

# NUMBER THEORY

TS.Nguyễn Việt Đông

1

## Number theory

- 1.Divisors
- 2.Primer Factorization
- 3.Congruence
- 4.Quadratic Residues

2

## 1.Divisors

**Theorem 1.1. Division Algorithm.** *Let  $n$  and  $d \geq 1$  be integers. There exist uniquely determined integers  $q$  and  $r$  such that  $n = qd + r$  and  $0 \leq r < d$ .*

Proof. Let  $X = \{n - td \mid t \in \mathbb{Z}, n - td \geq 0\}$ . Then  $X$  is nonempty (if  $n \geq 0$ , then  $n \in X$ ; if  $n < 0$ , then  $n(1 - d) \in X$ ). Hence let  $r$  be the smallest member of  $X$ . Then  $r = n - qd$  for some  $q \in \mathbb{Z}$ , and it remains to show that  $r < d$ . But if  $r \geq d$ , then  $0 \leq r - d = n - (q + 1)d$ , so  $r - d$  is in  $X$  contrary to the minimality of  $r$ .

As to uniqueness, suppose that  $n = q'd + r'$ , where  $0 \leq r' < d$ . We may assume that  $r \leq r'$  (a similar argument works if  $r' \leq r$ ). Then  $0 \leq r' - r = (q - q')d$ , so  $(q - q')d$  is a nonnegative multiple of  $d$  that is less than  $d$  (because  $r' - r \leq r' < d$ ). The only possibility is  $(q - q')d = 0$ , so  $q' = q$ , and hence  $r' = r$ .

3

## 1.Divisors

- Given  $n$  and  $d \geq 1$ , the integers  $q$  and  $r$  in Theorem 1.1 are called, respectively, the **quotient and remainder when  $n$  is divided by  $d$** .

**For example**, if we divide  $n = -29$  by  $d = 7$ , we find that  $-29 = (-5) \cdot 7 + 6$ , so the quotient is  $-5$  and remainder is  $6$ .

The usual process of long division is a procedure for finding the quotient and remainder for a given  $n$  and  $d \geq 1$ . However, they can easily be found with a calculator. For example, if  $n = 3196$  and  $d = 271$  then  $n/d = 11.79$  approximately, so  $q = 11$ . Then  $r = n - qd = 215$ , so  $3196 = 11 \cdot 271 + 215$ , as desired.

If  $d$  and  $n$  are integers, we say that  $d$  **divides  $n$** , or that  $d$  is a **divisor of  $n$** , if  $n = qd$  for some integer  $q$ . We write  $d \mid n$  when this is the case. Thus, a positive integer  $p > 1$  is prime if and only if  $p$  has no positive divisors except  $1$  and  $p$ . The following properties of the divisibility relation  $\mid$  are easily verified:

4

## 1.Divisors

- (i)  $n|n$  for every  $n$ .
- (ii) If  $d|m$  and  $m|n$ , then  $d|n$ .
- (iii) If  $d|n$  and  $n|d$ , then  $d = \pm n$ .
- (iv) If  $d|n$  and  $d|m$ , then  $d|(xm + yn)$  for all integers  $x$  and  $y$ .

Given positive integers  $m$  and  $n$ , an integer  $d$  is called a **common divisor** of  $m$  and  $n$  if  $d|m$  and  $d|n$ .

If  $m$  and  $n$  are integers, not both zero, we say that  $d$  is the **greatest common divisor of  $m$  and  $n$** , and write  $d = \gcd(m, n)$ , if the following three conditions are satisfied:

- (i)  $d \geq 1$ .
- (ii)  $d|m$  and  $d|n$ .
- (iii) If  $k|m$  and  $k|n$ , then  $k|d$ .

5

## 1.Divisors

- **Theorem 1.2.** Let  $m$  and  $n$  be integers, not both zero. Then  $d = \gcd(m, n)$  exists, and  $d = xm + yn$  for some integers  $x$  and  $y$ .

*Proof.* Let  $X = \{sm + tn \mid s, t \in \mathbb{Z}; sm + tn \geq 1\}$ . Then  $X$  is not empty since  $m^2 + n^2$  is in  $X$ , so let  $d$  be the smallest member of  $X$ . Since  $d \in X$  we have  $d \geq 1$  and

$d = xm + yn$  for integers  $x$  and  $y$ , proving conditions (i) and (iii) in the definition of the gcd.

Hence it remains to show that  $d|m$  and  $d|n$ . We show that  $d|n$ ; the other is similar. By the division algorithm

6

## 1.Divisors

write  $n = qd + r$ , where  $0 \leq r < d$ . Then

$r = n - q(xm + yn) = (-qx)m + (1 - qy)n$ . Hence, if  $r \geq 1$ , then  $r \in X$ , contrary to the minimality of  $d$ . So  $r = 0$  and we have  $d|n$ .

When  $\gcd(m, n) = xm + yn$  where  $x$  and  $y$  are integers, we say that  $\gcd(m, n)$  is a *linear combination* of  $m$  and  $n$ . There is an efficient way of computing  $x$  and  $y$  using the division algorithm.

The following example illustrates the method.

7

## 1.Divisors

- **Example . Find  $\gcd(37, 8)$  and express it as a linear combination of 37 and 8.**

*Proof.* It is clear that  $\gcd(37, 8) = 1$  because 37 is a prime; however, no linear combination is apparent. Dividing 37 by 8, and then dividing each successive divisor by the preceding remainder, gives the first set of equations.

$$\begin{aligned}
 37 &= 4 \cdot 8 + 5 & 1 &= 3 - 1 \cdot 2 = 3 - 1(5 - 1 \cdot 3) \\
 8 &= 1 \cdot 5 + 3 & &= 2 \cdot 3 - 5 = 2(8 - 1 \cdot 5) - 5 \\
 5 &= 1 \cdot 3 + 2 & &= 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3(37 - 4 \cdot 8) \\
 3 &= 1 \cdot 2 + 1 & &= 14 \cdot 8 - 3 \cdot 37 \\
 2 &= 2 \cdot 1 & &
 \end{aligned}$$

The last nonzero remainder is 1, the greatest common divisor, and this turns out always to be the case. Eliminating remainders from the bottom up (as in the second set of equations) gives  $1 = 14 \cdot 8 - 3 \cdot 37$ .

8

## 1.Divisors

- **Theorem 1.3. Euclidean Algorithm.** Given integers  $m$  and  $n \geq 1$ , use the division algorithm repeatedly:

$$m = q_1n + r_1 \quad 0 \leq r_1 < n$$

$$n = q_2r_1 + r_2 \quad 0 \leq r_2 < r_1$$

$$r_1 = q_3r_2 + r_3 \quad 0 \leq r_3 < r_2$$

...

...

$$r_{k-2} = q_k r_{k-1} + r_k \quad 0 \leq r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1} r_k$$

where in each equation the divisor at the preceding stage is divided by the remainder. These remainders decrease

$$r_1 > r_2 > \dots \geq 0$$

9

## 1.Divisors

so the process eventually stops when the remainder becomes zero. If  $r_1 = 0$ , then  $\gcd(m, n) = n$ . Otherwise,  $r_k = \gcd(m, n)$ , where  $r_k$  is the last nonzero remainder and can be expressed as a linear combination of  $m$  and  $n$  by eliminating remainders.

*Proof.* Express  $r_k$  as a linear combination of  $m$  and  $n$  by eliminating remainders in the equations from the second last equation up. Hence every common divisor of  $m$  and  $n$  divides  $r_k$ . But  $r_k$  is itself a common divisor of  $m$  and  $n$  (it divides every  $r_i$ —work up through the equations). Hence  $r_k = \gcd(m, n)$ .

10

## 1.Divisors

Two integers  $m$  and  $n$  are called relatively prime if  $\gcd(m, n) = 1$ . Hence 12 and 35 are relatively prime, but this is not true for 12 and 15. Because  $\gcd(12, 15) = 3$ . Note that 1 is relatively prime to every integer  $m$ . The following theorem collects three basic properties of relatively prime integers.

**Theorem 1.4.** If  $m$  and  $n$  are integers, not both zero:

(i)  $m$  and  $n$  are relatively prime if and only if  $1 = xm + yn$  for some integers  $x$  and  $y$ .

(ii) If  $d = \gcd(m, n)$ , then  $m/d$  and  $n/d$  are relatively prime.

(iii) Suppose that  $m$  and  $n$  are relatively prime.

(a) If  $m|k$  and  $n|k$ , where  $k \in \mathbb{Z}$ , then  $mn|k$ .

(b) If  $m|kn$  for some  $k \in \mathbb{Z}$ , then  $m|k$ .

11

## 1.Divisors

- *Proof.* (i) If  $1 = xm + yn$  with  $x, y \in \mathbb{Z}$ , then every divisor of both  $m$  and  $n$  divides 1, so must be 1 or  $-1$ . It follows that  $\gcd(m, n) = 1$ . The converse is by the euclidean algorithm.

(ii). By Theorem 1.2, write  $d = xm + yn$ , where  $x, y \in \mathbb{Z}$ . Then

$$1 = x(m/d) + y(n/d) \quad \text{and (ii) follows from (i).}$$

(iii). Write  $1 = xm + yn$ , where  $x, y \in \mathbb{Z}$ . If  $k = am$  and  $k = bn$ ,  $a, b \in \mathbb{Z}$  then  $k = kxm + kyn = (xb + ya)mn$ , and (a) follows. As to (b), suppose that  $kn = qm$ ,  $q \in \mathbb{Z}$ . Then  $k = kxm + kyn = (kx + qn)m$ , so  $m|k$ .

12

## 2. Prime Factorization

Recall that an integer  $p$  is called a **prime** if:

- (i)  $p \geq 2$ .
- (ii) The only positive divisors of  $p$  are 1 and  $p$ .

The reason for not regarding 1 as a prime is that we want the factorization of every integer into primes to be unique. The following result is needed.

13

## 2. Prime Factorization

• **Theorem 2.1. Euclid's Lemma.** Let  $p$  denote a prime.

- (i) If  $p|mn$  where  $m, n \in \mathbb{Z}$ , then either  $p|m$  or  $p|n$ .
- (ii) If  $p|m_1 m_2 \cdots m_r$ , where each  $m_i \in \mathbb{Z}$ , then  $p|m_i$  for some  $i$ .

*Proof.* (i) Write  $d = \gcd(m, p)$ . Then  $d|p$ , so as  $p$  is a prime, either  $d = p$  or  $d = 1$ .

If  $d = p$ , then  $p|m$ ; if  $d = 1$ , then since  $p|mn$ , we have  $p|n$  by Theorem 1.4.

(ii) This follows from (i) using induction on  $r$ .

14

## 2. Prime Factorization

• **Theorem 2.2.** Every integer  $n > 1$  is a product of primes.

• *Proof.* Let  $p_n$  denote the statement of the theorem. Then  $p_2$  is clearly true.

If  $p_2, p_3, \dots, p_k$  are all true, consider the integer  $k + 1$ . If  $k + 1$  is a prime, there is nothing to prove. Otherwise,

$k + 1 = ab$ , where  $2 \leq a, b \leq k$ . But then each of  $a$  and  $b$  are products of primes because  $p_a$  and  $p_b$  are both true by the (strong) induction assumption. Hence  $ab = k + 1$  is also a product of primes, as required.

15

## 2. Prime Factorization

• **Theorem 2.3. Prime Factorization Theorem.** Every integer  $n \geq 2$  can be written as a product of (one or more) primes. Moreover, this factorization is unique except for the order of the factors. That is,

$$\text{if } n = p_1 p_2 \cdots p_r \text{ and } n = q_1 q_2 \cdots q_s,$$

where the  $p_i$  and  $q_j$  are primes, then  $r = s$  and the  $q_j$  can be relabeled so that  $p_i = q_i$  for each  $i$ .

16

## 2.Prime Factorization

- *Proof.* The existence of such a factorization was shown in Theorem 2.2. To prove uniqueness, we induction the minimum of  $r$  and  $s$ . If this is 1, then  $n$  is a prime and the uniqueness follows from Euclid's lemma. Otherwise,  $r \geq 2$  and  $s \geq 2$ . Since  $p_1 | n = q_1 q_2 \cdots q_s$  Euclid's lemma shows that  $p_1$  divides some  $q_j$ , say  $p_1 | q_1$  (after possible relabeling of the  $q_j$ ). But then  $p_1 = q_1$  because  $q_1$  is a prime. Hence  $n/p_1 = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$ , so, by induction,  $r - 1 = s - 1$  and  $q_2, q_3, \dots, q_s$  can be relabeled such that  $p_i = q_i$  for all  $i = 2, 3, \dots, r$ . The theorem follows.

17

## 2.Prime Factorization

- It follows that every integer  $n \geq 2$  can be written in the form  $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ , where  $p_1, p_2, \dots, p_r$  are distinct primes,  $n_i \geq 1$  for each  $i$ , and the  $p_i$  and  $n_i$  are determined uniquely by  $n$ . If every  $n_i = 1$ , we say that  $n$  is **square-free**, while if  $n$  has only one prime divisor, we call  $n$  a **prime power**. If the prime factorization  $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$  of an integer  $n$  is given, and if  $d$  is a positive divisor of  $n$ , then these  $p_i$  are the only possible prime divisors of  $d$  (by Euclid's lemma). It follows that

18

## Prime Factorization

### Collorary 2.4

If the prime factorization of  $n$  is  $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ , then the positive divisors  $d$  of  $n$  are given as follows:

$$d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \text{ where } 0 \leq d_i \leq n_i \text{ for each } i.$$

19

## Prime Factorization

**Theorem 2.5** Suppose that  $m$  and  $n$  are positive integers, and write

$$\begin{aligned} n &= p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} & n_i &\geq 0 \\ m &= p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} & m_i &\geq 0, \end{aligned}$$

where the  $p_i$  are distinct primes. Then:

$$\begin{aligned} \gcd(m, n) &= p_1^{\min(m_1, n_1)} p_2^{\min(m_2, n_2)} \cdots p_r^{\min(m_r, n_r)} \\ \text{lcm}(m, n) &= p_1^{\max(m_1, n_1)} p_2^{\max(m_2, n_2)} \cdots p_r^{\max(m_r, n_r)}. \end{aligned}$$

20

Note that this all generalizes: Given a finite collection  $a, b, c, \dots$  of positive integers, write them as

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} & a_i &\geq 0 \\ b &= p_1^{b_1} p_2^{b_2} \dots p_r^{b_r} & b_i &\geq 0 \\ c &= p_1^{c_1} p_2^{c_2} \dots p_r^{c_r} & c_i &\geq 0, \\ &\vdots & & \\ &\vdots & & \end{aligned}$$

where the  $p_i$  are the distinct primes that divide at least one of  $a, b, c, \dots$ . Then define their **greatest common divisor** and **least common multiple** as follows:

$$\begin{aligned} \gcd(a, b, c, \dots) &= p_1^{\min(a_1, b_1, c_1, \dots)} p_2^{\min(a_2, b_2, c_2, \dots)} \dots p_r^{\min(a_r, b_r, c_r, \dots)} \\ \text{lcm}(a, b, c, \dots) &= p_1^{\max(a_1, b_1, c_1, \dots)} p_2^{\max(a_2, b_2, c_2, \dots)} \dots p_r^{\max(a_r, b_r, c_r, \dots)}. \end{aligned}$$

### 3. Congruences

- **Definition 3.1.** If  $m \geq 0$  is fixed, then integers  $a$  and  $b$  are *congruent modulo  $m$* , denoted by  $a \equiv b \pmod{m}$  if  $m \mid (a - b)$ . Usually, one assumes that the modulus  $m > 1$  because the cases  $m = 0$  and  $m = 1$  are not very interesting: if  $a$  and  $b$  are integers, then  $a \equiv b \pmod{0}$  if and only if  $0 \mid (a - b)$ , that is,  $a = b$ , and so congruence mod 0 is ordinary equality. The congruence  $a \equiv b \pmod{1}$  is true for every pair of integers  $a$  and  $b$  because  $1 \mid (a - b)$  always. Hence, every two integers are congruent mod 1.

### 3. Congruences

- If  $a$  and  $b$  are positive integers, then  $a \equiv b \pmod{10}$  if and only if they have the same last digit; more generally,  $a \equiv b \pmod{10^n}$  if and only if they have same last  $n$  digits. For example,  $526 \equiv 1926 \pmod{100}$ .
- London time is 6 hours later than Chicago time. What time is it in London if it is 10:00 A.M. in Chicago? Since clocks are set up with 12 hour cycles, this is really a problem about congruence mod 12. To solve it, note that  $10 + 6 = 16 \equiv 4 \pmod{12}$ ; and so it is 4:00 P.M. in London.

### 3. Congruences

- **Proposition 3.1.** If  $m > 0$  is a fixed integer, then for all integers  $a, b, c$ ,
  - (i)  $a \equiv a \pmod{m}$ ;
  - (ii) if  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$ ;
  - (iii) if  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$ .
- **Proposition 3.2.** Let  $m > 0$  be a fixed integer.
  - (i) If  $a = qm + r$ , then  $a \equiv r \pmod{m}$ .
  - (ii) If  $0 \leq r' < r < m$ , then  $r$  and  $r'$  are not congruent mod  $m$ ; in symbols,  $r \not\equiv r' \pmod{m}$ .
  - (iii)  $a \equiv b \pmod{m}$  if and only if  $a$  and  $b$  leave the same remainder after dividing by  $m$ .

### 3. Congruences

• **Proposition 3.3.** Let  $m > 0$  be a fixed integer.

(i) If  $a_i \equiv a'_i \pmod{m}$  for  $i = 1; 2; \dots; n$ , then

$$a_1 + \dots + a_n \equiv a'_1 + \dots + a'_n \pmod{m}:$$

In particular, if  $a \equiv a' \pmod{m}$  and  $b \equiv b' \pmod{m}$ , then

$$a + b \equiv a' + b' \pmod{m}:$$

(ii) If  $a_i \equiv a'_i \pmod{m}$  for  $i = 1; 2; \dots; n$ , then

$$a_1 \dots a_n \equiv a'_1 \dots a'_n \pmod{m}$$

In particular, if  $a \equiv a' \pmod{m}$  and  $b \equiv b' \pmod{m}$ , then  $ab \equiv a'b' \pmod{m}$

(iii) If  $a \equiv b \pmod{m}$ , then  $a^n \equiv b^n \pmod{m}$  for all  $n > 0$ .

25

### 3. Congruences

**Theorem 3.4 (Fermat).**

(i) If  $p$  is a prime, then

$$a^p \equiv a \pmod{p}$$

for every  $a$  in  $\mathbb{Z}$ .

(ii) If  $p$  is a prime, then

$$a^{p^k} \equiv a \pmod{p}$$

for every  $a$  in  $\mathbb{Z}$  and every integer  $k \geq 1$ .

26

### 3. Congruences

• **Theorem 3.5.** If  $(a; m) = 1$ , then, for every integer  $b$ , the congruence  $ax \equiv b \pmod{m}$  can be solved for  $x$ ; in fact,  $x = sb$ , where  $sa \equiv 1 \pmod{m}$ . Moreover, any two solutions are congruent mod  $m$ .

*Proof.* Since  $(a; m) = 1$ , there is an integer  $s$  with  $sa \equiv 1 \pmod{m}$  (because there is a linear combination  $1 = sa + tm$ ). It follows that  $b = sab + tmb$  and  $asb \equiv b \pmod{m}$ , so that  $x = sb$  is a solution. (Note that Proposition 3.2(i) allows us to take  $s$  with  $1 \leq s < m$ .)

If  $y$  is another solution, then  $ax \equiv ay \pmod{m}$ , and so  $m \mid a(x - y)$ . Since  $(a; m) = 1$ , Theorem 1.4 gives  $m \mid (x - y)$ ; that is,  $x \equiv y \pmod{m}$ .

27

### 4. Quadratic Residues

• **Definition 4.1.** If  $m$  is a positive integer, we say that the integer  $a$  is a *quadratic residue* of  $m$  if  $(a, m) = 1$  and the congruence  $x^2 \equiv a \pmod{m}$  has a solution.

If the congruence  $x^2 \equiv a \pmod{m}$  has a no solution, we say  $a$  is *quadratic nonresidue* of  $m$ .

**Example.** To determine which integers are quadratic residues of 11, we compute the squares of the integers 1, 2, 3, ..., 10. We find that  $1^2 \equiv 10^2 \equiv 1 \pmod{11}$ ,  $2^2 \equiv 9^2 \equiv 4 \pmod{11}$ ,  $3^2 \equiv 8^2 \equiv 9 \pmod{11}$ ,  $4^2 \equiv 7^2 \equiv 5 \pmod{11}$ , and  $5^2 \equiv 6^2 \equiv 3 \pmod{11}$ .

Hence, the quadratic residues of 11 are 1, 3, 4, 5, 9; the integers 2, 6, 7, 8, 10 are quadratic nonresidues of 11.

28

## 4. Quadratic Residues

- **Lemma 4.1.** Let  $p$  be odd prime and  $a$  an integer not divisible by  $p$ . Then the congruence  $x^2 \equiv a \pmod{p}$  has either no solutions or exactly two incongruent solutions modulo  $p$ .
- *Proof.* If  $x^2 \equiv a \pmod{p}$  has a solution, say  $x = x_0$ , then we can easily demonstrate that  $x = -x_0$  is second incongruent solution. Since  $(-x_0)^2 = x_0^2 \equiv a \pmod{p}$  we see that  $-x_0$  is solution. We note that  $x_0 \not\equiv -x_0 \pmod{p}$ , for if  $x_0 \equiv -x_0 \pmod{p}$ , then we have  $2x_0 \equiv 0 \pmod{p}$ . This is impossible since  $p$  is odd and  $p \nmid x_0$  (since  $x_0^2 \equiv a \pmod{p}$  and  $p \nmid a$ ).  
To show that there are no more than two incongruent solutions, assume that  $x \equiv x_0$  and  $x \equiv x_1$  are both solutions of  $x^2 \equiv a \pmod{p}$ . Then we have  $x_0^2 \equiv x_1^2 \equiv a \pmod{p}$ , so that

29

## 4. Quadratic Residues

$$x_0^2 - x_1^2 = (x_0 + x_1)(x_0 - x_1) \equiv 0 \pmod{p}.$$

Hence,  $p \mid (x_0 + x_1)$  or  $p \mid (x_0 - x_1)$ , so that  $x_1 \equiv -x_0 \pmod{p}$  or  $x_0 \equiv x_1 \pmod{p}$ . Therefore if there is a solution of  $x^2 \equiv a \pmod{p}$ , there are exactly two incongruent solution.

**Theorem 4.2.** If  $p$  is an odd prime, then there are exactly  $(p-1)/2$  quadratic residues of  $p$  and  $(p-1)/2$  quadratic nonresidues of  $p$  among the integer  $1, 2, \dots, p-1$ .

*Proof.* To find all the quadratic residues of  $p$  among the integers  $1, 2, \dots, p-1$  we compute the least positive residues modulo  $p$  of the squares of the integers  $1, 2, p-1$ .

30

## 4. Quadratic Residues

- Since there are  $p-1$  squares to consider and since each congruence  $x^2 \equiv a \pmod{p}$  has either zero or two solutions, there must be exactly  $(p-1)/2$  quadratic residues of  $p$  among the integer  $1, 2, \dots, p-1$ . The remaining  $p-1 - (p-1)/2 = (p-1)/2$  positive integers less than  $p-1$  are quadratic nonresidues of  $p$ .  $\square$

□

The special notation associated with quadratic residues is described in the following definition.

31

## 4. Quadratic Residues

- **Definition 4.2.** Let  $p$  be an odd prime and  $a$  an integer not divisible by  $p$ . The Legendre symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p \end{cases}$$

- The symbol is named after the French mathematician Adrien – Marie Legendre who introduced the use of this notation

32

### 4. Quadratic Residues

- Example . The previous example shows that the Legendre symbol

$$\left(\frac{a}{11}\right), a = 1, 2, \dots, 10$$

have the followings values :

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$$

33

### 4. Quadratic Residues

We now present a criterion for deciding whether an integer is a quadratic residue of prime. This criterion is useful in demonstraing propeties of the Legendre symbol.

**Theorem 4.3. Euler’s Criterion.**

Let  $p$  be an odd prime and let  $a$  be positive integer not divisible by  $p$ . Then

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

34

### 4. Quadratic Residues

*Proof.*

Firt ,assume that  $\left(\frac{a}{p}\right) = 1$  .Then , the congruence  $x^2 \equiv a \pmod{p}$

has a solution, say  $x = x_0$ . Using Fermat’s little theorem , we see that

$$a^{(p-1)/2} = (x_0^2)^{(p-1)/2} = x_0^{p-1} \equiv 1 \pmod{p}$$

Hence,if  $\left(\frac{a}{p}\right) = 1$ ,we know that  $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

35

### 4. Quadratic Residues

- Now cosider the case where  $\left(\frac{a}{p}\right) = -1$  .Then , the congruence  $x^2 \equiv a \pmod{p}$  has no solutions. For each integer  $i$  such that  $1 \leq i \leq p-1$ , there is a unique integer  $j$  with  $1 \leq j \leq p-1$ , such that  $ij \equiv a \pmod{p}$  . Furthermore , since the congruence  $x^2 \equiv a \pmod{p}$  has no solutions, we know that  $i \neq j$ . Thus, we can group the integer  $1, 2, \dots, p - 1$  into  $(p - 1)/2$  pairs each with product  $a$  . Multiplying these pairs together, we find that  $(p - 1)! \equiv a^{(p-1)/2} \pmod{p}$ . Since Wilson’s theorem tell us that  $(p - 1)! \equiv -1 \pmod{p}$ , we see that  $-1 \equiv a^{(p-1)/2} \pmod{p}$  . In this case, we also have  $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ .

36

## 4. Quadratic Residues

**Theorem 4.4.** Let  $p$  be an odd prime and  $a$  and  $b$  integers not divisible by  $p$ . Then

$$i) \text{ if } a \equiv b \pmod{p}, \text{ then } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

$$ii) \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

$$iii) \left(\frac{a^2}{p}\right) = 1.$$

37

## 4. Quadratic Residues

*Proof.*

i) If  $a \equiv b \pmod{p}$  then  $x^2 \equiv a \pmod{p}$  has a solution if and only if  $x^2 \equiv b \pmod{p}$  has a solution. Hence  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .

ii) By Euler's criterion we know that

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

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

38

## 4. Quadratic Residues

Hence,

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

Since the only possible values of a Legendre symbol are  $\pm 1$ , we conclude that

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

39

## 4. Quadratic Residues

• iii) Since  $\left(\frac{a}{p}\right) = \pm 1$ , from part (ii) it follows that

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$$

40