

## Chapter 2

# Fermat's First Theorem and Quadratic Residues

### Abstract

We start with Fermat's first theorem and sufficient conditions for the primality of numbers related to this theorem. It was generalized by Euler replacing a prime integer by the function  $\varphi(n)$  of an arbitrary integer  $n$ . Fermat and Euler theorems apply to the representation of primes as sums or differences of squares or higher powers according to their value modulo 8, to the factorization of quadratic forms and to the properties of the quadratic residues. Legendre's symbol is known for their representation, it had already been most studied by Lagrange, we prove and extend their properties. Wilson's theorem provides other conditions for the representations of the primes as sums or differences of squares.



## 2.1 Fermat's First Theorem

Fermat first theorem states necessary conditions for primality of numbers. Sufficient conditions are not reciprocal to these conditions. The first one is due to Lucas (1876) and it has been generalized by Lehmer (1927), we give further extensions in this section.

**Theorem 2.1.1 (Fermat first theorem)** *For all integers  $n$  prime and  $N$  prime to  $n$*

$$N^{n-1} \equiv 1 \pmod{n}.$$

*Proof.* From the development of  $(x+1)^n$  and since  $C_n^k$  is multiple of  $n$  for every  $k$  in  $\{1, \dots, n-1\}$ ,  $n$  divides  $(x+1)^n - 1 - x^n$  for every integer  $x$ . With  $x = N-1$ , this implies

$$\begin{aligned} N^n - 1 &\equiv (N-1)^n \pmod{n}, \\ N^n - N &\equiv (N-1)^n - (N-1) \pmod{n}, \\ &\equiv (N-2)^n - (N-2) = \dots = 0 \pmod{n}, \end{aligned}$$

the result follows, with  $N$  is prime to  $n$ . □

**Corollary 2.1.2** *For every prime  $n$  and for every integer  $x < n$ ,  $x^{n-1} \equiv 1 \pmod{n}$ . Every polynomial with integral coefficients such that  $f(x) \equiv 0 \pmod{n}$  for every integer  $x < n$  is a multiple of  $x^n - x$ .*

This is a consequence of Euclid's property (1.1) and Fermat first theorem. By the factorization

$$\begin{aligned} N^k - 1 &= (N-1)(N^{k-1} + N^{k-2} + \dots + N + 1) \\ &= (N^2 - 1)(N^{k-2} - N^{k-3} + \dots - N + 1) \end{aligned}$$

for every odd integer  $k$ , we deduce the following result from Fermat's first theorem.

**Corollary 2.1.3** *For every prime  $n$ , if  $n$  does not divide  $N$ ,  $N-1$  and  $N+1$ , then*

$$N^{n-3} - N^{n-4} + \dots - N + 1 \equiv 0 \pmod{n}.$$

**Proposition 2.1.4** *For all integers  $p$  odd prime and  $a$  prime to  $p$ , if  $p \mid x^2 \pm a$  then there exist  $s$  and  $t$  such that  $p = s^2 \pm at^2$ .*

Proof. From Theorem (2.1.1),  $p \mid x^2 \pm ay^2$  with  $y = a^{\frac{p-1}{2}}$  and, from Theorem (1.2.9), there exist  $s$  and  $t$  such that  $p = s^2 \pm at^2$ .  $\square$

**Corollary 2.1.5** *There are infinitely many Mersenne numbers  $M_m = 2^m - 1$  that do not belong to  $\mathbb{P}$ .*

In particular, for every  $m$  such that  $m + 1$  is prime,  $m + 1 \mid M_m$ .

**Proposition 2.1.6** *Let  $p$  be an odd prime such that  $p \mid x^2 - ay^2$  with  $a$  an integer and  $\gcd(x, y, p) = 1$ , this is equivalent to  $a^{\frac{p-1}{2}} = 1 \pmod{p}$ .*

Proof. By Theorem 2.1.1

$$(ay^2 - x^2)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} y^{p-1} - x^{p-1} \pmod{p} = a^{\frac{p-1}{2}} - 1 \pmod{p}$$

and  $ay^2 - x^2 = 0 \pmod{p}$ .  $\square$

**Corollary 2.1.7** *Let  $p$  be an odd prime and let  $a$  be an integer, for all integers  $x$  and  $y$  such that  $p \nmid x^2 - ay^2$  and  $\gcd(x, y, p) = 1$*

$$\begin{aligned} (x + a^{\frac{1}{2}}y)^{p+1} &= (x - a^{\frac{1}{2}}y)^{p+1} \pmod{p}, \\ \frac{(x + a^{\frac{1}{2}}y)^{p+2} - (x - a^{\frac{1}{2}}y)^{p+2}}{2a^{\frac{1}{2}}y} &\not\equiv 0 \pmod{p}. \end{aligned}$$

Proof. By Theorem 2.1.1, Proposition 2.1.6 and since  $p$  is odd, we have

$$\begin{aligned} (x + a^{\frac{1}{2}}y)^p &= x + a^{\frac{p}{2}}y \pmod{p} = x - a^{\frac{1}{2}}y \pmod{p}, \\ (x + a^{\frac{1}{2}}y)^{p+1} &= x^2 - ay^2 \pmod{p}, \\ (x - a^{\frac{1}{2}}y)^p &= x - a^{\frac{p}{2}}y \pmod{p} = x + a^{\frac{1}{2}}y \pmod{p}, \\ (x - a^{\frac{1}{2}}y)^{p+1} &= x^2 - ay^2 \pmod{p} \end{aligned}$$

and the result is obtained as the difference of  $(x^2 - ay^2)(x + a^{\frac{1}{2}}y)$  and  $(x^2 - ay^2)(x - a^{\frac{1}{2}}y)$ , the ratio of the corollary is  $x^2 - ay^2$ .  $\square$

The next sufficient conditions for primality of numbers are more restrictive than Lucas's conditions (1878) where  $N$  is not supposed to be prime. The smallest value  $n$  satisfying  $N^{n-1} = 1 \pmod{n}$  may be large if  $N$  is even.

**Proposition 2.1.8** *For every prime  $N$ , let  $n > N$  be the smallest integer such that  $N^{n-1} = 1 \pmod{n}$ , then  $n$  is prime.*

Proof. If  $n$  were not prime, let  $p \mid n$ ,  $p$  prime, there exist integers  $k \geq 1$  and  $m$  such that  $n = kp$  and  $N^{kp-1} = 1 + mkp$ . If  $k > 1$

$$\begin{aligned} N^{k(p-1)} N^{k-1} &= N^{k-1} \pmod{p}, \\ N^{kp-1} &= 1 \pmod{p} \end{aligned}$$

therefore  $N^{k-1} = 1 \pmod{p}$ , this is contradictory to  $k < n$  so  $n = p$ , it is prime.  $\square$

The smallest  $n$  such that  $a^{n-1} = 1 \pmod{n}$  with  $a = 2$  is 3, it is 5 with  $a = 3$ , it is 7 with  $a = 5$ , it is 11 with  $a = 7$ , etc. There are infinitely many composite integers  $n$  satisfying the other conditions of Fermat's first theorem 2.1.1.

**Theorem 2.1.9 (Lucas-Lehmer)** *For every integer  $N > 1$ , let  $n > N$  be an integer such that  $N^{n-1} = 1 \pmod{n}$  and  $N^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$  for every prime factor  $p$  of  $n-1$ , then  $n$  is prime.*

Proof. Let  $m$  be the smallest integer such that  $N^m = 1 \pmod{n}$ , it is written as  $N^m = kn + 1$  with an integer  $k \geq 1$ . If  $m$  did not divide  $n-1$ , there exist  $a$  in  $\{1, \dots, m-1\}$  such that  $1 = N^{n-1} = N^a \pmod{n}$ . This is impossible since  $a < m$  therefore  $m \mid n-1$ . Let

$$n-1 = \prod_{i=1}^I p_i^{a_i} = p_i m_i, \quad i = 1, \dots, I$$

the property  $m \mid n-1$  implies  $m = \prod_{i=1}^I p_i^{b_i}$  with  $0 \leq b_i \leq a_i$ . By assumption,  $m$  does not divide  $m_i$  therefore  $b_i > a_i - 1$  for every  $i = 1, \dots, I$ , hence  $m \geq n-1$  and  $m = n-1$ . The result follows from Lucas's Theorem or from Proposition 2.1.8 if  $N$  is an odd prime.  $\square$

## 2.2 Divisors of an Integer

The representation of an integer  $n$  as a sum or a difference of squares is a consequence of Fermat's first theorem 2.1.1 and Theorem 1.2.7. It depends on the value of  $n$  modulo 8. Most results in this domain have been published without proof in Fermat's letters and later by Euler and Lagrange. They are proved in this section from Legendre's Theorem 1.2.7 and Theorems 1.2.8 and 1.2.9.

**Theorem 2.2.1** *For every  $n \equiv 1 \pmod{8}$  in  $\mathbb{P}$ , there exist  $a$  and  $b$  in  $\mathbb{N}$  such that  $n = a^2 \pm 2b^2$  or  $n = a^2 \pm b^2$ .*

*Proof.* For every  $n \equiv 1 \pmod{8}$  prime and for every  $x$  prime to  $n$ , there exists  $k$  in  $\mathbb{N}$  such that  $x^{8k} \equiv 1 \pmod{n}$ , by Fermat first theorem. Then  $(x^{4k} - 1)(x^{4k} + 1) \equiv 0 \pmod{n}$  implies  $(x^{2k} - 1)(x^{2k} + 1) \equiv 0 \pmod{n}$  or

$$x^{4k} + 1 = (x^{2k} + 1)^2 - 2x^{2k} = (x^{2k} + 1)^2 + 2x^{2k} \equiv 0 \pmod{n}$$

and from Theorem 1.2.7, the prime factors of  $x^{2k} + 1$  and  $x^{4k} + 1$  have the form  $a^2 + b^2$ , the prime factors of  $x^{4k} - 1 = (x^{2k} + 1)(x^{2k} - 1)$  have the form  $a^2 \pm b^2$ . In each case, the prime factors of  $n$  are prime factors of  $x^{8k} - 1$ .  $\square$

For example  $n = 73$  is the sum or difference of two squares  $n = 37^2 - 36^2$  and  $n = 3^2 + 8^2$ . There is not unicity, it is also written as  $n = 1 + 2 \cdot 6^2$  and  $n = 35^2 - 2 \cdot 24^2$ .

**Theorem 2.2.2** *Every prime number  $n \equiv 3 \pmod{8}$  has the form  $a^2 - b^2$  with integers  $a$  and  $b$ .*

*Proof.* For every  $x$  prime to  $n$ ,  $x^{n-1} - 1 = x^{8k+2} - 1 \equiv 0 \pmod{n}$  and Theorem 1.2.7 applies.  $\square$

For example  $3 = 2^2 - 1$ ,  $11 = 6^2 - 5^2$ ,  $19 = 10^2 - 9^2$ ,  $51 = 10^2 - 7^2$ . This representation is not unique, some prime integers  $n \equiv 3 \pmod{8}$  have also the form  $a^2 + 3b^2$ ,  $43 = 4^2 + 3 \cdot 3^2$ ,  $67 = 8^2 + 3$ ,  $163 = 4^2 + 3 \cdot 7^2$ .

**Theorem 2.2.3** *Every prime number  $n \equiv 5 \pmod{8}$  is written as  $a^2 \pm b^2$  with integers  $a$  and  $b$ .*

Proof. For every  $x$  prime to  $n$ ,  $x^{n-1} - 1 = (x^{4k+2} - 1)(x^{4k+2} + 1) = 0 \pmod{n}$ , the result is a consequence of Theorem 1.2.7.  $\square$

**Theorem 2.2.4** Every prime number  $n = 7 \pmod{8}$  is written as  $a^2 - b^2$  with integers  $a$  and  $b$ .

Proof. For every  $x$  prime to  $n$ ,  $x^{n-1} - 1 = x^{6+8k} - 1 = 0 \pmod{n}$ , this is a difference of two squares and  $n$  has the same form as a prime factors of  $x^{n-1} - 1$ , by Theorem 1.2.7.  $\square$

For example  $7 = 4^2 - 3^2$ ,  $39 = 8^2 - 5^2$ . Lagrange established other results according to the congruence of  $n$  with respect to different values of  $p$ .

Theorems 2.2.1-2.2.4 extend to every prime factor of a multiple  $n$  of  $2^\alpha$ ,  $\alpha \geq 2$ .

**Proposition 2.2.5** The prime factors of  $n = 1 + 12k$  and  $n = 5 + 12k$  with  $k$  odd are written as  $a^2 \pm b^2$  with integers  $a$  and  $b$ . The prime factors of  $n = \pm 3 + 12k$ ,  $n = 7 + 12k$  and  $n = -1 + 12k$  with  $k$  odd have the form  $a^2 - b^2$ .

**Proposition 2.2.6** Every prime number  $n = 1 \pmod{6}$  has the form  $a^2 - b^2$  or  $a^2 + 3b^2$  with integers  $a$  and  $b$ .

Proof. Let  $n = 1 + 6k$ , for every  $x$  such that  $\gcd(x, n) = 1$   $x^{6k} - 1 = 0 \pmod{n}$  is equivalent to  $x^{2k} - 1 = 0 \pmod{n}$  or  $(x^{2k} - 1)^2 + 3x^{2k} = 0 \pmod{n}$  and the result is a consequence of Theorem 1.2.9.  $\square$

**Proposition 2.2.7** The product of prime numbers  $3 \pmod{4}$  ending with 3 or 7 has the form  $a^2 + 5b^2$  with integers  $a$  and  $b$ .

Proof. The number of this form are written  $20n + 3$  or  $20n + 7$  and their product is  $21 \pmod{4} = 5 \pmod{4}$ , then Theorem 1.2.8 applies.  $\square$

Tables of the divisors of number according to their modulo have been established and many other results of the same kind can be established (Lagrange).

The product of two integers  $n = ax^2 + bxy + cy^2$  and  $m = ux^2 + vxy + wy^2$  where  $av + bu = 0$  and  $bw + cv = 0$  satisfies

$$unm = a(ux^2 + wy^2)^2.$$

If  $\gcd(a, b) = 1$ ,  $a \mid u$  and  $b \mid v$ , then  $c \mid w$ ,  $u = ak$  and  $v = -bk$ , the equality is equivalent to

$$k(ax^2 - cy^2)^2 = nm$$

where  $k \mid \gcd(u, v, w)$  so that  $k \mid m$ . Either  $n$  and  $k^{-1}m$  are equal to  $ax^2 - cy^2$  or  $n = X^2$  and  $m = kY^2$  such that  $ux^2 + wy^2 = XY$ , with  $am = uY^2$ . If  $u \mid a$ , the equation is similar.

If  $a \mid n$ , then  $un'm = (ux^2 + wy^2)^2$  and  $n = aX^2$ ,  $um = Y^2$  such that  $ux^2 + wy^2 = XY$ . The possible cases are

$$u'n = a'X^2, \quad u''m = a''Y^2$$

with  $ux^2 + wy^2 = XY$ ,  $a = a'a''$  and  $u = u'u''$ , or

$$u = Z^2, \quad n = a'X^2, \quad m = a''Y^2$$

with  $ux^2 + wy^2 = XYZ$  and  $a = a'a''$ .

The particular cases  $n \mid m$  and  $m \mid n$  are included in the above factorizations. Finally, an integer such as  $n$  and  $m$  may divide a quadratic form  $x^2 + wy^2$ .

More generally, let  $n = py^2 + 2qyz + rz^2$  and  $m = p'y'^2 + 2q'y'z' + r'z'^2$  with  $\gcd(a, b) = 1$ , and let  $x = py + qz$  and  $x' = p'y' + q'z'$ , then

$$pn = x^2 + az^2, \quad p'm = x'^2 + a'z'^2.$$

Legendre proved that  $pp'nm$  has the form

$$\begin{aligned} pp'nm &= (xx' \pm azz')^2 + a(xz' \mp x'z)^2, \\ &= (pp'Y + \phi Z)^2 + aZ^2, \\ &= pp'Y^2 + 2\phi YZ + \psi Z^2, \end{aligned}$$

where  $\phi$  and  $\psi$  are not multiple of  $pp'$ . This quadratic form generalizes the previous case.

## 2.3 Quadratic Residues

Let  $p > 1$  be an odd prime, an integer  $a$  is a quadratic residue  $(\text{mod } p)$  if there exists an integer  $x$  such that  $a = x^2 \pmod{p}$ . From Fermat's first theorem,  $a^{\frac{p-1}{2}} = 1$  if  $p \nmid a$ .



For all integers  $n > 2$  prime and  $N$ , Legendre defined the symbol

$$\left(\frac{N}{n}\right) = N^{\frac{n-1}{2}} \pmod{n}$$

as the remainder of the division of  $N^{\frac{n-1}{2}}$  by  $n$ . If  $n \mid N$ ,  $\left(\frac{N}{n}\right) = 0$ .

The next properties follow straightforwardly from the definition of Legendre's symbol.

**Theorem 2.3.1** *For all integers  $M$  and  $N$*

$$\left(\frac{MN}{n}\right) = \left(\frac{M}{n}\right)\left(\frac{N}{n}\right) \quad (2.1)$$

Let  $N$  factors as a product of primes  $N = \prod_{i=1}^I p_i^{\alpha_i}$ , then

$$\left(\frac{N}{n}\right) = \prod_{i=1}^I \left(\frac{p_i}{n}\right)^{\alpha_i}.$$

Moreover  $\left(\frac{1}{n}\right) = 1$  and

$$\left(\frac{-N}{n}\right) = (-1)^{\frac{n-1}{2}} \left(\frac{N}{n}\right) = \begin{cases} \left(\frac{N}{n}\right) & \text{if } n \equiv 1 \pmod{4}, \\ -\left(\frac{N}{n}\right) & \text{if } n \equiv 3 \pmod{4}. \end{cases} \quad (2.2)$$

In particular

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv 3 \pmod{4}. \end{cases}$$

From Fermat's first theorem, for every  $N > 0$  prime to  $n$ , with  $n$  prime,

$$N^{n-1} - 1 = (N^{\frac{n-1}{2}} - 1)(N^{\frac{n-1}{2}} + 1) \equiv 0 \pmod{n}$$

implies

$$\left(\frac{N}{n}\right) = \pm 1 \pmod{n}.$$

and it is zero if  $N$  is not prime to  $n$ . If  $N$  is a quadratic residue modulo  $n$

$$\left(\frac{N}{n}\right) = 1$$

otherwise and if  $N$  is prime to  $n$

$$\left(\frac{N}{n}\right) = -1.$$

In other words for every  $n$  prime and for every  $N$  prime to  $n$ , the property (2.1) entails

1. if  $n$  divides  $x^2 - Ny^2$  and  $x^2 - My^2$ , it divides  $x^2 - MNy^2$ ,
2. if  $n$  that divides  $x^2 + Ny^2$  and  $x^2 + My^2$ , it divides  $x^2 + MNy^2$ .

Let  $F_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$  for an odd prime integer  $p$ ,  $z^{p-1} = 1$  for every  $z$  of  $F_p^*$ . For every  $p$  in  $\mathbb{P}$ , the unique solutions to the equality  $x^2 = 1$  are the units  $\pm 1$  of  $F_p$  and  $(-1)^2 = (p-1)^2 = 1 \pmod{p}$ .

By Theorem 2.1.1, the equation  $x^2 + 1 = 0 \pmod{p}$  has an integer solution if and only if  $p = 2$ , then the solutions are solutions of  $x^2 = 1 \pmod{p}$ , or  $\left(\frac{-1}{p}\right) = 1$  which is equivalent to  $p = 1 \pmod{4}$ .

For every prime  $p > 2$ , the field  $F_p$  is generated by a single element  $\omega > 1$  of  $\{0, 1, \dots, p-1\}$

$$F_n = \{0, \omega, \omega^2, \dots, \omega^{n-1}\}.$$

*Example.* The field  $F_5$  is generated by  $\omega = 2$  such that  $\omega^2 = 4$ ,  $\omega^3 \equiv 3$  and  $\omega^4 \equiv 1$ , the squares of  $F_5$  are 1 and 4.

*Example.* The field  $F_7$  is generated by  $\omega = 3$  such that  $\omega^2 \equiv 2$ ,  $\omega^3 \equiv 6$ ,  $\omega^4 \equiv 4$ ,  $\omega^5 \equiv 5$ ,  $\omega^6 \equiv 1$ , the squares of  $F_7$  are 1, 2 and 4.

Every element  $x = \omega^k$  of  $F_p$ ,  $1 < k < p$ , has an inverse  $x'$  in  $F_p$  such that  $xx' = 1$

$$x' = x^{-1}\omega^{p-1} = \omega^{p-k-1},$$

where  $\omega$  generates  $F_p$ . It has also an inverse  $x''$  in  $F_p$  such that  $xx'' = -1$

$$x' = \omega^{p-k-1}(p-1).$$

In  $F_5$ ,  $1.4 = -1$  and  $2.3 = 1$ , in  $F_{11}$ ,  $10 = -1$ ,  $2.5 = -1$ ,  $3.7 = -1$ ,  $4.8 = -1$  and  $6.9 = -1$ .

Let  $p \equiv 1 \pmod{8}$ , from Theorem 2.2.1, there exist integers  $a$  and  $b$  such that  $2b^2 \equiv a^2 \pmod{p}$  therefore

$$\left(\frac{2}{p}\right)b^{p-1} \equiv a^{p-1} \pmod{p}$$

where  $b^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p}$ .

**Theorem 2.3.2 (Fermat)** *Let  $p$  be odd in  $\mathbb{P}$*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}, \\ \pm 1 & \text{if } p \equiv \pm 1 \pmod{4}. \end{cases}$$

Proof. Let  $\omega$  be the generator of the solutions of the equation  $x^8 - 1 = 0$  in  $F_p$  which is solution of  $x^4 + 1 = 0$ , and let  $y = \omega + \omega^{-1}$ . In  $F_p$ ,  $y^2 = 2$  and  $y^p = \omega^p + \omega^{-p} = y2^{\frac{p-1}{2}}$ . With  $p \equiv 1 \pmod{8}$ ,  $y^{p-1} = y^{8k} = 1$ . With  $p \equiv -1 \pmod{8}$ ,  $y^p = \omega^p + \omega^{-p}$  due to the symmetry of  $y$  in  $\omega$  and  $\omega^{-1}$  therefore  $y^{p-1} = 1$  as in the previous case and  $\left(\frac{2}{p}\right) = 1$ . With  $p \equiv 5 \pmod{8}$

$$\begin{aligned} \omega^p &= \omega\omega^4 \pmod{p} \\ &= -\omega \pmod{p}, \\ \omega^{-p} &= \omega^{-1}\omega^{-4} \pmod{p} \\ &= -\omega^{-1} \pmod{p} \end{aligned}$$

and  $\left(\frac{2}{p}\right) = -1$ , the result is the same with  $p \equiv 5 \pmod{8}$ . □

**Theorem 2.3.3 (Fermat)** *Let  $p$  be odd in  $\mathbb{P}$*

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}, \\ 0 & \text{if } p \equiv \pm 3 \pmod{12}. \end{cases}$$

Proof. The theorem is true for  $p_0 \equiv \pm 1, \pm 3, \pm 5$ . Let  $p_k = p_0 + 12k$ ,  $k > 1$ . The result is true for  $p_k$

$$\begin{aligned} \left(\frac{3}{p_k}\right) &= (-1)^{\frac{p_k-1}{2}} \left(\frac{p_k}{3}\right) = (-1)^{\frac{p_k-1}{2}} \left(\frac{p_0}{3}\right), \\ &= (-1)^{p_0-1+6(k)} \left(\frac{3}{p_0}\right) = \left(\frac{3}{p_0}\right). \end{aligned}$$

□

**Theorem 2.3.4 (Quadratic reciprocity theorem)** *For all odd  $p$  and  $q \neq p$  in  $\mathbb{P}$*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = 1.$$

**Proof.** Let  $\omega$  be a root of  $x^q - 1$  on  $F_p$ . The roots  $\omega^2, \dots, \omega^q$  belong to an extension  $K = F_p(\omega)$  of  $F_p$  and  $\omega^q = 1$ . Let

$$y = \left(\frac{1}{q}\right)\omega + \left(\frac{2}{q}\right)\omega^2 + \dots + \left(\frac{q-1}{q}\right)\omega^{q-1},$$

then we have

$$y^2 = \sum_{x, x' \in F_q^*} \left(\frac{xx'}{q}\right)\omega^{x+x'} = \sum_{x \in F_q^*, t=x+x' \in F_q^*} \left(\frac{x(t-x)}{q}\right)\omega^t.$$

Denoting  $C_t$  the coefficient of  $\omega^t$  and by (2.2)

$$\begin{aligned} C_0 &= \left(\frac{-x^2}{q}\right) = (-1)^{\frac{q-1}{2}} = q(-1)^{\frac{q-1}{2}}, \\ C_t &= \sum_{x \in F_q^*} \left(\frac{-x^2(1-\frac{t}{x})}{q}\right) = \sum_{x \in F_q^*} (-1)^{\frac{q-1}{2}} \left(\frac{1-\frac{t}{x}}{q}\right), \quad t \neq 0, \end{aligned}$$

let  $x^*$  be the inverse of  $x$  in  $F_q^*$ , then  $z = 1 - \frac{t}{x} = 1 - tx^*$  belongs to the field  $F_q$  and  $z \neq 0$  for all distinct  $x$  and  $t$  in  $F_q^*$ . Furthermore, for all distinct  $x$  and  $x'$  in  $F_q^*$ ,  $1 - \frac{t}{x}$  and  $1 - \frac{t}{x'}$  are distinct. It follows that for every  $t$  in  $F_q^*$

$$C_t = (-1)^{\frac{q-1}{2}} \sum_{z \in F_q^*} \left(\frac{z}{q}\right) = (-1)^{\frac{q-1}{2}} \sum_{k \in F_q^*} \omega^{\frac{k(q-1)}{2}}.$$

Since  $\omega^q = 1$ ,  $\omega^{\frac{q-1}{2}} = \pm 1$  so that  $\omega^{\frac{k(q-1)}{2}} = 1$  if  $k$  is even and  $\omega^{\frac{k(q-1)}{2}} = -1$  if  $k$  is odd, hence

$$\sum_{k \in F_q^*} \left(\frac{\omega^k}{q}\right) = 0$$

and

$$y^2 = C_0 = q(-1)^{\frac{q-1}{2}}. \quad (2.3)$$

By the same arguments and since  $(a + b)^p = a^p + b^p$  in  $F_q^* = F_p(\omega)$ , we have

$$y^p = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right)^p \omega^{kp} = \sum_{k \in F_q^*} \left(\frac{k}{q}\right) \omega^{kp}.$$

It follows that

$$\left(\frac{p}{q}\right) y^p = \sum_{k \in F_q^*} \left(\frac{kp}{q}\right) \omega^{kp} = y$$

since  $F_q^* = \{kp, k \in F_q^*\}$ , therefore  $\left(\frac{p}{q}\right) y^{p-1} = 1$ . Finally, by (2.3)

$$\begin{aligned} y^{p-1} &= \left(y^2\right)^{\frac{p-1}{2}} = q^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}} \\ &= \left(\frac{q}{p}\right) (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}}. \end{aligned}$$

□

By Theorem 2.3.4

$$\left(\frac{-p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q+1}{2}} \left(\frac{p}{q}\right) \quad (2.4)$$

and

$$\left(\frac{k}{p_1 \cdots p_j}\right) = \left(\frac{k}{p_1}\right) \cdots \left(\frac{k}{p_j}\right).$$

Theorem 2.3.4 applies to the calculus of  $\left(\frac{a}{n}\right)$  for composite integers  $a$  and  $n$ . Let  $a > n$ , there exists  $b < n$  such that  $a = b \pmod{n}$  by the euclidean division of  $a$  by  $n$ , then

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

and by the reciprocity formula of Theorem 2.3.4, we have to calculate

$$\left(\frac{n}{b}\right) = \left(\frac{c}{b}\right)$$

where  $n = c \pmod{b}$ . This algorithm by descent is used iteratively for large integers  $a$  and  $n$  until  $\left(\frac{p_1}{p_2}\right)$  with  $p_1$  and  $p_2$  in  $\mathbb{P}$ .

The proof of Theorem 2.3.3 in  $F_p$  generalizes to higher prime integers, for example we have

$$\begin{aligned} \left(\frac{5}{3}\right) &= -1, & \left(\frac{5}{17}\right) &= -1, & \left(\frac{5}{7}\right) &= -1, & \left(\frac{5}{13}\right) &= -1, \\ \left(\frac{5}{9}\right) &= 1, & \left(\frac{5}{11}\right) &= 1, & \left(\frac{5}{19}\right) &= 1. \end{aligned}$$

**Theorem 2.3.5** *Let  $p$  be odd in  $\mathbb{P}$*

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{10}, \\ 0 & \text{if } p \equiv \pm 5 \pmod{10}. \end{cases}$$

**Proof.** This is true for 1, 3, 5, 7, 9, 11. Let  $p_0 = \pm 1, \pm 3, \pm 5$  and  $p_k = p_0 + 10k$ ,  $k \geq 1$ , for every  $k$  in  $\mathbb{Z}^*$ . By the quadratic reciprocity Theorem 2.3.4, we have

$$\left(\frac{5}{p_k}\right) = \left(\frac{p_k}{5}\right) = \left(\frac{p_0}{5}\right) = \left(\frac{5}{p_0}\right).$$

□

For  $n \equiv 1 \pmod{4}$  in  $\mathbb{P}$  and for every  $p$  in  $\mathbb{P}$ ,

$$\left(\frac{n}{p}\right) = \left(\frac{p}{n}\right) = \left(\frac{-p}{n}\right).$$

These rules apply to  $p = 13$  to prove the next results by the same arguments as for Theorem 2.3.5.

**Theorem 2.3.6** *Let  $p$  be odd in  $\mathbb{P}$*

$$\left(\frac{13}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 3, \pm 9 \pmod{26}, \\ -1 & \text{if } p \equiv \pm 5, \pm 7, \pm 11 \pmod{26}, \\ 0 & \text{if } p \equiv \pm 13 \pmod{26}. \end{cases}$$

**Proof.** The theorem is true for  $p_0 = \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 13$ , we have to show it is valid for  $p_k = \pm 1 + 26k, \pm 3 + 26k, \pm 5 + 26k$ ,  $k > 1$

$$\left(\frac{13}{p_k}\right) = \left(\frac{p_k}{13}\right) = \left(\frac{p_0}{13}\right).$$

□

For  $n \equiv 3 \pmod{4}$  in  $\mathbb{P}$  and for every  $n$  in  $\mathbb{P}$

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

**Theorem 2.3.7** *Let  $p$  be odd in  $\mathbb{P}$*

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{if } p = \pm 1, \pm 3, \pm 9 \pmod{28}, \\ -1 & \text{if } p = \pm 5, \pm 11, \pm 13 \pmod{28}, \\ 0 & \text{if } p = \pm 7 \pmod{28}. \end{cases}$$

**Proof.** The theorem is true for  $p_0 = \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 13$ . For every  $k$  in  $\mathbb{Z}^*$ , let  $p_k = \pm 1 + 12k, \pm 3 + 12k, \pm 5 + 12k = p_0 + 12k$

$$\begin{aligned} \left(\frac{7}{p_k}\right) &= (-1)^{\frac{p_k-1}{2}} \left(\frac{p_k}{7}\right) = (-1)^{\frac{p_k-1}{2}} \left(\frac{p_0}{7}\right), \\ &= (-1)^{p_0-1+6(k)} \left(\frac{7}{p_0}\right) = \left(\frac{7}{p_0}\right). \end{aligned}$$

□

**Theorem 2.3.8** *Let  $p_1$  and  $p_2$  be odd in  $\mathbb{P}$*

$$\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{-p_2}\right) = \pm 1 \pmod{2kp_1}$$

*with  $k = 1$  if  $p_1 = 1 \pmod{4}$  or  $k = 2$  if  $p_1 = 3 \pmod{4}$ . In particular  $\left(\frac{p_1}{p_2}\right) = 1$  if  $p_2 = \pm 1 \pmod{2kp_1}$ , for every  $p_1 > 3$ .*

**Proof.** The proof of the first part is similar to the proofs of Theorems 2.3.6-2.3.7. If  $p_1 = 1 \pmod{4} > 1$  and  $p_2$  is free-square

$$\left(\frac{p_1}{p_2}\right) = \begin{cases} \left(\frac{p_2}{p_1}\right) & = 1, \text{ if } p_2 = 1, \\ \left(\frac{-p_2}{p_1}\right) & = 1, \text{ if } p_2 = -1, \end{cases}$$

if  $p_1 = 3 \pmod{4} > 3$ , let  $p_1 = 3 + 4k$  with  $k = \pm 1 \pmod{3}$  prime

$$\left(\frac{p_1}{p_2}\right) = \begin{cases} \left(\frac{p_2}{p_1}\right) & = 1, \text{ if } p_2 = 1, \\ -\left(\frac{-1}{p_1}\right) & = 1, \text{ if } p_2 = -1, \end{cases}$$

these results extend to  $p_2 = \pm 1 \pmod{2kp_1}$ ,  $k = 1$  or  $k = 2$ , according to  $p_1$ . □

Theorems 2.3.2-2.3.7 and Fermat's first theorem are used to determine the square roots of the quadratic residues modulo  $p$  according to the value of  $p \pmod{4}$  or  $\pmod{8}$ , for  $p$  odd in  $\mathbb{P}$ .

Let  $p = 3 \pmod{4}$  and, for every  $a$  prime to  $p$ , let  $x = a^{\frac{p+1}{4}} \pmod{p}$  then

$$x^2 = a^{\frac{p+1}{2}} = a \cdot \left(\frac{a}{p}\right) = \pm a \pmod{p}.$$

If  $p = 1 \pmod{4}$ , every  $a$  prime to  $p$  is a quadratic residue  $\pmod{p}$  and  $x^2 = a \pmod{p}$ . Smaller solutions  $\pmod{p}$  exist if  $p = 5 \pmod{8}$ , then

$$a^{\frac{p-1}{4}} = \pm 1 \pmod{p}$$

$$x = \begin{cases} a^{\frac{p+3}{8}} \pmod{p} & \text{if } a^{\frac{p-1}{4}} = 1 \pmod{p}, \\ \left(2^{\frac{p-1}{2}} a^{\frac{p+3}{4}}\right)^{\frac{1}{2}} \pmod{p} & \text{if } a^{\frac{p-1}{4}} = -1 \pmod{p}. \end{cases}$$

Let  $p = 1 \pmod{8}$  then  $a^{\frac{p+3}{4}} = 1 \pmod{p}$  for every  $a$  prime to  $p$  and

$$x = a^{\frac{p-1}{8}} \pmod{p}$$

is a solution. There exist smaller solutions if  $p-1 = 2^k r$  with  $r$  odd so that  $2^{-(k-1)}(p-1) = 2r$  is even and  $a^{2r} = 1 \pmod{p}$ , we have the solution

$$x = a^{2^{-k}(p-1)+\frac{1}{2}}.$$

**Proposition 2.3.9** *Let  $p$  be odd in  $\mathbb{P}$  and let  $a$  be prime to  $p$ . If  $a^{\frac{p-1}{2}} = 1$ , the equation  $x^2 - a = 0 \pmod{p}$  has the solutions  $x = \pm a^{\frac{p+1}{2}}$ . If  $\left(\frac{a}{p}\right) = -1$ , the equation  $x^2 + a = 0 \pmod{p}$  has the solution  $x = \pm a^{\frac{p+1}{4}}$ .*

*Proof.* With  $a$  be prime to  $p$ ,  $x$  is also prime to  $p$  and  $x^{p-1} = 1 \pmod{p}$ . In the first case,  $x = \pm a^{\frac{p-1}{2}}$  is obviously solution. In the second case, let  $x = a^{\frac{p+1}{4}}$

$$x^2 + a = a(a^{\frac{p-1}{2}} + 1) \pmod{p}.$$

□

The question of finding the cubic and biquadratic residues  $\pmod{p}$ , for  $p$  prime, is similar.

**Proposition 2.3.10** *Let  $p$  be odd in  $\mathbb{P}$  such that  $p = 2 \pmod{3}$  and let  $a$  be prime to  $p$ . The equation  $x^3 = a \pmod{p}$  has the solution  $x = a^{\frac{p+1}{3}}$  and, if  $\left(\frac{a}{p}\right) = -1$ , it has the solution  $x = \pm a^{\frac{p+1}{6}}$ . Let  $p = 3 \pmod{4}$  in  $\mathbb{P}$  and let  $a$  be prime to  $p$  be such that  $\left(\frac{a}{p}\right) = -1$ , then  $x = \pm a^{\frac{p+1}{8}}$  is solution of the equation  $x^4 = a \pmod{p}$ .*



**Theorem 2.3.11 (Legendre)** *Necessary conditions for  $p$  prime to divide  $x^n + 1$  are  $p = 2kn + 1$  where  $k$  is an integer, or  $p$  divides  $x^m + 1$  where  $m \mid p$  and  $m^{-1}p$  is an odd integer.*

The proof relies on the euclidean division of  $p$  by  $2n$  and Theorem 1.1.1 for  $p$  and for the remainder term of the division. As consequences

If  $n$  is an odd prime and  $p$  prime divides  $x^n + 1$ , then it divides  $x + 1$  or  $p = 2kn + 1$ .

If  $n = 2^a$  and  $p$  prime divides  $x^n + 1$ , then  $p = 2kn + 1$ .

If  $n = 2^a \nu$  and  $p$  prime divides  $x^n + 1$ , then  $p = 2^{a+1}k + 1$ .

If  $n = \mu\nu$  with  $\mu$  and  $\nu$  odd primes and  $p$  prime divides  $x^n + 1$ , then  $p$  divides  $x + 1$  or  $p = 2\mu k + 1$  or  $p = 2\nu k + 1$ .

**Theorem 2.3.12 (Legendre)** *Necessary conditions for  $p$  prime to divide  $x^n - 1$  are  $p = kn + 1$  with  $k$  integer, or  $p$  divides  $x^m - 1$  where  $m \mid p$ .*

It is proved using the euclidean division of  $p$  by  $n$  and Theorem 1.1.1. It follows that

If  $n$  is prime and  $p$  is an odd prime that divides  $x^n - 1$ , then it divides  $x - 1$  or  $p = 2kn + 1$ .

If  $n = \mu\nu$  with  $\mu$  and  $\nu$  odd primes and  $p$  prime divides  $x^n - 1$ , then  $p = 2nk + 1$  or  $p = 2\mu k + 1$  or  $p = 2\nu k + 1$ .

If  $n = 2^a$  and  $p$  prime divides  $x^n - 1$ , then  $p = kn + 1$  or  $p = k2^{-m}n + 1$ , with  $m = 1, \dots, a - 1$ .

*Example.* The equation

$$x^2 + 1 = 0 \pmod{p}$$

has the solutions  $x = 2$  and  $3$  in  $F_5$ , and  $x = 5$  in  $F_{13}$ ,

$$x^3 + 1 = 0 \pmod{p}$$

has the solutions  $x = 4$  in  $F_5$ ,  $x = 3, 5, 6$  in  $F_7$ , and  $x = 4, 10, 12$  in  $F_{13}$ ,

$$x^5 + 1 = 0 \pmod{p}$$

has the solutions  $x = 4$  in  $F_5$ ,  $x = 2, 6, 7, 8, 10$  in  $F_{11}$ , and  $x = 12$  in  $F_{13}$ ,

$$x^6 + 1 = 0 \pmod{p}$$

has the solutions  $x = 2, 3$  in  $F_5$  and  $x = 2, 5, 6, 7, 8, 11$  in  $F_{13}$ .

*Example.* The equation

$$x^2 = 1 \pmod{p}$$

has the solutions  $x = 1, p - 1$  in  $F_p$ , for every integer  $p$ ,

$$x^3 = 1 \pmod{p}$$

has the solutions  $x = 1$  in  $F_5$ ,  $x = 1, 2, 4$  in  $F_7$ , and  $x = 1, 3, 9$  in  $F_{13}$ ,

$$x^5 = 1 \pmod{p}$$

has the solutions  $x = 1$  in  $F_5$ ,  $x = 1, 3, 4, 5, 9$  in  $F_{11}$ , and  $x = 1$  in  $F_{13}$ ,

$$x^6 = 1 \pmod{p}$$

has the solutions  $x = 1, 4$  in  $F_5$  and  $x = 1, 3, 4, 9, 10, 12$  in  $F_{13}$ .

Table 2.1: Integer roots of  $x^n - 1$

$F_2$	$F_3$	$F_4$	$F_5$	$F_6$	$F_7$	$F_8$	$F_9$	$F_{10}$	$F_{11}$	$F_{12}$
1	1	1	1	1	1	1	1	1	1	1
3		3								
5	4	5		5			4			
7	7	7	6	7		7	7			
9		9			8	9		9		
11	10						10			
		11	11	11				11		11

**Theorem 2.3.13 (Gauss)** *Let  $p$  odd in  $\mathbb{P}$ , the equation*

$$\frac{x^p - 1}{x - 1} = 0 \pmod{p}$$

has  $p - 1$  trigonometric solutions

$$x_k = e^{\frac{2ki\pi}{n}}.$$

For every  $n$ , 1 is a root of the  $P_n$  in  $F_{n+1}$  where  $P_n(1) = 0$ , for every even  $n$ ,  $-1$  is a root of  $P_{n-1}$  in  $F_n$  and for every odd  $n$ ,  $-1$  is a root of  $P_n$  in  $F_{n+1}$ . In  $F_3 = \{0, 1, 2\}$ , there exists a single root 1 of  $P_2(x) = (x - 1)^2$ . In  $F_4 = \{0, 1, 2, 3\}$ , the roots of

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

are  $\pm 1$  each with parity 1, 2 or 3.

## 2.4 Wilson's Theorem and Sums of Squares

Lagrange (1771) published a proof of the necessary part of Wilson's theorem and deduced from it a proof of Fermat's first theorem, here the proof is simpler and the theorem is generalized to an equivalence due to Serret (1866).

**Theorem 2.4.1** *An integer  $n > 4$  is prime if and only if*

$$(n - 1)! + 1 = 0 \pmod{n}.$$

**Proof.** To prove the sufficiency, let us assume that  $n > 4$  is not prime and let  $n = \prod_{i=1}^{I_n} p_i^{\alpha_i}$ , with  $I_n > 1$ . For every  $i$ ,  $p_i^{\alpha_i} < n$  and it divides  $(n - 1)!$ , they are relatively prime which would imply  $n \mid (n - 1)!$ . If  $I_n = 1$ , let  $n = p^\alpha$  where  $\alpha \geq 2$ , then  $p \mid m$  for every  $m = kp < n$  and for every  $n > 4$ ,  $\alpha p < p^\alpha$  which would imply  $n \mid (n - 1)!$ .

Reciprocally,  $F_n$  is generated by a single  $\omega$  of  $F_n$  and  $\omega^{n-1} = 1$ , for every prime  $n$ . The sets  $\{\omega^k, k = 1, \dots, n - 2\}$  and  $F_n \setminus \{0, 1\}$  are identical so their product is

$$(n - 1)! = \omega^{\frac{n(n-1)}{2}},$$

furthermore  $\omega$  is not a square since it would not be the generator of  $F_n$ , therefore  $(n - 1)! = (-1)^n = -1 \pmod{n}$ .  $\square$

Theorem 2.4.1 is equivalent to

$$(n-2)! \equiv 1 \pmod{n}.$$

**Corollary 2.4.2** *For every  $n > 2$  in  $\mathbb{P}$*

$$\left(\frac{n-1}{2}\right)!^2 = \begin{cases} -1 \pmod{n}, & \text{if and only if } n \equiv 1 \pmod{4}, \\ +1 \pmod{n}, & \text{if and only if } n \equiv 3 \pmod{4}. \end{cases}$$

Proof. For  $n > 2$  prime,  $m = n - 1$  is even, writing  $n - k \equiv -k \pmod{n}$  we have

$$\begin{aligned} m! &= \prod_{j=1}^{n-1} (n-k) = (-1)^{\frac{m}{2}} \prod_{k=2}^{\frac{m}{2}} k^2 \pmod{n} \\ &= (-1)^{\frac{m}{2}} \left(\frac{m}{2}\right)!^2 \pmod{n}. \end{aligned}$$

By Theorem 2.4.1,  $\left(\frac{n-1}{2}\right)!^2 \equiv (-1)^{\frac{n+1}{2}} \pmod{n}$  and the result follows.  $\square$

If  $n \equiv 3 \pmod{4}$ , it follows that  $\frac{n-1}{2}! \equiv \pm 1 \pmod{n}$ . The first prime integers  $n \equiv 3 \pmod{4}$  are 3, 7, 11, 19, 23, 29 and for each of them

$$\left(\frac{n-1}{2}\right)! \equiv -1 \pmod{n}.$$

**Theorem 2.4.3** *Every  $p \equiv 1 \pmod{4}$  in  $\mathbb{P}$  is the sum of two squares.*

Proof. The previous corollary establishes that

$$p \mid \left(\frac{p-1}{2}\right)!^2 + 1$$

which is the sum of two squares and  $p$  has the same form by Theorem 1.2.7.  $\square$

The product of two sums of two squares is a sum of two squares (1.5). For example,  $2^\alpha$  is a square if  $\alpha$  is even, and by (1.5) it is a sum of two squares if  $\alpha$  is odd.

The product of two sums of four squares is a sum of four squares (Euler)

$$\begin{aligned} &(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned} \tag{2.5}$$

An integer

$$n = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

with  $p_i \equiv 1 \pmod{4}$  in  $\mathbb{P}$  for  $i = 1, \dots, k$ , is a sum of two squares for every  $\alpha_i \geq 1$  by Theorem 2.4.3 and by (1.5). This is a special case of Fermat's Theorem 1.2.1 for squares.

**Theorem 2.4.4** *Every  $p \equiv 3 \pmod{4}$  in  $\mathbb{P}$  is the difference of two squares.*

Proof. The previous theorem establishes that

$$p \mid \left( \frac{p-1}{2}! \right)^2 - 1$$

which is the difference of two squares. From Theorem 1.2.7,  $p$  has the same form.  $\square$

Let  $n = 2^\alpha p$  be an integer such that  $p \equiv 3 \pmod{4}$  in  $\mathbb{P}$ ,  $n$  is the difference between two squares if  $\alpha$  is even and it is the difference of two sums of two squares if  $\alpha$  is odd. The product of two difference of two squares is the difference of two squares

$$(x_1^2 - y_1^2)(x_2^2 - y_2^2) = (x_1x_2 + y_1y_2)^2 - (x_1y_2 - y_1x_2)^2,$$

we deduce the following decomposition of integers.

**Proposition 2.4.5** *For every  $n = 2^\alpha \prod_i p_i^{\alpha_i}$  such that  $p_i \equiv 3 \pmod{4}$  in  $\mathbb{P}$ , there exist  $n_1, \dots, n_4$  in  $\mathbb{N}$  such that  $n = n_1^2 + n_2^2 - n_3^2 - n_4^2$  if  $\alpha$  is odd and  $n = n_1^2 - n_2^2$  if  $\alpha$  is even.*

The equations  $x^2 + y^2 = z^3$  and more generally  $x^2 + y^2 = z^{2k+1}$  have non trivial integer solutions such that  $z \equiv 1 \pmod{4}$ .

**Proposition 2.4.6** *Let  $n$  be an integer having a representation*

$$n = x^2 + y^2$$

*with integers  $x$  and  $y$  and let  $p \equiv 3 \pmod{4}$ , then  $p$  does not divide  $n$ .*

Proof. Let  $p \equiv 3 \pmod{4}$  in  $\mathbb{P}$ , it is not sum of two squares by corollary 2.4.2. Let  $n = x^2 + y^2$  be such that  $p \mid n$ , then  $p$  should be also a sum of two squares by Theorem 1.2.7 which is contradictory. If  $p$  is not prime, there exists  $p_0$  in  $\mathbb{P}$  such that  $p = p_0^\alpha$  with an odd exponent  $\alpha$  and  $p_0$  cannot divide a sum of two squares.  $\square$

Table 2.2: Representation of  $n = 3 \pmod{4}$  as a sum of square

$k$	$n = 3 + 4k$	$S$
1	7	$4 + 1 + 1 + 1$
2	11	$9 + 1 + 1$
3	15	$9 + 4 + 1 + 1$
4	19	$16 + 1 + 1 + 1$
5	23	$9 + 9 + 4 + 1$
6	27	$25 + 1 + 1$
7	31	$25 + 4 + 1 + 1$
8	35	$25 + 9 + 1$
9	39	$36 + 1 + 1 + 1$
10	43	$25 + 9 + 9$
11	47	$25 + 9 + 9 + 4$
12	51	$25 + 16 + 9 + 1$
13	55	$25 + 25 + 4 + 1$
17	71	$25 + 16 + 16 + 4$
19	79	$25 + 25 + 25 + 4$
20	83	$49 + 25 + 9$
22	91	$36 + 25 + 16 + 4$
23	95	$49 + 36 + 16 + 4$
24	99	$49 + 49 + 1$

**Proposition 2.4.7 (Euler)** *For every odd  $p$  in  $\mathbb{P}$ , there exist  $x$  and  $y$  in  $\mathbb{N}$  such that*

$$1 + x^2 + y^2 = mp, \quad 0 < m < p.$$

Proof. The  $\frac{p+1}{2}$  integers  $x^2$  such that  $0 \leq x \leq \frac{p-1}{2}$  are distinct and the  $\frac{p+1}{2}$  integers  $-(1 + y^2)$  such that  $0 \leq y \leq \frac{p-1}{2}$  are distinct, it follows that there exist  $x$  and  $y$  such that  $1 + x^2 + y^2 = 0 \pmod{p}$ .  $\square$

**Theorem 2.4.8 (Lagrange)** *Every integer  $n$  is a sum of  $k$  squares, with  $k = 1, 2, 3$  or  $4$ .*

Proof. By (1.5), it is sufficient to prove the result for every prime integer. Let  $p$  be odd in  $\mathbb{P}$  and let  $1 \leq m_0 < p$  be the least integer such that

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

such integers  $x_i$  and  $m_0$  exist by Proposition 2.4.7. If  $m_0 > 1$  is odd, by the euclidean division of  $x_i$  by  $m_0$ , there exist  $y_i$  such that  $x_i = y_i \pmod{m_0}$  and  $|y_i| < \frac{m_0}{2}$  for  $i = 1, \dots, 4$ , therefore

$$\begin{aligned} y_1^2 + y_2^2 + y_3^2 + y_4^2 &< m_0^2, \\ y_1^2 + y_2^2 + y_3^2 + y_4^2 &= 0 \pmod{m_0} \end{aligned}$$

this entails a contradiction,  $m_0$  being the least integer.

If  $m_0$  is even, let  $x_1$  and  $x_2$  and, respectively  $x_3$  and  $x_4$ , have the same parity so their sum and difference are even

$$\frac{m_0 p}{2} = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

and  $m_0$  cannot be the least integer, then  $m_0 = 1$ . □

Lagrange's Theorem 2.4.8 is extended according to the value of the integers modulo 8, every odd integer except those equivalent to 7 (mod 8) are sums of three squares. For  $p = 3 \pmod{4}$  and every integer  $k > 1$

$$\begin{aligned} p^{2k} &= 1 \pmod{4}, \\ p^{2k+1} &= 3 \pmod{4}, \end{aligned}$$

they are sums of three or four squares. Every integer  $n = 3 \pmod{4}$  is written as  $n = \prod_{i=1}^k p_i^{\alpha_i}$  with  $p_i = 3 \pmod{4}$  with at least an odd exponent or  $p_i = 1 \pmod{4}$ . Table (2.1) gives the representation of numbers  $n = 3 \pmod{4}$  as a sum of three or four squares. It shows that the integers  $n = 3 \pmod{8}$  are sums of three squares and the integers  $n = 7 \pmod{8}$  are sums of four squares. The even integers  $8n + 6$  are sums of three squares and the integers  $8n + 2$  are sums of two squares.

The polygonal numbers have been defined in Section 1.2, now we prove Fermat's Theorem 1.2.1 on the representation of the integers as sums of polygonal numbers. A necessary and sufficient condition for an integer  $k$  to be a sum of three triangular numbers

$$k = p_{3,n_1} + p_{3,n_2} + p_{3,n_3}$$

is  $8k + 3$  is a sum of three squares defined by  $n_1, n_2$  and  $n_3$

$$8k + 3 = (2n_1 + 1)^2 + (2n_2 + 1)^2 + (2n_3 + 1)^2$$

and this equality is true for every  $k$ .

An integer  $k$  is sum of two triangular numbers if  $8k + 2$  is sum of two squares

$$8k + 2 = (2n_1 + 1)^2 + (2n_2 + 1)^2$$

and the condition for  $k = p_{3,n}$  is

$$8k + 1 = (2n + 1)^2.$$

Some classes of integers cannot be sum of no less than three triangular numbers such as the numbers  $2^{2n+1}$ ,  $n \geq 1$ . For every pentagonal number  $p_{5,k}$ ,  $8p_{5,k} + 1$  is sum of three squares

$$8p_{5,k} + 1 = (2k - 1)^2 + 2(2k)^2$$

and  $24p_{5,k} + 1 = (6k - 1)^2$ .

A necessary and sufficient condition for the representation of an integer  $k$  as a sum of five pentagons is

$$24k + 5 = (6n_1 - 1)^2 + (6n_2 - 1)^2 + \dots + (6n_5 - 1)^2$$

where  $24k + 5 \equiv 1 \pmod{4}$  and for each square  $(6n_i - 1)^2 \equiv 1 \pmod{12}$ ,  $i = 1, \dots, 5$ . Reversely, every integer equivalent to 5 (mod 12) is sum of five squares  $(6n_i - 1)^2 \equiv 1 \pmod{12}$  which entails  $k$  is sum of five pentagons. An integer  $k$  is sum of  $m$  pentagons if and only if  $24k + m$  is sum of  $m$  squares of the same form  $(6n_i - 1)^2$ ,  $i = 1, \dots, m$ .

The same argument is generalized to every polygonal number  $p_{\alpha+2,k}$ . For a heptagonal integer  $p_{7,k}$ ,  $2p_{7,k} = 5k^2 - 3k$  and

$$40p_{7,k} + 9 = (10k - 3)^2.$$

A necessary and sufficient condition for the representation of an integer  $k$  as a sum of seven heptagons is

$$40k + 63 = (10n_1 - 3)^2 + (10n_2 - 3)^2 + \dots + (10n_7 - 3)^2$$



where  $40k + 45 = 3 \pmod{20}$ . Reversely, every integer equivalent to  $3 \pmod{20}$  is sum of seven squares  $(10n_i - 3)^2 = 9 \pmod{20}$  which entails every integer  $k$  is sum of seven heptagons.

For an  $\alpha$ -polygonal number  $p_{\alpha+2,k}$ ,  $2p_{\alpha+2,k} = \alpha n^2 - (\alpha - 2)n$  and

$$8\alpha p_{\alpha+2,k} + (\alpha - 2)^2 = (2\alpha n - \alpha + 2)^2.$$

A necessary and sufficient condition for the representation of an integer  $k$  as a sum of  $\alpha + 2$  polygons of order  $\alpha + 2$  is

$$8\alpha k + (\alpha + 2)(\alpha - 2)^2 = (2\alpha n_1 - \alpha + 2)^2 + \cdots + (2\alpha n_{\alpha+2} - \alpha + 2)^2$$

where  $8\alpha k + (\alpha + 2)(\alpha - 2)^2 = \alpha^3 + 2\alpha^2 + 8 \pmod{4\alpha}$  and for every  $i$

$$(2\alpha n_i - \alpha + 2)^2 = \alpha^2 + 4 \pmod{4\alpha}.$$

Every integer satisfying this equivalence is sum of  $\alpha + 2$  polygons of order  $\alpha + 2$ .

## 2.5 Euler's $\phi(n)$

The function  $\phi$  is used to generalize Fermat's first theorem to composite numbers.

**Theorem 2.5.1** *Let  $a$  and  $n$  be relatively primes, then*

$$a^{\phi(n)} = 1 \pmod{n}.$$

*Proof.* Let  $(x_k)_{k=1, \dots, \phi(n)}$  be the sequence of the integers smaller than  $n$  and relatively prime to  $n$  and let  $a$  be relatively prime to  $n$ . The integers of the sequence  $(ax_k)_{k=1, \dots, \phi(n)}$  and their differences cannot be multiple of  $n$  and they are distinct modulo  $n$ , they are therefore equivalent to  $(x_k)_{k=1, \dots, \phi(n)} \pmod{n}$ . This implies  $a^{\phi(n)} = 1 \pmod{n}$ , since  $\prod_{k=1, \dots, \phi(n)} x_k$  is relatively prime to  $n$ .  $\square$

**Corollary 2.5.2** *Let  $p$  be odd and let  $a$  be relatively prime to  $p$ , if  $p \mid x^2 \pm a$  then there exist  $s$  and  $t$  such that  $p = s^2 \pm at^2$ .*

Proof. The proof is the same as for Corollary 2.1.4. Using Euler's theorem,  $x^2 \pm ay^2$  is multiple of  $p$  with Let  $p \mid x^2 \pm a$  and let

$$y = \begin{cases} a^{\frac{p-1}{2}} & \text{if } p \in \mathbb{P}, \\ a^{\frac{\phi(p)-1}{2}} & \text{if } p \notin \mathbb{P}, \end{cases}$$

then  $x^2 \pm ay^2$  is multiple of  $p$  by Fermat or Euler theorems. From Theorem 1.2.9, there exist  $s$  and  $t$  such that  $p = s^2 \pm at^2$ .  $\square$

Wilson's Theorem 2.4.1 generalizes to composite integers (Sylvester 1838, Serret 1866).

**Theorem 2.5.3** *Let  $n$  in  $\mathbb{N}$  and let  $N$  be the product of the integers prime to  $n$  and smaller than  $n$ , then  $N = \pm 1 \pmod{n}$ . We have  $N = -1 \pmod{n}$  if  $n = p^\alpha$  where  $p > 2$  belongs to  $\mathbb{P}$ , or  $n = 2p^\alpha$  or  $n = 4$ , otherwise  $N = 1 \pmod{n}$ .*

**Corollary 2.5.4** *Let  $N$  in  $\mathbb{N}$  and let  $a$  be relatively prime to  $N$ , the smallest integer  $n$  satisfying  $a^n = 1 \pmod{N}$  is such that  $n \mid \phi(N)$ .*

Proof. Let  $n$  be the smallest integer such that  $a^n = 1 \pmod{N}$ , the integers of the sequence  $1, a, \dots, a^{n-1}$  are smaller than  $N$  and they are distinct, therefore

$$\begin{aligned} a^{kn} &= 1 \pmod{N}, k \geq 1, \\ a^m &\neq 1 \pmod{N}, m \neq kn, k \geq 1. \end{aligned}$$

Theorem 2.5.1 implies there exists  $k \geq 1$  such that  $\phi(N) = kn$ .  $\square$

If all numbers smaller than  $N$  and relatively prime to  $N$  belong to the sequence  $1, a, a^2, \dots, a^{n-1}$ , then  $n = \phi(N)$ .

## 2.6 Exercises

*Exercise 2.1.* Find the solutions of  $ax = b \pmod{p}$  with  $p$  in  $\mathbb{P}$  and  $\gcd(a, p) = 1$ .

*Exercise 2.2.* Give the values of  $\left(\frac{11}{p}\right)$  and  $\left(\frac{17}{p}\right)$ .

*Exercise 2.3.* Find the solutions of  $x^n = a \pmod{p}$  with  $p$  in  $\mathbb{P}$ .

*Exercise 2.4.* Find the solutions of  $x^{p^n} = a \pmod{p}$  with  $p$  in  $\mathbb{P}$ .

*Exercise 2.5.* Prove that a triangular number cannot be a bisquare, except one.