Number Theory

Dr. Sanhan M. S. Khasraw

Salahaddin University-Erbil
College of Education
Department of Mathematics

Fourth Year
Spring 2022-2023

1 Some Preliminary Considerations

Well-Ordering Priciple. Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that $a \leq b$ for all b belonging to S.

Theorem 1.1. ***(Archimedean Property)***
If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$.

Theorem 1.2. ***(Principle of Finite Induction)***
Let S be a set of positive integers with the following properties:

(i) 1 belongs to S, and

(ii) Whenever the integer k is in S, the next integer $k+1$ must also be in S.

Then S is the set of all positive integers.

Definition 1.3. *For any positive integer n and any integer k satisfying $0 \leq k \leq n$, the **binomial coefficients** are defined by*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Theorem 1.4. ***(Pascal's Rule)***
For $1 \leq k \leq n$,

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

2 Divisibility Theory in the Integers

"Integral numbers are the fountainhead of all mathematics".
H. MINKOWSKI

2.1 THE DIVISION ALGORITHM

Theorem 2.1. ***(Division Algorithm).*** *Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying*

$$a = qb + r, \qquad 0 \leq r < b.$$

The integers q and r are called, respectively, the ***quotient*** *and* ***remainder*** *in the division of a by b.*

Corollary 2.2. *If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that*

$$a = qb + r, \qquad 0 \leq r < |b|.$$

Definition 2.3. *An integer n is* ***even*** *if $n = 2k$ for some k, and is* ***odd*** *if $n = 2k + 1$ for some k.*

Example 2.4. *The square of an integer leaves the remainder 0 or 1 upon division by 4.*

2.2 THE GREATEST COMMON DIVISOR

Definition 2.5. *An integer b is said to be* ***divisible*** *by an integer $a \neq 0$, in symbols $a \mid b$, if there exits some integer c such that*

$$b = ac.$$

We write $a \nmid b$ to indicate that b is not divisible by a.

Example 2.6. .

(1) $3 \mid 12$,

(2) $3 \nmid 10$.

Theorem 2.7. *For integers a, b, c, d, the following hold:*

1. $a \mid 0, \;\; 1 \mid a, \;\; a \mid a$.
2. $a \mid 1$ *if and only if* $a = \pm 1$.
3. *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
4. *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
5. $a \mid b$ *and* $b \mid a$ *if and only if* $a = \pm b$.
6. *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.
7. *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for arbitrary integers* x *and* y.

Definition 2.8. *If a and b are arbitrary integers, then an integer d is said to be a* ***common divisor*** *of a and b if both $d \mid a$ and $d \mid b$.*

Definition 2.9. *Let a and b be given integers, with at least one of them different form zero. The* ***greatest common divisor*** *of a and b, dented by* ***gcd(a, b)****, is the positive integer d satisfying*

1. *$d \mid a$ and $d \mid b$,*
2. *if $c \mid a \quad$ and $\quad c \mid b$, then $c \leq d$.*

Example 2.10. *The positive divisors of -12 are $1, 2, 3, 4, 6, 12$, while those of 30 are $1, 2, 3, 5, 6, 10, 15, 30$, hence, the positive common divisors of -12 and 30 are* ***1, 2, 3, 6****.*
Since ***6*** *is the largest of these integers, it follows that $gcd(-12, 30) = 6$.*

Example 2.11. $gcd(-5, 5) = 5, \quad gcd(8, 15) = 1, \quad gcd(-8, -36) = 4.$

Theorem 2.12. *Given integers a and b, not both of which are zero, there exist integers x and y such that*

$$gcd(a, b) = ax + by.$$

Corollary 2.13. *If a and b are given integers, not both zero, then the set $T = \{ax + by \mid x, y \text{ are integers}\}$ is precisely the set of all multiples of $d = gcd(a, b)$.*

Example 2.14.

$$gcd(-12, 30) = 6 = (-12) \cdot 2 + (30) \cdot 1,$$

$$gcd(-8, -36) = 4 = (-8) \cdot 4 + (-36) \cdot (-1).$$

Definition 2.15. *Two integers a and b, not both of which are zero, are said to be **relatively prime** whenever $gcd(a, b) = 1$.*

Example 2.16. *Since $gcd(8, 15) = 1$, then 8 and 15 are relatively prime.*

Theorem 2.17. *Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.*

Corollary 2.18. *If $gcd(a, b) = d$, then $gcd(a/d, b/d) = 1$.*

Example 2.19. $gcd(-12, 30) = 6$ *and* $gcd(-12/6, 30/6) = gcd(-2, 5) = 1$.

Remark 2.20. *It is not true, without adding an extra condition, that* $a \mid c$ *and* $b \mid c$ *together give* $ab \mid c$*. For instance,* $10 \mid 30$ *and* $15 \mid 30$*, but* $10 \cdot 15 \nmid 30$.

Corollary 2.21. *If* $a \mid c$ *and* $b \mid c$*, with* $gcd(a, b) = 1$*, then* $ab \mid c$.

Theorem 2.22. ***(Euclid's Lemma)*** *If* $a \mid bc$*, with* $gcd(a, b) = 1$*, then* $a \mid c$.

Remark 2.23. *If* a *and* b *are not relatively prime, then the conclusion of Euclid's Lemma may fail to hold. For example,* $10 \mid 5 \cdot 6$ *but* $10 \nmid 5$ *and* $10 \nmid 6$.

Theorem 2.24. *Let a, b be integers, not both zero. For a positive integer d, $d = gcd(a, b)$ if and only if*

1. *$d \mid a$ and $d \mid b$,*

2. *whenever $c \mid a$ and $c \mid b$, then $c \mid d$.*

2.3 THE EUCLIDEAN ALGORITHM

Lemma 2.25. *If $a = qb + r$, then $gcd(a, b) = gcd(b, r)$.*

The Euclidean Algorithm.

Example 2.26. *Find* $gcd(195, 70)$.

Example 2.27. *Find* $gcd(295, 140)$ *and* $gcd(12378, 3054)$.

Theorem 2.28. *If* $k>0$, *then* $gcd(ka, kb) = k\ gcd(a, b)$.

Corollary 2.29. *For any integer* $k \neq 0$, $gcd(ka, kb) = |k|gcd(a, b)$.

Example 2.30. $gcd(12, 30) = 3\ gcd(4, 10) = 3 \cdot 2\ gcd(2, 5) = 6 \cdot 1 = 6.$

Definition 2.31. *The **least common multiple** of two nonzero integers a and b, denoted by* $lcm(a, b)$*, is the positive integer m satisfying*

1. $a \mid m$ *and* $b \mid m$,
2. $a \mid c$ *and* $b \mid c$, *with* $c>0$, *then* $m \leq c$.

Example 2.32. $lcm(-12, 30) = 60$.

Theorem 2.33. *For positive integers a and b,*

$$gcd(a, b) \cdot lcm(a, b) = ab.$$

Corollary 2.34. *Given positive integers a and b,* $lcm(a, b) = ab$ *if and only if* $gcd(a, b) = 1$.

2.4 THE DIOPHANTINE EQUATION $ax + by = c$

Definition 2.35. *Any equation in one or more unknowns which is to be solved in integers is called* ***Diophantine equation****.*

The linear Diophantine equation in two unknowns is of the form

$$ax + by = c,$$

where a, b, c are given integers and a, b not both zero.

A solution of this equation is a pair of integers x_0, y_0 which satisfy it.

Example 2.36. *The equation $3x + 6y = 18$ has solutions*

$$3.4 + 6.1 = 18,$$

$$3(-6) + 6.6 = 18,$$

$$3.10 + 6(-2) = 18.$$

Example 2.37. *The equation $4x + 18y = 11$ has no solution.*

Theorem 2.38. *The linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by*

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t$$

for varying integers t.

Example 2.39. *Solve the linear Diophantine equation*

$$172x + 20y = 1000.$$

Example 2.40. *Solve the following linear Diophantine equations*

1. $24x + 138y = 18$,
2. $56x + 72y = 40$.

Corollary 2.41. *If* $gcd(a, b) = 1$ *and if* x_0, y_0 *is a particular solution of the linear Diophantine equation* $ax + by = c$*, then all solutions are given by*

$$x = x_0 + bt, \quad y = y_0 - at$$

for integral values of t*.*

3 Primes and their Distribution

Definition 3.1. *An integer $p>1$ is called a **prime number**, or a **prime**, if its only positive divisors are 1 and p. An integer greater than 1 which is not a prime is called **composite**.*

Theorem 3.2. *If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Corollary 3.3. *If p is a prime and $p|a_1 a_2 \cdots a_n$, then $p|a_k$ for some k, where $1 \leq k \leq n$.*

Corollary 3.4. *If $p, q_1, q_2, \cdots, q_n$ are all primes and $p|q_1 q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.*

Theorem 3.5 (**Fundamental Theorem of Arithmetic**). *Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.*

Of course, several of the primes that appear in the factorization of a given positive integer may be repeated, as is the case with

$$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5.$$

By collecting like primes and replacing them by a single factor, we can rephrase Theorem 3.5 as a corollary.

Corollary 3.6. *Any positive integer $n > 1$ can be written uniquely in a* ***canonical form***

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where, for $i = 1, 2, ..., r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r \cdot$

Example 3.7.

$$360 = 2^3 \cdot 3^2 \cdot 5,$$

$$4725 = 3^3 \cdot 5^2 \cdot 7,$$

$$17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2.$$

Prime factorizations provide another means of calculating greatest common divisors. For suppose that $p_1, p_2, \cdots, p_n$ are the distinct primes that divide either of a or b. Allowing zero exponents, we can write

$$a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \quad b = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n}$$

Then

$$gcd(a, b) = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$$

where $r_i = min(k_i, j_i)$, the smaller of the two exponents associated with p_i in the two representations.

Example 3.8.

$$4725 = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7, \quad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

and so

$$gcd(4725, 17460) = 2^0 \cdot 3^2 \cdot 5 \cdot 7 = 315.$$

Theorem 3.9 (**Pythagoras**). *The number* $\sqrt{2}$ *is irrational.*

Theorem 3.10 (**Euclid**). *There is an infinite number of primes.*

Theorem 3.11. *If* p_n *is the nth prime number, then* $p_n \leq 2^{2^{n-1}}$.

Corollary 3.12. *For* $n \geq 1$*, there are at least* $n+1$ *primes less than* 2^{2^n}.

Lemma 3.13. *The product of two or more integers of the form* $4n + 1$ *is of the same form.*

Theorem 3.14. *There are an infinite number of primes of the form* $4n + 3$.

4 The Theory of Congruences

4.1 CARL FRIEDRICH GAUSS

A short background about the German mathematician Carl Friedrich Gauss (1777-1855).

4.2 BASIC PROPERTIES OF CONGRUENCE

Definition 4.1. *Let n be a fixed positive integer. Two integers a and b are said to be* ***congruent modulo*** *n, symbolized by*

$$a \equiv b \ (mod\ n)$$

if n divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer k.
When $n \nmid (a - b)$, we say that a ***is incongruent to*** *b* ***modulo*** *n, and in this case we write $a \not\equiv b \ (mod\ n)$.*

Example 4.2. *To fix the idea, consider $n = 7$.*

(1) $3 \equiv 24 \ (mod\ 7)$,

(2) $25 \not\equiv 12 \ (mod\ 7)$.

Theorem 4.3. *For arbitrary integers a and b, $a \equiv b \ (mod\ n)$ if and only if a and b leave the same nonnegative remainder when divided by n.*

Theorem 4.4. *Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:*

(1) $a \equiv a \ (mod\ n)$.

(2) *If* $a \equiv b \ (mod\ n)$, *then* $b \equiv a \ (mod\ n)$.

(3) *If* $a \equiv b \ (mod\ n)$ *and* $b \equiv c \ (mod\ n)$, *then* $a \equiv c \ (mod\ n)$.

(4) *If* $a \equiv b \ (mod\ n)$ *and* $c \equiv d \ (mod\ n)$, *then* $a + c \equiv b + d \ (mod\ n)$ *and* $ac \equiv bd \ (mod\ n)$.

(5) *If* $a \equiv b \ (mod\ n)$, *then* $a + c \equiv b + c \ (mod\ n)$ *and* $ac \equiv bc \ (mod\ n)$.

(6) *If* $a \equiv b \ (mod\ n)$, *then* $a^k \equiv b^k \ (mod\ n)$ *for any positive integer* k.

Example 4.5. *Show that* 41 *divides* $2^{20} - 1$.

Example 4.6. *Find the remainder when the sum*

$$1! + 2! + 3! + 4! + \cdots + 99! + 100!$$

is divided by 12.

Theorem 4.7. *If* $ca \equiv cb \ (mod\ n)$*, then* $a \equiv b \ (mod\ n/d)$*, where* $d = gcd(c, n)$*.*

Corollary 4.8. *If* $ca \equiv cb \ (mod\ n)$ *and* $gcd(c, n) = 1$*, then* $a \equiv b \ (mod\ n)$*.*

Corollary 4.9. *If* $ca \equiv cb \ (mod\ p)$ *and* $p \nmid c$*, where* p *is a prime number, then* $a \equiv b \ (mod\ p)$*.*

4.3 SPECIAL DIVISIBILITY TEST

Given an integer $b > 1$, any positive integer N can be written uniquely in terms of powers of b as

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots a_2 b^2 + a_1 b + a_0,$$

where the coefficients a_k can take on the b different values $0, 1, 2, \cdots, b-1$. Thus, the number N may be replaced by the simpler symbol

$$N = (a_m a_{m-1} \cdots a_2 a_1 a_0)_b$$

(the right-hand side is not to be interpreted as a product, but only as an abbreviation for N). We call this the **base** b **place value notation for** N.

When the base $b = 2$, and the resulting system of enumeration is called the **binary number system** (from the Latin **binarius**, two). The fact that when a number is written in the binary system only the integers 0 and 1 can appear as coefficients means that every positive integer is expressible in exactly one way as a sum of distinct powers of 2.

Example 4.10. *The integer* 105 *can be written as*

$$105 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1 = 2^6 + 2^5 + 2^3 + 1$$

or, in abbreviated form,

$$105 = (1101001)_2$$

In the other direction, $(1001111)_2$ translates into

$$1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 79.$$

When $b = 10$, then it is called the **decimal system** (from the Latin **decem**, ten). For example

$$2023 = 2 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10 + 3.$$

Theorem 4.11. *Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b \ (mod\ n)$, then $P(a) \equiv P(b) \ (mod\ n)$.*

Note 4.12. *If $P(x)$ is a polynomial with integral coefficients, we say that a is a solution of the congruence $P(x) \equiv 0 \ (mod\ n)$ if $P(a) \equiv 0 \ (mod\ n)$.*

Corollary 4.13. *If a is a solution of $P(x) \equiv 0 \ (mod\ n)$ and $a \equiv b \ (mod\ n)$, then b also is a solution.*

Example 4.14. *4 is a solution of* $p(x) = x^2 + x + 1 \equiv 0 \ (mod\ 3)$ *and* $4 \equiv 1 \ (mod\ 3)$*, then* 1 *is also a solution of* $p(x)$ *because* $P(4) \equiv P(1) \equiv 0 \ (mod\ 3)$.

Theorem 4.15. *Let* $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots a_2 10^2 + a_1 10 + a_0$ *be the decimal expansion of the positive integer* N*,* $0 \leq a_k < 10$*, and let* $S = a_0 + a_1 + \cdots + a_m$*. Then* $9 \mid N$ *if and only if* $9 \mid S$.

Example 4.16. *The number* $149, 235, 678$ *is divisible by* 9 *because*

$$1 + 4 + 9 + 2 + 3 + 5 + 6 + 7 + 8 = 45$$

is divisible by 9.

Theorem 4.17. *Let* $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots a_2 10^2 + a_1 10 + a_0$ *be the decimal expansion of the positive integer* N*,* $0 \leq a_k < 10$*, and let* $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$*. Then* $11 \mid N$ *if and only if* $11 \mid T$.

Example 4.18. *The number* $1, 571, 724.$ *is divisible by* 11 *because*

$$4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$$

is divisible by 11.

4.4 LINEAR CONGRUENCES

Definition 4.19. *An equation of the form $ax \equiv b \ (mod\ n)$ is called a* ***linear congruence****.*

An integer x_0 is called a solution of $ax \equiv b \ (mod\ n)$ if $ax_0 \equiv b \ (mod\ n)$, that is, $n \mid (ax_0 - b)$.

Theorem 4.20. *The linear congruence $ax \equiv b \ (mod\ n)$ has a solution if and only if $d \mid b$, where $d = gcd(a, n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n.*

Note that the solution of $ax \equiv b \ (mod\ n)$ has the form

$$x = x_0 + \frac{n}{d}t$$

for some choice of t.

Among the various integers satisfying the first of these formulas, consider those that occur when t takes on the successive values $t = 0, 1, 2, \cdots, d-1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \cdots, x_0 + \frac{(d-1)n}{d}.$$

Corollary 4.21. *If $gcd(a, n) = 1$, then the linear congruence $ax \equiv b \ (mod\ n)$ has a unique solution modulo n.*

Example 4.22. *Solve the linear congruence $18x \equiv 30 \ (mod\ 42)$.*

Example 4.23. *Solve the linear congruence* $9x \equiv 21 \ (mod\ 30)$.

Example 4.24. *Solve the linear congruence* $6x \equiv 15 \ (mod\ 21)$.

Theorem 4.25 **(Chinese Remainder Theorem).** *Let* $n_1, n_2, \cdots, n_r$ *be positive integers such that* $gcd(n_i, n_j) = 1$ *for* $i \neq j$. *Then the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \ (mod\ n_1) \\ x &\equiv a_2 \ (mod\ n_2) \\ &\vdots \\ x &\equiv a_r \ (mod\ n_r) \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Example 4.26. *Solve the system*

$$x \equiv 2 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 5)$$
$$x \equiv 2 \ (mod\ 7).$$

Example 4.27. *Solve the system*

$$x \equiv 0 \ (mod\ 3)$$
$$x \equiv 1 \ (mod\ 4)$$
$$x \equiv 9 \ (mod\ 23).$$

5 Fermat's Theorem

5.1 FERMAT'S LITTLE THEOREM

Theorem 5.1 (**Fermat's Little Theorem**). *If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Example 5.2. *Take $a = 2$ and $p = 7$. Then*

Corollary 5.3. *If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.*

Example 5.4. *Show that* $(a+1)^p \equiv a+1$ $(mod\ p)$.

Example 5.5. *Show that* $5^{38} \equiv 4$ $(mod\ 11)$.

Lemma 5.6. *If* p *and* q *are distinct primes such that* $a^p \equiv a$ $(mod\ q)$ *and* $a^q \equiv a$ $(mod\ p)$, *then* $a^{pq} \equiv a$ $(mod\ pq)$.

Example 5.7. $2^{11} \equiv 2$ $(mod\ 31)$ *and* $2^{31} \equiv 2$ $(mod\ 11)$. *Then* $2^{11\cdot 31} \equiv 2$ $(mod\ 11 \cdot 31)$ *or* $2^{341} \equiv 2$ $(mod\ 341)$.

Example 5.8. *Find the units digit of* 3^{100} *by the use of Fermat's Theorem.*

Definition 5.9. *A composite integer* n *is called* ***pseudoprime*** *whenever* $n \mid 2^n - 2$.

The smallest four pseudoprimes are 341, 561, 645, and 1105.

Example 5.10. *Show that* 561 *is a pseudoprime.*

$561 = 3 \cdot 11 \cdot 17$.

5.2 WILSON'S THEOREM

Theorem 5.11 (**Wilson**)**.** *If* p *is a prime, then* $(p-1)! \equiv -1 \ (mod\ p)$.

Example 5.12. *Apply Wilson's Theorem when* $p = 17$.

Solution: It is possible to divide the integers $2, 3, \cdots, 15$ into $(p-3)/2 = 7$ pairs each of whose products is congruent to 1 modulo 17. To write these congruences out explicity:

$$2 \cdot 9 \equiv 1 \ (mod\ 17),$$

$$3 \cdot 6 \equiv 1 \ (mod\ 17),$$
$$4 \cdot 13 \equiv 1 \ (mod\ 17),$$
$$5 \cdot 7 \equiv 1 \ (mod\ 17),$$
$$10 \cdot 12 \equiv 1 \ (mod\ 17),$$
$$8 \cdot 15 \equiv 1 \ (mod\ 17),$$
$$11 \cdot 14 \equiv 1 \ (mod\ 17).$$

Multiplying these congruences gives the result

$$15! = (2 \cdot 9)(3 \cdot 6)(4 \cdot 13)(5 \cdot 7)(10 \cdot 12)(8 \cdot 15)(11 \cdot 14) \equiv 1 \ (mod\ 17)$$

and so

$$16! \equiv 16 \equiv -1 \ (mod\ 17).$$

Theorem 5.13. *The quadratic congruence $x^2 + 1 \equiv 0 \ (mod\ p)$, where p is an odd prime, has a solution if and only if $p \equiv 1 \ (mod\ 4)$.*

p must be of the form $p = 4k + 1$ and $[(p-1)/2]!$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \ (mod\ p)$.

Example 5.14. *Take $p = 13$.*

Example 5.15. *Show that $x^2 + 1 \equiv 0 \ (mod\ 3)$ has no solution.*

6 Number-Theoretic Functions

6.1 The Functions τ and σ

Definition 6.1. *Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors.*

Example 6.2. *Consider $n = 12$. Since 12 has the positive divisors $1, 2, 3, 4, 6, 12$, we find that*

$$\tau(12) = 6 \ \textit{and} \ \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

For the first few integers,

$$\tau(1) = 1, \ \ \tau(2) = 2, \ \ \tau(3) = 2, \ \ \tau(4) = 3, \ \ \tau(5) = 2, \ \ \tau(6) = 4, \cdots$$

and

$$\sigma(1) = 1, \ \ \sigma(2) = 3, \ \ \sigma(3) = 4, \ \ \sigma(4) = 7, \ \ \sigma(5) = 6, \ \ \sigma(6) = 12, \cdots.$$

Remark 6.3.

It is not difficult to see that

1. $\tau(n) = 2$ if and only if n is a prime number.
2. $\sigma(n) = n + 1$ if and only if n is a prime number.

Theorem 6.4. *If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $0 \le a_i \le k_i$ $(i = 1, 2, \cdots, r)$.

Theorem 6.5. *If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then*

(*a*) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$, *and*

(*b*) $\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$.

Example 6.6. *The number* $180 = 2^2 \cdot 3^2 \cdot 5$ *has*

$$\tau(180) = (2+1)(2+1)(1+1) = 18$$

positive divisors. The sum of these integers is

$$\sigma(n) = \frac{2^3-1}{2-1}\,\frac{3^3-1}{3-1}\,\frac{5^2-1}{5-1} = 7 \cdot 13 \cdot 6 = 546.$$

Example 6.7. *Find* $\tau(18)$ *and* $\sigma(18)$*.*

Example 6.8. *Find* $\tau(1575)$ *and* $\sigma(1575)$*, where* $1575 = 3^2 \cdot 5^2 \cdot 7$*.*

Remark 6.9.

$$\tau(2 \cdot 10) = \tau(20) = 6 \neq 2 \cdot 4 = \tau(2) \cdot \tau(10).$$

At the same time,

$$\sigma(2 \cdot 10) = \sigma(20) = 42 \neq 3 \cdot 18 = \sigma(2) \cdot \sigma(10).$$

These calculations bring out the nasty fact that, in general, it need not be true that

$$\tau(mn) = \tau(m)\tau(n) \;\; \textit{and} \;\; \sigma(mn) = \sigma(m)\sigma(n).$$

Definition 6.10. *A number-theoretic function f is said to be **multiplicative** if*

$$f(mn) = f(m)f(n)$$

whenever $gcd(m,n) = 1$.

Remark 6.11. *If f is multiplicative and $n_1, n_2, \cdots, n_r$ are positive integers that are pairwise relatively prime, then*

$$f(n_1 n_2 \cdots n_r) = f(n_1)f(n_2)\cdots f(n_r).$$

Remark 6.12.

Multiplicative functions have one big advantage for us: they are completely determined once their values at prime powers are known. Indeed, if $n > 1$ is a given positive integer, then we can write $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ in canonical form; since the $p_i^{k_i}$ are relatively prime in pairs, the multiplicative property ensures that

$$f(n) = f(p_1^{k_1})f(p_2^{k_2})\cdots f(p_r^{k_r}).$$

If f is a multiplicative function that does not vanish identically, then there exists an integer n such that $f(n) \neq 0$. But

$$f(n) = f(n \cdot 1) = f(n)f(1).$$

Being nonzero, $f(n)$ may be canceled from both sides of this equation to give $f(1) = 1$.

Theorem 6.13. *The functions τ and σ are both multiplicative functions.*

Definition 6.14. *A positive integer n is said to be*

1. *a* ***deficient number*** *if $\sigma(n) < 2n$,*
2. *an* ***abundant number*** *if $\sigma(n) > 2n$,*
3. *a* ***perfect number*** *if $\sigma(n) = 2n$.*

Example 6.15.

6.2 The Mӧbius μ-function.

Definition 6.16. *For a positive integer n, define μ by the rules*

$$\mu(n) = \begin{cases} 1 & if \;\; n = 1 \\ 0 & if \;\; p^2 \mid n \; for \; some \; prime \; p \\ (-1)^r & if \;\; n = p_1 p_2 \cdots p_r, where \; p_i \; are \; distinct \; primes \end{cases}$$

The first few values of μ are

$$\mu(1) = 1, \;\; \mu(2) = -1, \;\; \mu(3) = -1, \;\; \mu(4) = 0, \;\; \mu(5) = -1, \;\; \mu(6) = 1, \cdots.$$

If p is a prime number, it is clear that $\mu(p) = -1$; also, $\mu(p^k) = 0$ for $k \geq 2$.

Theorem 6.17. *The function μ is a multiplicative function.*

Definition 6.18. *The* ***Liouville λ-function*** *is defined by*

$$\lambda(n) = \begin{cases} 1 & if \;\; n = 1 \\ (-1)^{k_1+k_2+\cdots+k_r} & if \;\; n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}. \end{cases}$$

Example 6.19. $\lambda(360) = \lambda(2^3 \cdot 3^2 \cdot 5) = (-1)^{3+2+l} = (-1)^6 = 1.$

Theorem 6.20. *The function λ is a multiplicative function.*

6.3 The Greatest Integer Function

Definition 6.21. *For an arbitrary real number x, we denote by $[x]$ the largest integer less than or equal to x; that is, $[x]$ is the unique integer satisfying $x - 1 < [x] \le x$.*

Example 6.22. *By way of illustration, [ ] assumes the particular values*

$$[-3/2] = -2, \; [\sqrt{2}] = 1, \; [1/3] = 0, \; [\pi] = 3, \; [-\pi] = -4.$$

Note 6.23. *From the Definition 6.21, we observe the following*

1. *$[x] = x$ if and only if x is an integer.*
2. *Any real number x can be written as $x = [x] + \theta$ for a suitable choice of θ, with $0 \le \theta < 1$.*

We now plan to investigate the question of how many times a particular prime p appears in $n!$. For instance, if $p = 3$ and $n = 9$, then

$$\begin{aligned} 9! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \\ &= 2^7 \cdot 3^4 \cdot 5 \cdot 7, \end{aligned}$$

so that the exact power of 3 that divides $9!$ is 4.

Theorem 6.24. *If n is a positive integer and p a prime, then the exponent of the highest power of p that divides $n!$ is*

$$\sum_{k=1}^{\infty} [\frac{n}{p^k}].$$

(This is not an infinite series, since $[n/p^k] = 0$ for $p^k > n$).

Example 6.25. *Find the number of zeros with which the decimal representation of $50!$ terminates.*

Theorem 6.26. *If n and r are positive integers with $1 \leq r < n$, then the binomial coefficient*

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is also an integer.

Corollary 6.27. *For a positive integer r, the product of any r consecutive positive integers is divisible by $r!$.*

Example 6.28. $(n-1)n(n+1)$ *is divisible by* $3! = 6$*. That is,* $n^3 - n$ *is divisible by* 6*.*

7 Euler's Generalization of Fermat's Theorem

7.1 LEONHARD EULER

A short background about the Swiss mathematician Leonhard Euler (1707-1783).

7.2 EULER'S PHI-FUNCTION

Definition 7.1. *For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.*

Example 7.2. *To illustrate the definition,*

1. $\phi(9) = 6$, *and*
2. $\phi(15) = 8$.

For the first few positive integers,

$$\phi(1) = 1,\ \ \phi(2) = 1,\ \ \phi(3) = 2,\ \ \phi(4) = 2,\ \ \phi(5) = 4,\ \ \phi(6) = 2,\ \ \phi(7) = 6, \cdots .$$

Remark 7.3. $\phi(n) = n - 1$ *if and only if n is prime.*

Theorem 7.4. *If p is a prime and $k > 0$, then*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}).$$

Example 7.5. $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$.

Lemma 7.6. *Given integers a, b, c, $gcd(a, bc) = 1$ if and only if $gcd(a, b) = 1$ and $gcd(a, c) = 1$.*

Theorem 7.7. *The function ϕ is a multiplicative function.*

Theorem 7.8. *If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then*

$$\begin{aligned}\phi(n) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r}).\end{aligned}$$

Example 7.9.

To calculate $\phi(360)$. The prime-power decomposition of 360 is $2^3 \cdot 3^2 \cdot 5$. By Theorem 7.8,

$$\begin{aligned}\phi(360) &= 360(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) \\ &= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96.\end{aligned}$$

Theorem 7.10. *For $n > 2$, $\phi(n)$ is an even integer.*

7.3 EULER'S THEOREM

Lemma 7.11. *Let $n > 1$ and $gcd(a, n) = 1$. If $a_1, a_2, \cdots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then*

$$aa_1, aa_2, \cdots, aa_{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \cdots, a_{\phi(n)}$ in some order.

Theorem 7.12 (Euler). *If $n \geq 1$ and $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Example 7.13. *To illustrate the proof, take $n = 9$ and $a = -4$. Then*

Remark 7.14. *If p is a prime, then $\phi(p) = p-1$; hence, whenever $gcd(a, p) = 1$, we get*

$$a^{p-1} \equiv a^{\phi(n)} \equiv 1 \ (mod\ n)$$

and so we have the following corollary.

Corollary 7.15 (Fermat). *If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \ (mod\ n)$.*

Example 7.16. *Find the last two digits in the decimal representation of 3^{203}.*