $N_2(n)$ of twin-primes up to an integer n states that

$$N_2(n) = 2c_2 \int_2^n \frac{dx}{(\log x)^2}$$

with a constant

$$c_2 = \prod_{p>2, p\in\mathbb{P}} \frac{p(p-2)}{(p-1)^2}.$$

4.7 Exercises

Exercise 4.1. Find the primes of $\mathbb{Q}[\sqrt{5}]$ and $\mathbb{Q}[i\sqrt{5}]$.

Exercise 4.2. Let z be a complex prime in $\mathbb{Z}[i]$ and let a in $\mathbb{C}$ such that $\gcd(a, z) = 1$, prove that $z^{N(z)-1} = 1 \pmod{N(z)}$ if $N(z) = 1 \pmod 4$ and $z^{N^2(z)-1} = 1 \pmod{N^2(z)}$ if $N(z) = 3 \pmod 4$.

Exercise 4.3 Find all roots of the equations

$$\begin{aligned} x^2 - 2y^2 &= \pm 1, \\ x^2 - 2y^2 &= \pm 2. \end{aligned}$$

Exercise 4.4. Find the roots of the equation $x^6 = 7 \pmod 3$.

Exercise 4.5. Let p in $\mathbb{P}$, prove that the equation $y^2 = x^3 - p^2x$ has no solution.

Exercise 4.6. Find the solutions of the equation $x^2 + y^3 = z^4$.

Exercise 4.7. Find the solutions of the equation $x^2 + y^3 = z^5$.