Theory of Numbers

Hechen Hu

December 24, 2017

Contents

1

Divisibility, the Fundamental Theorem of Number Theory

1.1 Divisibility

Definition. The divisors of a number that are less than the number itself is called its *parts*. If a number is the sum of its parts, it's called a *perfect number*(e.g. 6, 28, and 496). If two numbers are the sum of the other one's parts, they are called *amicable*(e.g. 220 and 284).

Theorem 1.1.1 (Remainder Theorem)**.** *For all numbers a and $b \neq 0$, there is an integer c and a number d such that*

$$a = bc + d \quad \text{and} \quad 0 \leqslant d < |b|$$

and only one such c and d exist. We say that a divided by b has quotient c with remainder d.

Proposition. For all numbers a and $b \neq 0$, there is an integer c' and a number d' such that

$$a = bc' + d' \quad \text{and} \quad -\frac{|b|}{2} < d' \leqslant \frac{|b|}{2}$$

and only one such c' and d'.

Theorem 1.1.2 (Four Number Theorem)**.** *If a and c are numbers and b and d are integers such that*

$$ab = cd$$

then there exists a positive number r and positive integers s, t, and u such that the following equalities hold:

$$a = rs, \quad b = tu, \quad c = rt, \quad d = su$$

If, in addition, a and c are integers, then r may be taken to be an integer.

Definition. An integer a is a *divisor* of an integer b if there exists a number c such that

$$b = ac$$

In this case we also say that b is *divisible* by a and denoted $a|b$. Otherwise, it is denoted $a \nmid b$. Among the divisors of a, 1, -1, a, and $-a$ is called its *trivial divisors*. Other positive divisors smaller than a are called its *proper divisors*. 1 and -1 is called *units*.

Definition. Two numbers that do not have a common divisor other than the units are called *relatively prime*.

***Example* 1.1.** *for any number a*

- $a|0$*;*
- 0 *is only a divisor of* 0*.*
- *If $a|b$ and $b|c$, then $a|c$.*

  Division is reflexive and transitive. In general it is not symmetric.

If b_i are integers such that $a|b_i$, and c_i are arbitrary integers ($i = 1, 2, \cdots, k$), then $a| \sum_{i=1}^{k} b_i c_i$.

Definition. A number a and $-a$ is said to be *associates* of each other. Theorems relating to divisibility apply to the classes of associated numbers.

***Example* 1.2.** *If $a|b$, then $ca|cb$, and if $c \neq 0$, then the first relation follows from the second.*

Lemma (Euclid's Lemma)**.** *If a number divides the product of two numbers and is relatively prime to one of the factors, then it must divide the other factor.*

1.2 Prime Numbers

Definition. If a number only has the trivial ones as its divisors, it's called *prime*. If a number is not prime and not unit, it's called a *composite number*.

Theorem 1.2.1. *Every number larger than one has a prime divisor.*

Theorem 1.2.2. *There are infinitely many prime numbers.*

Theorem 1.2.3. *Every number different from* 0 *and not a unit can be decomposed into the product of finitely many primes.*

Definition. For certain number, if it divide a product of numbers, it also divide one of the factors. Numbers of this type that are different from 0 and the units have the *prime property*.

Theorem 1.2.4. *The prime numbers are precisely those with the prime property.*

Theorem 1.2.5 (Fundamental Theorem of Arithmetic)**.** *The prime factorization of a nonzero number that is not a unit is unique up to the order and signs of the factors.*

Proposition. If $a_1, \cdots, a_j$; $b_1, \cdots, b_k$ are integers such that

$$a_1 a_2 \cdots a_j = b_1 b_2 \cdots b_k$$

then there exists integer t_{uv} $(1 \leqslant u \leqslant j, 1 \leqslant v \leqslant k)$ such that

$$a_u = \prod_{v=1}^{k} t_{uv}, \qquad b_v = \prod_{u=1}^{j} t_{uv}$$

Definition. A number can be written in the form

$$n = e p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

where e is either -1 or $+1$, depending on the sign of n; $p_1 \cdots p_r$ are positive distinct prime numbers; and α_i are positive integral exponents. If this also includes primes to the power of 0, it will be called a *canonical decomposition.*

1.3 Divisors, Multiples, and Common Divisors and Multiples

Definition. The *multiples* of n are those numbers that have n as a divisor.

Theorem 1.3.1. *The number n given its canonical decomposition*

$$n = \prod_{i=1}^{r} p_k^{k_i}$$

has divisors given by

$$a = \prod_{i=1}^{r} p_i^{j_i}, \quad \textit{whre} \quad 0 \leqslant j_i \leqslant k_i \quad (1 \leqslant i \leqslant r)$$

multiples given by

$$t = \prod_{i=1}^{u} p_i^{s_i}, \quad \textit{where} \quad u \geqslant r, \quad \textit{and} \quad k_i \leqslant s_i \quad \textit{for} \quad 1 \leqslant i \leqslant r$$

and the number of its divisors given by

$$\tau(n) = \prod_{i=1}^{r} (k_i + 1)$$

Definition. The number whose divisors are exactly all the common divisors of a series of integers is called *distinguished common divisor*. The number that is a multiple of a series of integers and a divisor of all their common multiples is called *distinguished common multiple*.

Theorem 1.3.2. *The distinguished common divisor of the numbers*

$$n_i = \prod_{h=1}^{r} p_h^{k_{ih}}, \quad i = 1, 2, \cdots, s$$

is

$$D = \prod_{h=1}^{r} p_h^{m_h}, \quad \text{where} \quad m_h = \min(k_{1h}, k_{2h}, \cdots, k_{sh}), \quad 1 \leqslant h \leqslant r$$

the distinguished common multiple is

$$t = \prod_{h=1}^{r} p_h^{M_h}, \quad \text{where} \quad M_h = \max(k_{1h}, k_{2h}, \cdots, k_{sh}), \quad 1 \leqslant h \leqslant r$$

If some of the n_i are 0, then they are ignored in the case of the distinguished common divisor, unless all of the n_i are 0, in which case the distinguished common divisor is also 0. If at least one of the n_i is 0, then the distinguished common multiple is 0.
Both the distinguished common divisor and the distinguished common multiple are uniquely defined.
The distinguished common divisor is equal to the greatest common divisor if the latter exists, and the distinguished common multiple is equal to the least common multiple.
When considering distinguished common multiples and divisors where n_i can be arbitrary integers, we use the absolute values of the numbers.

The greatest common divisor is abbreviated as $g.c.d$(denoted $(n_1, n_2, \cdots, n_r)$) and the least common multiple is abbreviated as $l.c.m$(denoted $[n_1, n_2, \cdots, n_r]$). Unless otherwise stated, these two terms are used to refer to the distinguished ones.

***Example* 1.3.** *$n_1, n_2, \cdots, n_r$ are relatively prime if*

$$(n_1, n_2, \cdots, n_r) = 1$$

Theorem 1.3.3. *If a positive integer is not a kth power, then its kth root is irrational.*

Theorem 1.3.4. *The canonical decomposition of $n!$ is*

$$n! = \prod_{p \leqslant n} p^{k(n,p)}, \quad \text{where} \quad k(n,p) = \sum_{t=1}^{r} [\frac{n}{p^t}]$$

The product is over all primes not larger than n, and $r = r(n,p)$ is such that

$$q^r \leqslant n < p^{r+1}$$

Proof. Left for Exercise □

Theorem 1.3.5. *The canonical decomposition of the binomial coefficient $\binom{n}{j} = \frac{n!}{j!(n-j)!}$ is*

$$\binom{n}{j} = \prod_{p \leqslant n} p^h, \quad h = \sum_{t=1}^{r} ([\frac{n}{p^t}] = [\frac{j}{p^t}] - [\frac{n-j}{p^t}]),$$

where $r = r(n,p)$ satisfies $p^r \leqslant n < p^{r+1}$.

1.4 Pythagorean Triples

Theorem 1.4.1. *The number preceding the square of an off integer is divisible by 8. that is, if n is odd,*

$$n^2 - 1 = 4(\frac{n-1}{2})(\frac{n+1}{2})$$

Definition. Numbers satisfying

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

are called *Pythagorean triples.* If a Pythagorean triple is relatively prime, it's called a *primitive triple.*

Theorem 1.4.2. *All Pythagorean triples are of the form*

$$x = 2sab, \quad y = s(a^2 - b^2), \quad z = s(a^2 + b^2)$$

where s, a, and b are positive integers, a and b are relatively prime, one of them is even, and $a > b$(omit this if considering the absolute value of y, since this condition is necessary for y to be positive).
The primitive triples are those for which $s = 1$.

Proof. Left for Exercise □

Theorem 1.4.3. *If a and b are integers, then the sum*

$$a^2 + b^2$$

cannot have a positive divisor of the form $4k - 1$ relatively prime to a and b.

Definition. A proof by *infinite descent* is a particular kind of proof by contradiction that relies on the least integer principle. One typical application is to show that a given equation has no solutions.

Typically, one shows that if a solution to a problem existed, which in some sense was related to one or more natural numbers, it would necessarily imply that a second solution existed, which was related to one or more 'smaller' natural numbers. This in turn would imply a third solution related to smaller natural numbers, implying a fourth solution, therefore a fifth solution, and so on. However, there cannot be an infinity of ever-smaller natural numbers, and therefore by mathematical induction (repeating the same step) the original premise—that any solution exists— is incorrect: its correctness produces a contradiction.

Proof. Assume that there exists a positive number of the form $4k-1$ that has a multiple that is the sum of two squares a^2+b^2, where the bases of the squares are both relatively prime to the number. Let c be the smallest such number and call the multiple $a_1^2+b_1^2$, where

$$(c,a_1)=(c,b_1)=1$$

The number a_1 and b_1 are at a distance of at most $c/2$ from the closest multiple of the odd number c. Therefore, there exist integers q,r,a_2,b_2 such that

$$a_1=cq+a_2,\quad |a_2|\leqslant\frac{c}{2},\quad b_1=cr+b_2,\quad |b_2|\leqslant\frac{c}{2}$$

by the fact that they are relatively prime, a_2 and b_2 are nonzero. Then

$$a_1^2+b_1^2=c(cq^2+cr^2+2qa_2+2rb_2)+(a_2^2+b_2^2)$$

Since the left-hand side and the first term of the right-hand side are divisible by c, we have that $(a_2^2+b_2^2)$ is divisible by c. Here we also have that $(a_2,c)=(b_2,c)=1$.

Let d be the g.c.d of a_2 and b_2. Then

$$a_2=da_3,\quad b_2=db_3,\quad (a_3,b_3)=1$$

It follows that $(c,d)=1$ and $c|d^2(a_3^2+b_3^2)(d^2(a_3^2+b_3^2)$ is divisible by c). It is obvious that

$$|a_3|\leqslant|a_2|,\quad |b_3|\leqslant|b_2|$$

then

$$a_3^2+b_3^2\leqslant a_2^2+b_2^2\leqslant\frac{c^2}{4}+\frac{c^2}{4}<c^2$$

Then there is a positive integer c' such that

$$cc'=a_3^2+b_3^2<c^2;\quad c'<c$$

Since $(a_3, b_3) = 1$, at least one of them is odd, and $a_3^2 + b_3^2$ is of the form $4m + 1$ or $8m + 2$.
Additionally c' is relatively prime to the two squares.
In conclusion, the existence of c' contradicts the fact that c is the smallest such number. □

Theorem 1.4.4. *If the integers $a_1, a_2, \cdots, a_r$ have a distinguished common divisor, then it is unique, and can be written as*

$$\sum_{i=1}^{r} a_i u_i$$

where $u_1, u_2, \cdots, u_r$ are integers.

If c is such that $ca_1, ca_2, \cdots, ca_r$ are integers, then the distinguished common divisor of these is $|c|$ times the distinguished common divisor of the a_i's.

Theorem 1.4.5 (The Euclidean Algorithm for the case of two numbers)**.** *Let a and b be integers. If one is zero, then the other is the distinguished common divisor. If neither is zero, then we divide a by b, with remainder. If the remainder is not zero, we divide b by the remainder, then the old remainder by the new one, and so on. This procedure must terminate, since the remainders are nonnegative decreasing integers. In this way we get the following formulation:*

$$\begin{aligned}
a &= bq_1 + r_1, && 0 < r_1 < |b| \\
b &= r_1 q_2 + r_2, && 0 < r_2 < r_1 \\
r_{j-1} &= r_j q_j + r_{j+1}, && 0 < r_{j+1} < r_j, \quad j = 2, 3, \cdots, n-1 \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

and $(a, b) = r_n$.

Theorem 1.4.6. *If an indecomposable number is a divisor of a product, then it is a divisor of one of the factors.*

Proof. Left for Exercise □

1.5 First-order Diophantine equations

Theorem 1.5.1 (First-order Diophantine equations with two unknowns)**.** *The equation*

$$ax + by = c$$

has given integer a, b, and c. The goal is to find integers x and y satisfying it. The problem has solution iff

$$(a, b) | c$$

If this is satisfied and x_0, y_0 is a solution to it, then all solutions are given by the formula

$$x' = x_0 - \frac{wb}{(a,b)}, \quad y' = y_0 + \frac{wa}{(a,b)}$$

where w is any integer. We can find a solution with the help of the Euclidean algorithm.

2

Congruences

2.1 Congruences

Definition. We say that a is *congruent to b modulo m(or just mod m)* if a and b have the same remainder when divided by m(or by an equivalent statement, if $a-b$ is divisible by m). This is denoted $a \equiv b \pmod{m}$. If two numbers that are not congruent are called *incongruent*, and denoted $a \not\equiv b \pmod{m}$. Congruence is a equivalence relationship.

***Example* 2.1.** *$m|a$ is equivalent to the expression*

$$a \equiv 0 \pmod{m}$$

Definition. $a \equiv b \pmod{0}$ is the same as $a = b$.

***Example* 2.2.** *Congruence modulo 1 is not very useful for integers, since in that case all integers are congruent. However, for the real numbers, this says that the fractional parts of the two numbers are equal, and this notation is often used.*

Theorem 2.1.1. *If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, k is an integer and $(k, m) = 1$, then*

- *If $kc = bk \pmod{m}$, then $a \equiv b \pmod{m}$, provided $(k, m) = 1$;*
- *$a \pm c \equiv b \pm d \pmod{m}$;*
- *$ac \equiv bd \pmod{m}$.*

That is, adding, subtracting, and multiplying congruent numbers with respect to the same mudulus maintains congruence. Moreover, we have

- *If n is a positive integer, then $a^n \equiv b^n \pmod{m}$;*
- *If $f(x)$ is a polynomial with integer coefficients, then $f(a) \equiv f(b) \pmod{m}$;*

- *If* $a \equiv b \pmod{mm'}$ *and* $m' \neq 0$, *then* $a \equiv b \pmod{m}$.

***Example* 2.3.** *We see that*

$$10 \equiv 1 \pmod{9}, \qquad 10 \equiv -1 \pmod{11}$$

Then for integers $a_0, \cdots, a_n$

$$\sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \pmod{9}, \qquad \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} (-1)^i a_i \pmod{9}$$

2.2 Residue Classes and Systems

Definition. If we choose an arbitrary integer and form a class consists of elements that are congruent modulo m to it and denoted by $(a)_m$, where a is an element of this class, then it is clear that no two arbitrary classes have a common element if they are not the same class. These classes are called the *residue classes modulo* m.

Theorem 2.2.1. *For all integers in a residue class modulo* m *their g.c.d with* m *are the same.*

Proof. If $a \equiv b \pmod{m}$ and $(b, m) = d$, then $a \equiv b \equiv 0 \pmod{d}$, i.e., $d|a$. Since $(b, m)|m$, we have that

$$(b, m)|(a, m)$$

and by the commutativity of modulus and let $(a, m) = k$, we have

$$(a, m)|(b, m)$$

then we have

$$(a, m) = (b, m)$$

□

Definition. A set that contains exactly one element from every residue class modulo m is called a *complete residue system modulo* m.

Theorem 2.2.2. *If a set of numbers has* m *elements that are pairwise incongruent modulo* m, *then the set is a complete residue system modulo* m.

Theorem 2.2.3. *If* a *and* m *are relatively prime integers,* b *is an arbitrary integer, and* $r_1, r_2, \cdots, r,$ *is a complete residue system modulo* m, *then*

$$ar_1 + b, ar_2 + b, \cdots, ar_m + b$$

is a complete residue system modulo m.

Definition. If we consider residue classes all corresponding to different moduli, the system of congruences is called *disjoint* if all classes are disjoint and *covering* if the union of all classes is all integers.

Theorem 2.2.4. *In a covering system of congruences, the sum of the reciprocals of the moduli is larger than* 1.

Proof. Left for Exercise □

Definition. For a sequence(finite or infinite) of integers $c_1, c_2, \cdots$, the corresponding function $z^{c_1} + z^{c_2} + \cdots$ is called the *generating function of the series.*

Theorem 2.2.5. *In a covering system of congruences, the sum of the reciprocals of the moduli is larger than* 1.

Proof. Left for Exercise □

Theorem 2.2.6. *For integers a, b, m, the congruence*

$$ax \equiv b \pmod{m}$$

has solutions iff

$$(a, m)|b$$

If this holds, then there are (a, m) residue classes modulo m that satisfy the congruence.

Theorem 2.2.7. *The congruence $ax \equiv b \pmod{m}$ has a solution iff the Diophantine equation*

$$ax - my = b$$

has a solution, and this has a solution iff

$$(a, b)|b$$

If this holds, then the solution of the congruence is a residue class modulo $m/(a, m)$; the solution can be found using the Euclidean algorithm with a and m.

Definition. The general system of congruences

$$a_i x \equiv b_i \pmod{m_i}, \qquad i = 1, 2, \cdots, k$$

is called *simultaneous systems of congruences.*

Theorem 2.2.8. *If a simultaneous systems of congruences has a solution and the conditions $(a_i, m_i) = 1$ are satisfied, then all the solutions form a residue class modulo the least common multiple of the moduli.*

Proof. Left for Exercise □

Theorem 2.2.9 (Chinese Remainder Theorem)**.** *If the moduli in the simultaneous congruence system*

$$a_i x \equiv b_i \pmod{m_i}, \qquad i = 1, 2, \cdots, k$$

are pairwise relatively prime and

$$(a_i, m_i) = 1, \qquad i = 1, 2, \cdots, k$$

then the system has a solution. This solution is a residue class modulo the product of the moduli.

Theorem 2.2.10. *For any given number N, there exists a prime number that is at least N greater than the previous prime number and at least N smaller than the following one.*

Theorem 2.2.11 (Dirichlet's Theorem)**.** *If a and m are integers, relatively prime to each other, then there are infinitely many positive integers k such that $a + km$ is prime.*

Proof. Left for Exercise □

2.3 Reduced Residue Systems

Definition. A set of representatives, one from each class relatively prime to the modulus, is called a *reduced residue system* and denoted by $\varphi(m)$, the number of residue classes relatively prime to m.

Definition. The *Euler's φ-function* is defined as follows: $\varphi(m)$ is the number of integers from 0 to $m - 1$ that are relatively prime to m.

Theorem 2.3.1. *For Euler's φ-function,*

$$\sum_{d|n} \varphi(d) = n$$

In other words, the summation of the values of the φ-function for all divisors d of n equals to n.

Proof. Left for Exercise □

Theorem 2.3.2. *If $\varphi(m)$ integers are relatively prime to m and are pairwise incongruent modulo m, then they form a reduced residue system modulo m.*

Theorem 2.3.3 (Euler-Fermat Theorem)**.** *If m is an integer greater than 1 and a is an integer relatively prime to m, then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Proof. Let m be an integer greater than 1, a an integer relatively prime to m, and $r_1, r_2, \cdots, r_{\varphi(m)}$ a reduced residue system modulo m. Then by the former theorem

$$ar_1, ar_2, \cdots, ar_{\varphi(m)} \tag{2.1}$$

is a reduced residue system, since each of it is a product of two integers relatively prime to m and it has $\varphi(m)$ elements that are relatively prime to m. For each element there is exactly one element congruent to it from the original system.

$$ar_i \equiv r_{j_i} \pmod{m}, \quad i = 1, 2, \cdots, \varphi(m)$$

Here $j_1, j_2, \cdots, c_{\varphi(m)}$ is a permutation of $1, 2, \cdots, \varphi(m)$(since a and r_i are both relatively prime to m, then their product must be relatively prime to m, and thus congruent to only one other element in the original reduced residue system). Now multiply all the left sides together and all the right sides together

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}$$

and since $(r_1 r_2 \cdots r_{\varphi(m)}, m) = 1$, divide the congruence equation by $r_1 r_2 \cdots r_{\varphi(m)}$, and our proof is complete. □

Theorem 2.3.4 (Fermat's Theorem)**.** *If p is a prime and $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}$$

or equivalently,

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

***Example* 2.4.** *We can now solve the congruence $ax \equiv b \pmod{m}$ where $(a, m) = 1$. We have*

$$x \equiv a^{\varphi(m)-1} b \pmod{m}$$

and the solution of it is the residue class

$$(a^{\varphi(m)-1} b)_m$$

Definition. The smallest exponent of a number c for which c raised to this exponent is congruent to 1 modulo m the *order of c modulo m*. By the Euler-Fermat theorem, there exists such exponent, like $\varphi(m)$, but the smallest such exponent could be smaller than $\varphi(m)$.

2.4 Polynomial and Congruences

Theorem 2.4.1. *If the coefficients of a polynomial $f(x)$ are not all congruent to 0 modulo m and $f(a) \equiv 0 \pmod{m}$, then there exists a polynomial $g(x)$ such that*

$$f(x) \equiv (x-a)g(x) \pmod{m}$$

for all x and the degree of g is one less than the degree of f.

Proof. Consider the polynomial $F(x) = f(x+a)$, whose constant term is c_0. Then it can be written as

$$F(x) = c_0 + xG(x)$$

where $G(x)$ is of degree $n-1$, and it follows that

$$F(0) = c_0 = f(a) \equiv 0 \pmod{m}$$

Returning to f, we have

$$f(x) = F(x-a) = c_0 + (x-a)G(x-a) \equiv (x-a)G(x-a) \pmod{m}$$

Hence letting $g(x) = G(x-a)$, we have found such a polynomial g satisfying the claim. □

Theorem 2.4.2. *For a prime modulus, a nonzero polynomial cannot have more(residue classes as) roots than the degree of the polynomial.*

Proof. The theorem is true for degree one polynomials. Let p be a prime, k an integer greater than 1, and assume that the theorem is true for polynomials of degree $k-1$. If $f(x)$ is a polynomial of degree k and

$$f(x) \equiv 0 \pmod{m}$$

has no solution for an integer x, or the elements of only one residue class satisfy the congruence, then the theorem is true for f as well. If the congruence holds for a and b (from different residue classes) modulo p, then there is a polynomial g of degree $k-1$ for which

$$f(x) \equiv (x-a)g(x) \pmod{p}$$

Substituting in b, we have

$$(b-a)g(b) \equiv 0 \pmod{p}$$

The first factor is not congruent to 0(since if so they would have been came from the same residue class), and there fore by the prime property, the second factor is divisible by p. Therefore, every solution of $f(x) \equiv 0 \pmod{m}$ not congruent to a modulo p is a solution of

$$g(x) \equiv 0 \pmod{p}$$

The polynomial g is of degree $k-1$, and by induction it has at most $k-1$ roots, so f can have at most k roots. □

Theorem 2.4.3 (Wilson's Theorem)**.** *If p is a prime number, then*

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

Proof. For $p = 2$, the statement is clearly true, and we may assume p to be an odd prime. The degree of the polynomial

$$(x-1)(x-2)(x-(p-1)) - (x^{p-1}-1) = a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_0$$

if it exists, is at most $p-2$, since the term of degree $p-1$ cancels out. However, this polynomial has $p-1$ distinct roots, and the second term $(x^{p-1}-1)$ is congruent to 0 modulo p by Fermats' theorem. Therefore, their difference is congruent to 0 modulo p, which is possible only if the polynomial on the right-hand side is the zero polynomial, *i.e.* $x = 0$(if not so this polynomial will have more roots than the degree of this polynomial). Substituting this into the congruence, we get

$$a_0 = (-1)^{p-1}(p-1)! - (-1) = (p-1)! + 1 \equiv 0 \pmod{p}$$

Alternatively, the polynomial on the right is congruent to 0 modulo p means that

$$a_{p-2} \equiv a_{p-3} \equiv \cdots \equiv a_1 \equiv a_0 \equiv 0 \pmod{p}$$

and Wilson's theorem follows from $a_0 \equiv 0 \pmod{p}$. □

Theorem 2.4.4. *For all primes p of the form $4k+1$, there exists an integer c for which*

$$c^2 + 1 \equiv 0 \pmod{p}$$

Theorem 2.4.5. *If p is an odd prime and $k|p-1$, then the congruence*

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

has k roots.

Proof. If $k|(p-1)$, then the polynomial $x^{p-1}-1$ factors into

$$x^{p-1} - 1 = (x^k - 1)g(x)$$

where $g(x)$ is some polynomial of degree $p-1-k$. By Fermat's theorem, the left side has $p-1$ roots modulo p. Since the modulus is prime, the right-hand side can be congruent to 0 modulo p iff one of its factors is congruent to 0. The first factor has at most k roots and the second at most $p-1-k$ roots.If one of these factors had fewer than this many, then their product would have fewer than $p-1$ roots. Therefore, both factors have their maximum number of roots. □

2.5 Properties of the Order of an Element

Theorem 2.5.1. *If a number c has order n modulo m, then the numbers $1, c, c^2, \cdots, c^{n-1}$ are pairwise incongruent modulo m. If*

$$c^u \equiv c^v \pmod{m}, \quad \textit{then} \quad u \equiv v \pmod{n}$$

In the special case where $v = 0$, then $n|u$.

Proof. The first part follows from the Euler-Fermat theorem that $n|\varphi(m)$. Now we prove the second part. Without loss of generality, we may assume that $u \geqslant v$. Then $c^{u-v} \equiv 1 \pmod{m}$. Dividing $u - v$ by n with remainder we get

$$u - v = nq + z$$

where q is an integer and $0 \leqslant s < n$. We have

$$c^{u-v} = (c^n)^q c^s \equiv c^s \equiv 1 \pmod{m}$$

Among the positive integral powers of c the nth is the first that is congruent to 1 modulo m. Therefore, $s = 0$, and hence $n|u - v$. □

Definition. The numbers that have order $\varphi(m)$ are called *primitive roots of congruence modulo m*. If for a given modulus m there exists a primitive root g, then for every c that is relatively prime to m, the smallest nonnegative exponent k for which

$$c \equiv g^k \pmod{p}$$

is called the *index(with respect to g) of c modulo m.*

Theorem 2.5.2. *The number of elements of order n modulo a prime p is $\varphi(n)$ if $n|p-1$; otherwise, it is 0. Based on this, there are $\varphi(p-1)$ primitive roots modulo p.*

Proof. By the previous theorem, for an arbitrary $m > 0$ it follows that only divisors of $\varphi(m)$ can possibly occur as orders of elements, which proves the second claim.

Left for Exercise □

2.6 Some Properties of the Euler Function

Definition. A function f defined on the positive integers is called *multiplicative* if for all pairs of relatively prime integers a and b, it satisfies $f(ab) = f(a)f(b)$. If this is satisfied for all a and b, then the function is called *totally* or *completely multiplicative.*

Theorem 2.6.1. *Euler's φ-function is multiplicative.*

Proof. Left for Exercise □

Definition. If the congruence

$$x^2 \equiv c \pmod{p}$$

has a solution, then we say that c is a *quadratic residue* modulo p. If there is no solution, then it is called a *quadratic nonresidue*. Whether or not a number is a quadratic residue is called c's *quadratic character*.

Theorem 2.6.2. *The product of two numbers is a quadratic residue if both of the factors are quadratic residues or if both are nonresidues; the product is a quadratic nonresidue if one of the factors is a quadratic residue and the other is a nonresidue. Using the Legendre symbol, the theorem can be restated as*

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

Proof. Left for Exercise □

Definition. The function, written $(\frac{c}{p})$, called the *Legendre symbol*, is defined as follows: its value is 1 if c is a quadratic residue modulo p, -1 if c is a quadratic nonresidue, and 0 if c is divisible by p.

Theorem 2.6.3 (Euler's Lemma)**.** *If p is an odd prime, then for every c,*

$$(\frac{c}{p}) \equiv c^{(p-1)/2} \pmod{p}$$

Proof. Left for Exercise □

Lemma (Gauss's Lemma)**.** *Let p be an odd prime and c an integer not divisible by p. Consider the number of residues of smallest absolute value of the numbers $c, 2c, \cdots, ((p-1)/2)c$ that are negative. Then c is a residue or nonresidue according to whether this number is even or odd, respectively.*

Lemma. *The number -3 is a quadratic residue for primes of the form $6k+1$ and a nonresidue for primes of the form $6p-1$.*

Theorem 2.6.4. *For a positive number c, whether or not it is a quadratic residue modulo a prime depends only on the residue of the prime modulo $4c$; furthermore, those primes with residues r and $4c-r$ agree, or more simply, whose with residues r and $-r$ agree.*

Theorem 2.6.5 (Reciprocity Theorem)**.** *If p and q are distinct odd primes, then*

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

Theorem 2.6.6. *For p a positive odd prime*

$$(\frac{-1}{p}) = (-1)^{(p-1)/2}, \qquad (\frac{2}{p}) = (-1)^{(p^2-1)/8}$$

3

Rational and Irrational Numbers. Approximation of Numbers by Rational Numbers (Diophantine Approximation)

4

Geometric Methods in Number Theory

5

Properties of Prime Numbers

6

Sequences of Integers

7

Diophantine Problems

8

Arithmetic Functions