Contents

Chapter 1

UNIT I

1.1 Mathematical Induction

Definition 1.1.1. [**Well-Ordering Principle**]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's belonging to S.

Theorem 1.1.2. [**Archimedean property**] *If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$.*

Proof. Assume that the statement of the theorem is not true, so that for some a and b, $na < b$ for every positive integer n, Then the set

$$S = \{b - na : \; n \text{ a positive integer}\}$$

consists entirely of positive integers. By the $Well-OrderingPrinciple$, S will possess a least element, say, $b - ma$. Note that $b - (m + 1)a$ also lies in S, because S contains all integers of this form. Furthermore, we have

$$b - (m + 1)a = (b - ma) - a < b - ma$$

contrary to the choice of $b - ma$ as the smallest integer in S. This contradiction arose out of our original assumption that the Archimedean property did not hold; hence, this property is proven true. □

Theorem 1.1.3 (First Principle of Finite Induction.). *Let S be a set of positive integers with the following properties:*

(a) The integer 1 belongs to S.

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

Then S is set of all positive integers.

Proof. Let T be the set of all positive integers not in S, and assume that T is nonempty. The $Well-OrderingPrinciple$ tells us that T possesses a least element, which we denote by a. Because 1 is in S, certainly $a > 1$, and so $0 < a-1 < a$. The choice of a as the smallest positive integer in T implies that $a-1$ is not a member of T, or equivalently that $a-1$ belongs to S. By hypothesis, S must also contain $(a-1)+1 = a$, which contradicts the fact that a lies in T. We conclude that the set T is empty and in consequence that S contains all the positive integers. □

Remark 1.1.4. When giving induction proofs, we shall usually shorten the argument by eliminating all reference to the set S, and proceed to show simply that the result in question is true for the integer 1, and if true for the integer k is then also true for $k+1$.

Example 1.1.5. Consider the *Lucas sequence*

$$1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$$

Except for the first two terms, each term of this sequence is the sum of the preceding two, so that the sequence may be defined inductively by

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 3 \\ a_n &= a_{n-1} + a_{n-2} \quad for\ alln \geq 3 \end{aligned}$$

We contend that the inequality

$$a_n < (7/4)^n$$

holds for every positive integer n. The argument used is interesting because in the inductive step, it is necessary to know the truth of this inequality for two successive values of n to establish its truth for the following value.

First of all, for $n = 1$ and 2, we have

$$a_1 = 1 < (7/4)^1 = 7/4 \text{ and } a_2 = 3 < (7/4)^2 = 49/16$$

whence the inequality in question holds in these two cases. This provides a basis for the induction. For the induction step, choose an integer $k \geq 3$ and assume that the inequality is valid for $n = 1, 2, \cdots, k-1$. Then, in particular,

$$a_{k-1} < (7/4)^{k-1} \text{ and } a_{k-2} < (7/4)^{k-2}$$

By the way in which the Lucas sequence is formed, it follows that

$$\begin{aligned} a_k = a_{k-1} + a_{k-2} &< (7/4)^{k-1} + (7/4)^{k-2} \\ &= (7/4)^{k-2}(7/4 + 1) \\ &= (7/4)^{k-2}(11/4) \\ &< (7/4)^{k-2}(7/4)^2 = (7/4)^k \end{aligned}$$

Because the inequality is true for n=k whenever it is true for the integers $1, 2, \ldots, k-1$, we conclude by the second induction principle that $a_n < (7/4)^n$ for all $n \geq 1$.

1.2 The Binomial Theorem

1.2.1 Introduction

A BINOMIAL is an algebraic expression of two terms which are connected by the operation '+'(or) '−'For example, $x + 2y, x - y, x^3 + 4y, a + b$ etc$\cdots$ are binomials.

Theorem 1.2.1 (The Binomial Theorem). *For any natural number* n

$(x + a)^n = nC_0 x^n a^0 + nC_1 x^{n-1} a^1 + \cdots + nC_r x^{n-r} a^r + \cdots + nC_{n-1} x^1 a^{n-1} + nC_n x^0 a^n.$

Proof. We shall prove the theorem by the principle of mathematical induction.

Let $P(n)$ denote the statement:

$(x+a)^n = nC_0x^na^0 + nC_1x^{n-1}a^1 + \cdots + nC_rx^{n-r}a^r + \cdots + nC_{n-1}x^1a^{n-1} + nC_nx^0a^n.$

Step 1: Put $n = 1$

Then $P(1)$ is the statement: $(x+a)^1 = 1C_0x^1a^0 + 1C_1x^{1-1}a^1$

$$x + a = x + a$$

$\therefore$ $P(1)$ is true

Step 2: Now assume that the statement be true for $n = k$.

(i.e.,)assume that $P(k)$ be true.

$$(x+a)^k = kC_0x^ka^0 + kC_1x^{k-1}a^1 + \cdots + kC_rx^{k-r}a^r + \cdots + kC_nx^0a^k \text{ be true.} \qquad \cdots(1)$$

Step 3: Now to prove $p(k+1)$ is true.

(ie.,)To prove:

$(x+a)^{k+1} = k+1C_0x^{k+1}a^0 + k+1C_1x^{(k+1)-1}a^1 + \cdots + k+1C_rx^{(k+1)-r}a^r + \cdots + k+1C_{k+1}x^0a^{k+1}$. Consider $(x+a)^{k+1} = (x+a)^k(x+a)$

$$\begin{aligned}
&= [kC_0x^ka^0 + kC_1x^{k-1}a^1 + kC_2x^{k-2}a^2 + \cdots + kC_{(r-1)}x^{k-(r-1)}a^{(r-1)} + kC_rx^{k-r}a^r \\
&\qquad + \cdots + kC_nx^0a^k](x+a) \\
&= [kC_0x^{k+1}a^0 + kC_1x^ka^1 + kC_2x^{k-1}a^2 + \cdots + kC_{(r-1)}x^{k-r+2}a^{(r-1)} + kC_rx^{k-r+1}a^r \\
&\quad + \cdots + kC_nxa^k] + [kC_0x^ka + kC_1x^{k-1}a^2 + kC_2x^{k-2}a^3 + \cdots + kC_{(r-1)}x^{k-(r-1)}a^{r)} \\
&\qquad + kC_rx^{k-r}a^{r+1} + \cdots + kC_nx^0a^{k+1}]
\end{aligned}$$

$$(x+a)^{k+1} = kC_0x^{k+1} + (kC_1+kC_0)x^ka + (kC_2+kC_1)x^{k-1}a^2 + \cdots + (kC_r+kC_{r-1})x^{k-r+1}a^r + \cdots + kC_ka^{k+1} \qquad \cdots(2)$$

$$\begin{aligned}
\text{We know that } kC_r + kC_{r-1} &= {}_{(k+1)}C_r \text{ Put } r = 1, 2, 3, \cdots, etc. \\
kC_1 + kC_0 &= {}_{(k+1)}C_1 \\
kC_2 + kC_1 &= {}_{(k+1)}C_2
\end{aligned}$$

$$\begin{aligned} kC_r + kC_{r-1} &= {}_{(k+1)}C_r \text{ for } 1 \le r \le k \\ kC_0 &= 1 =_{(k+1)} C_0 \\ kC_k &= 1 =_{(k+1)} C_{(k+1)} \end{aligned}$$

$\therefore$(2) becomes $(x+a)^{k+1} =_{(k+1)} C_0 x^{k+1} +_{(k+1)} C_1 x^k a +_{(k+1)} C_2 x^{k-1} a^2 + \cdots + {}_{(k+1)}C_r x^{k-r+1} a^r +_{(k+1)} C_k a^{k+1}$

$\therefore$ $P(k+1)$ is true.

Thus if $P(k)$ is true, $P(k+1)$ is true.

$\therefore$ By the principle of mathematical induction $P(n)$ is true for all $n \in \mathbb{N}$

$(x+a)^n = nC_0 x^n a^0 + nC_1 x^{n-1} a^1 + \cdots + nC_r x^{n-r} a^r + \cdots + nC_{n-1} x^1 a^{n-1} + nC_n x^0 a^n$ for all $n \in \mathbb{N}$. $\square$

Some observations:

1. In the expansion
   $(x+a)^n = nC_0 x^n a^0 + nC_1 x^{n-1} a^1 + \cdots + nC_r x^{n-r} a^r + \cdots + nC_{n-1} x^1 a^{n-1} + nC_n x^0 a^n$,
   the general term is $nC_r x^{n-r} a^r$.
   Since this is nothing but the $(r+1)^{th}$ term, it is denoted by T_{r+1}
   i.e. $T_{r+1} = nC_r x^{n-r} a^r$.

2. The $(n+1)^{th}$ term is $T_{r+1} = nC_n x^{n-n} a^n = nC_n a^n$, the last term.

   $\boxed{\text{Thus there are } (n+1) \text{ terms in the expansion of } (x+a)^n}$

3. The degree of x in each term decreases while that of "a" increases such that the sum of the powers in each term is equal to n.

   $\boxed{\text{We can write } (x+a)^n = \sum_{r=0}^{n} nC_r x^{n-r} a^r}$

4. $nC_0, nC_1, nC_2, \ldots, nC_n$ are called binomial coefficients. They are also written as $C_0, C_1, C_2, \ldots, C_n$.

5. From the relation $nC_r = nC_{n-r}$, we see that the coefficients of terms equidistant from the beginning and the end are equal.

6. The binomial coefficients of the various terms of the expansion of $(x+a)^n$ for $n = 1, 2, 3, \ldots$ form a pattern.

Binomials	**Binomial coefficients**
$(x+a)^0$	1
$(x+a)^1$	1 1
$(x+a)^2$	1 2 1
$(x+a)^3$	1 3 3 1
$(x+a)^4$	1 4 6 4 1
$(x+a)^5$	1 5 10 10 5 1

This arrangement of the binomial coefficients is known as Pascal's triangle after the French mathematician Blaise Pascal (1623-1662). The numbers in any row can be obtained by the following rule. The first and last numbers are 1 each. The other numbers are obtained by adding the left and right numbers in the previous row.

1, 1+4=5, 4+6=10, 6+4=10, 4+1=5, 1

Some Particular Expansions:

In the expansion

$$(x+a)^n = nC_0x^na^0+nC_1x^{n-1}a^1+\cdots+nC_rx^{n-r}a^r+\cdots+nC_{n-1}x^1a^{n-1}+nC_nx^0a^n \cdots (1)$$

1. If we put $-a$ in the place of a

$\therefore \quad (x-a)^n =$

$$nC_0x^na^0 - nC_1x^{n-1}a^1 + nC_2x^{n-2}a^2 - \cdots + (-1)^r nC_rx^{n-r}a^r + \cdots + (-1)^n nC_nx^0a^n$$

We note that the signs of the terms are positive and negative alternatively.

2. If we put 1 in the place of a in (1) we get

$$(1+x)^n = 1 + nC_1x + nC_2x^2 + \cdots + nC_rx^r + \cdots + nC_nx^n \qquad \cdots (2)$$

3. If we put $-x$ in the place of x in (2) we get

$$(1-x)^n = 1 - nC_1x + nC_2x^2 - \cdots + (-1)^r nC_rx^r + \cdots + (-1)^n nC_nx^n$$

Middle Term:

The number of terms in the expansion of $(x+a)^n$ depends upon the index n. The index is either even (or) odd. Let us find the middle terms.

Case(i): n is even

The number of terms in the expansion is $(n+1)$, which is odd.

Therefore, there is only one middle term and it is given by $T_{\frac{n}{2}+1}$.

Case(ii): n is odd

The number of terms in the expansion is $(n+1)$, which is even.

Therefore, there is two middle terms and they are given by $T_{\frac{n+1}{2}}$ and $T_{\frac{n+3}{2}}$.

Particular Terms:

Sometimes a particular term satisfying certain conditions is required in the binomial expansion of $(x+a)^n$. This can be done by expanding $(x+a)^n$ and then locating the required term. Generally this becomes a tedious task, when the index n is large. In such cases, we begin by evaluating the general term T_{r+1} and then finding the values of r by assuming T_{r+1} to be the required term.

To get the term independent of x, we put the power of x equal to zero and get the value of r for which the term independent of x. Putting this value of r in T_{r+1}, we get the term independent of x.

Example 1.2.2. Find the expansion of: (i) $(2x+3y)^5$ (ii) $\left(2x^2-\frac{3}{4}\right)^4$

Solution.

$$\begin{aligned}
(i)(2x+3y)^5 &= {}_5C_0(2x)^5(3y)^0 +_5 C_1(2x)^4(3y)^1 +_5 C_2(2x)^3(3y)^2 +_5 C_3(2x)^2(3y)^3 \\
&\qquad +_5 C_4(2x)^1(3y)^4 +_5 C_5(2x)^0(3y)^5 \\
&= 1(32)x^5(1) + 5(16x^4)(3y) + 10(8x^3)(9y^2) + 10(4x^2)(27y^3) \\
&\qquad + 5(2x)(81y^4) + (1)(1)(243y^5) \\
&= 32x^5 + 240x^4y + 720x^3y^2 + 1080x^2y^3 + 810xy^4 + 243y^5
\end{aligned}$$

$$
\begin{aligned}
(ii)\left(2x^2-\frac{3}{4}\right)^4 &= {}_4C_0(2x^2)^4\left(-\frac{3}{x}\right)^0 +_4 C_1(2x^2)^3\left(-\frac{3}{x}\right)^1 +_4 C_2(2x^2)^2\left(-\frac{3}{x}\right)^2 + \\
&\quad {}_4C_3(2x^2)^1\left(-\frac{3}{x}\right)^3 +_4 C_4(2x^2)^0\left(-\frac{3}{x}\right)^4 \\
&= (1)16x^8+4(8x^6)\left(-\frac{3}{x}\right)+6(4x^4)\left(\frac{9}{x^2}\right)+4(2x^2)\left(-\frac{27}{x^3}\right) \\
&\quad +(1)(1)\left(\frac{81}{x^4}\right) \\
&= 16x^8-96x^5+216x^2-\frac{216}{x}+\frac{81}{x^4}
\end{aligned}
$$

Example 1.2.3. Using binomial theorem, find the 7^{th} power of 11.

Solution.

$$
\begin{aligned}
11^7 &= (1+10)^7 \\
&= {}_7C_0(1)^7(10)^0 +_7 C_1(1)^6(10)^1 +_7 C_2(1)^5(10)^2 +_7 C_3(1)^4(10)^3 +_7 C_4(1)^3(10)^4 + \\
&\quad {}_7C_5(1)^2(10)^5 +_7 C_6(1)^1(10)^6 +_7 C_7(1)^0(10)^7 \\
&= 1+70+\frac{7\times 6}{1\times 2}10^2+\frac{7\times 6\times 5}{1\times 2\times 3}10^3+\frac{7\times 6\times 5}{1\times 2\times 3}10^4+\frac{7\times 6}{1\times 2}10^5+7(10)^6+10^7 \\
&= 1+70+2100+35000+350000+2100000+7000000+10000000 \\
&= 19487171
\end{aligned}
$$

Example 1.2.4. If $n \in \mathbb{N}$, in the expansion of $(1+x)^n$ prove the following :

(i) Sum of the binomial coefficients $= 2^n$

(ii) Sum of the coefficients of odd terms = Sum of the coefficients of even terms = 2^{n-1}

Solution. The coefficients $nC_0, nC_1, nC_2, \ldots, nC_n$ in the expansion of $(1+x)^n$ are called the binomial coefficients, we write them as $C_0, C_1, C_2, \cdots, C_n$,

$$(1+x)^n = C_0 + C_1 x + C_2 x^2 + \cdots + C_r x^r + \cdots + C_n x^n$$

It is an identity in x and so it is true for all values of x.

Putting $x = 1$ we get $2^n = C_0 + C_1 + C_2 + \cdots + C_n \qquad \cdots (1)$

put $x = -1$ $0 = C_0 - C_1 + C_2 - C_3 + \cdots (-1)^n C_n$

$\Rightarrow \quad C_0 + C_2 + C_4 + \cdots = C_1 + C_3 + C_5 + \cdots$

It is enough to prove that

$$\begin{aligned}
C_0 + C_2 + C_4 + \cdots &= C_1 + C_3 + C_5 + \cdots = 2^{n-1} \\
\text{Let } C_0 + C_2 + C_4 + \cdots &= C_1 + C_3 + C_5 + \cdots = k \qquad \cdots (2) \\
\text{From (1)}, C_0 + C_1 + C_2 + \cdots + C_n &= 2^n \\
2k &= 2^n \text{From (2)} \\
k &= 2^{n-1} \\
\text{From (2)}, C_0 + C_2 + C_4 + \cdots &= C_1 + C_3 + C_5 + \cdots = 2^{n-1}
\end{aligned}$$

1.3 The Division Algorithm

Theorem 1.3.1 (Division Algorithm)**.** *Given integers a and b, with $b > 0$, there exist unique integer 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.

Proof. We begin by proving that the set

$$S = \{a - xb : \ x \text{ an integer}; \ a - xb \geq 0\}$$

is nonempty. To do this, it suffices to exhibit a value of x making $a - xb$ nonnegative. Because the integer $b \geq 1$. we have $|a|b \geq |a|$, and so

$$a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$$

For the choice $x = -|a|$,then, $a - xb$ lies in S. This paves the way for an application of the *Well-Ordering Principle* , from which we infer that the set S contains a smallest integer, call it r. By the definition of S, there exists an integer q satisfying

$$r = a - qb \quad 0 \leq r$$

We argue that $r < b$, If this were not the case, then $r \geq b$ and

$$a - (q + 1)b = (a - qb) - b = r - b \geq 0$$

The implication is that the integer $a - (q + 1)b$ has the proper form to belong to the set S. But $a - (q + 1)b = r - b < r$, leading to a contradiction of the choice of r as the smallest member of S. Hence, $r < b$.

Next we turn to the task of showing the uniqueness of q and r. Suppose that a has two representations of the desired form, say,

$$a = qb + r = q'b + r'$$

where $0 \leq r < b$, $0 \leq r' < b$. Then $r' - r = b(q - q')$ and, owing to the fact that the absolute value of a product is equal to the product of the absolute values,

$$|r' - r| = b|q - q'|$$

Upon adding the two inequalities $-b < -r \leq 0$ and $0 \leq r' < b$, we obtain
$-b < r' - r < b$ or, in equivalent terms, $|r' - r| < b$. Thus, $b|q - q'| < b$, which yields

$$0 \leq |q - q'| < 1$$

Because $|q - q'|$ is a nonnegative integer, the only possibility is that $|q - q'| = 0$, whence $q = q'$; this, in turn, gives $r = r'$, ending the proof. $\square$

Corollary 1.3.2. *If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that*

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

Proof. It is enough to consider the case in which b is negative. Then $|b| > 0$, and Theorem 1.3.1 produces unique integers q' and r for which

$$a = q'|b| + r \qquad 0 \leq r < |b|$$

Noting that $|b| = -b$, we may take $q = -q'$ to arrive at $a = qb + r$, with $0 \leq r < |b|$. □

Example 1.3.3. Show that the expression $a(a^2 + 2)/3$ is an integer for all $a \geq 1$. According to the Division Algorithm, every a of the form $3q, 3q + 1$, or $3q + 2$. Assume that first of these cases. Then

$$\tfrac{a(a^2+2)}{3} = q(9q^2 + 2)$$

which clearly is an integer. Similarly, if $a = 3q + 1$. then

$$\tfrac{(3q+1)((3q+1)^2+2)}{3} = (3q + 1)(3q^2 + 2q + 1)$$

and $a(a^2 + 2)/3$ is an integer in this instance also. Finally, for $a = 3q + 2$, we obtain

$$\tfrac{(3q+2)((3q+2)^2+2)}{3} = (3q + 2)(3q^2 + 4q + 2)$$

an integer once more. Consequently, our result is established in all cases.

1.4 The Greatest Common Divisor

Definition 1.4.1. An integer b is said to be *divisible* by an integer $a \neq 0$, in symbols $a|b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Theorem 1.4.2. *For integers a,b,c, the following hold* *(a)* $a|0, 1|a, a|a$.

(b) $a|1$ *if and only if* $a = \pm 1$.

(c) *If* $a|b$ *and* $c|d$, *then* $ac|bd$.

(d) *If* $a|b$ *and* $b|c$, *then* $a|c$.

(e) $a|b$ *and* $b|a$ *if and only if* $a = \pm b$.

(f) *If* $a|b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.

(g) *If* $a|b$ *and* $a|c$, *then* $a|(bx + cy)$ *for arbitrary integers* x *and* y.

Proof. We shall prove assertions (f) and (g), leaving the other parts as an exercise. If $a|b$, then there exists an integer c such that $b = ac$; also $b \neq 0$ implies that $c \neq 0$. Upon taking absolute values, we get $|b| = |ac| = |a||c|$. Because $c \neq 0$, it follows that $|c| \geq 1$, whence $|b| = |a||c| \geq |a|$.

As regards (g), the relations $a|b$ and $a|c$ ensure that $b = ar$ and $c = as$ for suitable integers r and s. But then whatever the choice of x and y,

$$bx + cy = arx + asy = a(rx + sy)$$

Because $rx + sy$ is an integer, this says that $a|(bx + cy)$, as desired. □

Definition 1.4.3. Let a and b be given integers, with at least one of them different from zero. The *greatest common divisor* of a and b, denoted dy $gcd(a, b)$, is the positive integer d satisfying the following:

(a) $d|a$ and $d|b$.

(b) If $c|a$ and $c|b$, then $c \leq d$.

Example 1.4.4. The positive divisors of -12 are $1, 2, 3, 4, 6, 12$, whereas those of 30 are $1, 2, 3, 5, 6, 10, 15, 30$; hence, the positive common divisors of -12 and 30 are $1, 2, 3, 6$, Because 6 is the largest of these integers, it follows that $gcd(-12, 30) = 6$. In the same way, we can show that

$$gcd(-5, 5) = 5 \quad gcd(8, 17) = 1 \quad gcd(-8, -36) = 4$$

Theorem 1.4.5. *Given integers a and b, not both of which are zero, there exist integers x and y such that*

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

Proof. Consider the set S of all positive linear combinations of a and b:

$$S = \{au + bv : \ au + bv > 0; \ u, v \text{ integers}\}$$

Notice first that S is not empty. For example, if $a \neq 0$, then the integer $|a| = au + b.0$ lies in S, where we choose $u = 1$ or $u = -1$ according as a is positive or negative. By virtue of the Well-ordering Principle, S must contain a smallest element d. Thus, from the very definition of S, there exists integers x and y for which $d = ax + by$. We claim that $d = gcd(a, b)$.

Taking stock of the Division Algorithm, we can obtain integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r can be written in the form

$$\begin{aligned} r = a - qd &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \end{aligned}$$

If r were positive, then this representation would imply that r is a member of S, contradicting the fact that d is the least integer in S (recall that $r < d$). Therefore, $r = 0$, and so $a = qd$, or equivalently $d|a$. By similar reasoning, $d|b$, the effect of which is to make d a common divisor of a and b.

Now, if c is an arbitrary positive common divisor of the integers a and b, then part (g) of Theorem 1.4.2 allows us to conclude that $c|(ax + by)$; that is, $c|d$. by part (f) of the same theorem, $c = |c| \leq |d| = d$, so that d is greater than every positive common divisor of a and b. Piecing the bits of information together, we see that $d = gcd(a, b)$.

□

Corollary 1.4.6. *If a and b are given integers, not both zero, then the set*

$$T = \{ax + by : \ x, y \text{ are integers}\}$$

is precisely the set of all multiples of $d = gcd(a, b)$.

Proof. Because $d|a$ and $d|b$, we know that $d|(ax + by)$ for all integers x, y. Thus, every member of T is a multiple of d. Conversely, d may be written as $d = ax_0 + by_0$ for suitable x_0, and y_0, so that any multiple nd of d is of the form

$$nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0)$$

Hence, nd is a linear combination of a and b, and, by definition, lies in T. □

Definition 1.4.7. Two integers a and b, not both of which are zero, are said to be *relatively prime* whenever $gcd(a, b) = 1$.

Theorem 1.4.8. *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 $1 = ax + by$.*

Proof. If a and b are relatively prime so that $gcd(a, b) = 1$, then Theorem 1.4.5 guarantees the existence of integers x and y satisfying $1 = ax + by$. As for the converse, suppose that $1 = ax + by$ for some choice of x and y, and that $d = gcd(a, b)$. Because $d|a$ an $d|b$, Theorem 1.4.2 yields $d|(ax + by)$, or $d|1$. Inasmuch as d is a positive integer, this last divisibility condition forces d to equal 1 (part (b) of Theorem 1.4.2 plays a role here), and the desired conclusion follows. □

Corollary 1.4.9. *If $gcd(a, b) = d$, then $gcd(a/d, b/d) = 1$.*

Proof. Before starting with the proof proper, we should observe that although a/d and b/d have the appearance of fractions, in fact, they are integers because d is a divisor both of a and of b. Now, knowing that $gcd(a, b) = d$, it is possible to find integers x and y such that $d = ax + by$. Upon dividing each side of this equation by d, we obtain the expression

$$1 = \left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y$$

Because a/d and b/d are integers, an appeal to the theorem is legitimate. The conclusion is that a/d and b/d are relatively prime. $\square$

Corollary 1.4.10. *If $a|c$ and $b|c$, with $gcd(a, b) = 1$, then $ab|c$.*

Proof. In as much as $a|c$ and $b|c$, integers r and s can be found such that $c = ar = bs$. Now the relation $gcd(a, b) = 1$ allows us to write $1 = ax + by$ for some choice of integers x and y. Multiplying the last equation by c, it appears that

$$c = c.1 = c(ax + by) = acx + bcy$$

If the appropriate substitutions are now made on the right-hand side, then

$$c = a(bs)x + b(ar)y = ab(sx + ry)$$

or, as a divisibility statement, $ab|c$. $\square$

Theorem 1.4.11 (Euclid's Lemma)**.** *If $a|bc$, with $gcd(a, b) = 1$, then $a|c$.*

Proof. We start again from Theorem 1.4.5, writing $1 = ax + by$, where x and y are integers. Multiplication of this equation by c produces

$$c = 1.c = (ax + by)c = acx + bcy$$

Because $a|ac$ and $a|bc$, it follows that $a|(acx + bcy)$, which can be recast as $a|c$. $\square$

Theorem 1.4.12. *Let a, b be integers, not both zero. For a positive integer d, $d = gcd(a, b)$ if and only if*

(a) $d|a$ and $d|b$.

(b) Whenever $c|a$ and $c|b$, then $c|d$.

Proof. To being, suppose that $d = gcd(a, b)$. Certainly, $d|a$ and $d|b$, so that (a) holds. In light of Theorem 1.4.5, d is expressible as $d = ax + by$ for some integers x, y. Thus, if $c|a$ and $c|b$, then $c|(ax + by)$, or rather $c|d$. In short, condition (b) holds. Conversely, let d be any positive integer satisfying the stated conditions. Given any common divisor c of a and b, we have $c|d$ from hypothesis (b). The implication is that $d \geq c$, and consequently d is the greatest common divisor of a and b. □

1.5 The Euclidean Algorithm

Let a and b be two integers whose greatest common divisors is desired. Because $gcd(|a|, |b|) = gcd(a, b)$, there is no harm in assuming that $a \geq b > 0$. The first step is to apply the Division Algorithm to a and b to get

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

If it happens that $r_1 = 0$, then $b|a$ and $gcd(a, b) = b$. When $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears, say, at the $(n + 1)$th stage where r_{n-1} is divided by r_n (a zero remainder occurs sooner or later because the decreasing sequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain more than b integers).

The result is the following system of equations:

$$\begin{aligned}
a &= q_1 b + r_1 \qquad 0 < r_1 < b \\
b &= q_2 r_1 + r_2 \qquad 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 \qquad 0 < r_3 < r_2 \\
&. \\
&. \\
&. \\
r_{n-2} &= q_n r_{n-1} + r_n \qquad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

We argue that r_n, the last nonzero remainder that appears in this manner, is equal to $gcd(a, b)$. Our proof is based on the lemma below.

Lemma 1.5.1. *If* $a = qb + r$, *then* $gcd(a, b) = gcd(b, r)$

Proof. If $d = gcd(a, b)$, then the relations $d|a$ and $d|b$ together imply that $d|(a - qb)$, or $d|r$. Thus, d is a common divisor of both b and r. On the other hand, if c is an arbitrary common divisor of b and r, then $c|(qb + r)$, whence $c|a$. This makes c a common divisor of a and b, so that $c \leq d$. It now follows from the definition of $gcd(b, r)$ that $d = gcd(b, r)$. □

Example 1.5.2. Let us see how the Euclidean Algorithm works in a concrete case by calculating, say, $gcd(12378, 3054)$. The appropriate applications of the Division

Algorithm produce the equations

$$\begin{aligned}
12378 &= 4.3054 + 162 \\
3054 &= 18.162 + 138 \\
162 &= 1.138 + 24 \\
138 &= 5.24 + 18 \\
24 &= 1.18 + 6 \\
18 &= 3.6 + 0
\end{aligned}$$

Our previous discussion tells us that the last nonzero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

$$6 = gcd(12378, 3054)$$

Theorem 1.5.3. *If* $k > 0$*, then* $gcd(ka, kb) = k.gcd(a, b)$

Proof. If each of the equations appearing in the Euclidean Algorithm for a and b is multiplied by k, we obtain

$$\begin{aligned}
ak &= q_1(bk) + r_1k \quad 0 < r_1k < bk \\
bk &= q_2(r_1k) + r_2k \quad 0 < r_2k < r_1k \\
&. \\
&. \\
&. \\
r_{n-2}k &= q_n(r_{n-1}k) + r_nk \quad 0 < r_nk < r_{n-1}k \\
r_{n-1}k &= q_{n+1}(r_nk) + 0
\end{aligned}$$

But this is clearly the Euclidean Algorithm applied to the integers ak and bk, so that their greatest common divisor is the last nonzero remainder r_nk; that is,

$$gcd(ka, kb) = r_nk = k.gcd(a, b)$$

as stated in the theorem. □

Corollary 1.5.4. *For any integer $k \neq 0$, $gcd(ka, kb) = |k|gcd(a, b)$.*

Proof. It suffices to consider the case in which $k < 0$. Then $-k = |k| > 0$ and, by Theorem 1.5.3

$$\begin{aligned} gcd(ak, bk) &= gcd(-ak, -bk) \\ &= gcd(a|k|, b|k|) \\ &= |k|gcd(a, b) \end{aligned}$$

An alternate proof of the above Theorem runs very quickly as follows: $gcd(ak, bk)$ is the smallest positive integer of the form $(ak)x + (bk)y$, which, in turn, is equal to k times the smallest positive integer of the form $ax + by$; the latter value is equal to $k.gcd(a, b)$. □

Definition 1.5.5. The *least common multiple* of two nonzero integers a and b, denote by $lcm(a, b)$, is the positive integer m satisfying the following:

(a) $a|m$ and $b|m$.

(b) If $a|c$ and $b|c$, with $c > 0$, then $m \leq c$.

Theorem 1.5.6. *For positive integers a and b*

$$gcd(a, b)lcm(a, b) = ab$$

Proof. To being, put $d = gcd(a, b)$ and write $a = dr, b = ds$ for integers r and s. If $m = ab/d$, then $m = as = rb$, the effect of which is to make m a (positive) common multiple of a and b.

Now let c be any positive integer that is a common multiple of a and b; say, for definiteness, $c = au = bv$. As we know, there exist integers x and y satisfying $d = ax + by$. In consequence,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx + uy$$

This equation states that $m|c$, allowing us to conclude that $m \leq c$. Thus, in accordance with Definition of lcm, $m = lcm(a, b)$; that is,

$$lcm(a, b) = \frac{ab}{d} = \frac{ab}{gcd(a,b)}$$

which is what we started out to prove. $\square$

Corollary 1.5.7. *For any choice of positive integers a and b, $lcm(a, b) = ab$ if and only if $gcd(a, b) = 1$.*

1.6 The Diophantine Equation $ax + by = c$

Theorem 1.6.1. *The linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by*

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

where t is an arbitrary integer.

Proof. To establish the second assertion of the theorem, let us suppose that a solution x_0, y_0 of the given equation is known. If x', y' is any other solution, then

$$ax_0 + by_0 = c = ax' + by'$$

which is equivalent to

$$a(x' - x_0) = b(y_0 - y')$$

By the corollary to Theorem 1.4.8, there exist relatively prime integers r and S such that $a = dr$, $b = ds$. Substituting these values into the last-written equation and canceling the common factor d, we find that

$$r(x' - x_0) = s(y_0 - y')$$

The situation is now this: $r|s(y_0 - y')$, with $gcd(r, s) = 1$. Using Euclid's lemma, it must be the case that $r|(y_0 - y')$; or, in other words, $y_0 - y' = rt$ for some integer t. Substituting, we obtain

$$x' - x_0 = st$$

This leads us to the formulas

$$x' = x_0 + st = x_0 + \left(\tfrac{b}{d}\right) t$$
$$y' = y_0 - rt = y_0 - \left(\tfrac{a}{d}\right) t$$

It is easy to see that these values satisfy the Diophantine equation,regardless of the choice of the integer t; for

$$\begin{aligned} ax' + by' &= a\left[x_0 + (\frac{b}{d})t\right] + b\left[y_0 - (\frac{a}{d})t\right] \\ &= (ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right) t \\ &= c + 0.t \\ &= c \end{aligned}$$

Thus, there are an infinite number of solutions of the given equation, one for each value of t. □

Example 1.6.2. Consider the linear Diophantine equation

$$172x + 20y = 1000$$

Applying the Euclidean's Algorithm to the evaluation of $gcd(172, 20)$, we find that

$$\begin{aligned} 172 &= 8.20 + 12 \\ 20 &= 1.12 + 8 \\ 12 &= 1.8 + 4 \\ 8 &= 2.4 \end{aligned}$$

whence $gcd(172, 20) = 4$. Because $4|1000$, a solution to this equation exists. To obtain the integer 4 as a linear combination of 172 and 20, we work backward through the previous calculations, as follows:

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2.12 - 20 \\ &= 2(172 - 8.20) - 20 \\ &= 2.172 + (-17)20 \end{aligned}$$

Upon multiplying this relation by 250, we arrive at

$$\begin{aligned} 1000 = 250.4 &= 250[2.172 + (-17)20] \\ &= 500.172 + (-4250)20 \end{aligned}$$

so that $x = 500$ and $y = -4250$ provide one solution to the Diophantine equation in question. All other solutions are expressed by

$$x = 500 + (20/4)t = 500 + 5t$$
$$y = -4250 - (172/4)t = -4250 - 43t$$

for some integer t. A little further effort produces the solutions in the positive integers, if any happen to exist. For this, t must be chosen to satisfy simultaneously the inequalities

$$5t + 500 > 0 \quad -43t - 4250 > 0$$

or, what amounts to the same thing,

$$-98\tfrac{36}{43} > t > -100$$

Because t must be an integer, we are forced to conclude that $t = -99$. Thus, our Diophantine equation has a unique positive solution $x = 5, y = 7$ corresponding to the value $t = -99$.

Corollary 1.6.3. *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.

Example 1.6.4. A customer bought a dozen pieces of fruit, apples and oranges, for \$1.32. If an apple costs 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

To set up this problem as a Diophantine equation, let x be the number of apples and y be the number of oranges purchased; in addition, let z represent the cost(in cents) of an orange. Then the conditions of the problem lead to

$$(z+3)x + zy = 132$$

or equivalently

$$3x + (x+y)z = 132$$

Because $x + y = 12$, the previous equation may be replaced by

$$3x + 12z = 132$$

which, in turn, simplifies to $x + 4z = 44$.

Stripped of inessentials, the object is to find integers x and z satisfying the Diophantine equation

$$x + 4z = 44 \tag{1.1}$$

Inasmuch as $gcd(1,4) = 1$ is a divisor of 44, there is a solution to this equation. Upon multiplying the relation $1 = 1(-3) + 4.1$ by 44 to get

$$44 = 1(-132) + 4.44$$

it follows that $x_0 = 132$, $z_0 = 44$ serves as one solution. All other solutions of Equation (1.1) are of the form

$$x = -132 + 4t \qquad z = 44 - t$$

where t is an integer.

Not all of the choices for t furnish solutions to the original problem. Only values of t that ensure $12 \geq x > 6$ should be considered. This requires obtaining those values of t such that

$$12 \geq -132 + 4t > 6$$

Now, $12 \geq -132 + 4t$ implies that $t \leq 36$, whereas $-132 + 4t > 6$ gives $t > 34\frac{1}{2}$. The only integral values of t to satisfy both inequalities are $t = 35$ and $t = 36$. Thus, there are two possible purchases: a dozen apples costing 11 cents apiece(the case where $t = 36$), or 8 apples at 12 cents each and 4 oranges at 9 cents each(the case where $t = 35$).

Chapter 2

UNIT II

2.1 The Fundamental Theorem of Arithmetic

Definition 2.1.1. *An integer $p > 1$ is called a $prime\ number$, or simply a $prime$, if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is termed $composite$.*

Theorem 2.1.2. *If p is a prime and $p|ab$, then $p|a$ or $p|b$.*

Proof. If $p|a$, then we need go no further, so let us assume that $p \nmid a$. Because the only positive divisors of p are 1 and p itself, this implies that $gcd(p, a) = 1$. (In general, $gcd(p, a) = p$ or $gcd(p, a) = 1$ according as $p|a$ or $p \nmid a$.) Hence, citing Euclid's lemma, we get $p|b$. □

Corollary 2.1.3. *If p is a prime and $p|a_1a_2 \cdots a_n$, then $p|a_k$ for some k, where $1 \leq k \leq n$.*

Proof. We proceed by induction on n, the number of factors. When $n = 1$, the stated conclusion obviously holds; whereas when $n = 2$, the result is the content of Theorem 2.1.2. Suppose, as the induction hypothesis, that $n > 2$ and that whenever p divides a product of less than n factors, it divides at least one of the factors. Now $p|a_1a_2 \cdots a_n$.

From Theorem 2.1.2, either $p|a_n$ or $p|a_1a_2\cdots a_{n-1}$. If $p|a_n$, then we are through. As regards the case where $p|a_1a_2\cdots a_{n-1}$, the induction hypothesis ensures that $p|a_k$ for some choice of k, with $1 \leq k \leq n-1$. In any event, p divides one of the integers $a_1, a_2, \ldots, a_n$. □

Corollary 2.1.4. *If $p, q_1, q_2, \cdots, q_n$ are all primes and $p|q_1q_2\cdots q_n$, then $p = qk$ for some k, where $1 \leq k \leq n$.*

Proof. By virtue of Corollary 2.1.3, we know that $p|q_k$ for some k, with $1 \leq k \leq n$. Being a prime, q_k is not divisible by any positive integer other than 1 or q_k itself. Because $p > 1$, we are forced to conclude that $p = q_k$. □

Theorem 2.1.5 (Fundamental Theorem of Arithmetic)**.** *Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.*

Proof. Either n is a prime or it is composite; in the former case, there is nothing more to prove. If n is composite, then there exists an integer d satisfying $d|n$ and $1 < d < n$. Among all such integers d, choose p_1 to be the smallest (this is possible by the $Well-Ordering\ Principle$). Then p_1 must be a prime number. Otherwise it too would have a divisor q with $1 < q < p_1$; but then $q|p_1$ and $p_1|n$ imply that $q|n$, which contradicts the choice of p_1 as the smallest positive divisor, not equal to 1, of n.

We therefore may write $n = p_1n_1$,where p_1 is prime and $1 < n_1 < n$. If n_1 happens to be a prime, then we have our representation. In the contrary case, the argument is repeated to produce a second prime number p_2 such that $n_1 = p_2n_2$; that is,

$$n = p_1p_2n_2 \quad 1 < n_2 < n_1$$

If n_2 is a prime, then it is not necessary to go further. Otherwise, write $n_2 = p_3n_3$, with p_3 a prime:

$$n = p_1p_2p_3n_3 \quad 1 < n_3 < n_2$$

The decreasing sequence

$$n > n_1 > n_2 > \cdots > 1$$

cannot continue indefinitely, so that after a finite number of steps n_{k-1} is a prime, call it, p_k. This leads to the prime factorization

$$n = p_1 p_2 \cdots p_k$$

To establish the second part of the proof-the uniqueness of the prime factorization-let us suppose that the integer n can be represented as a product of primes in two ways; say,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad r \leq s$$

where the p_i and q_j are all primes, written in increasing magnitude so that

$$p_1 \leq p_2 \leq \cdots p_r \qquad q_1 \leq q_2 \leq \cdots q_s$$

Because $p_1 | q_1 q_2 \cdots q_s$, Corollary 2.1.4 of Theorem 2.1.2 tells us that $p_1 = q_k$ for some k; but then $p_1 \geq q_1$. Similar reasoning gives $q_1 \geq p_1$, whence $p_1 = q_1$. We may cancel this common factor and obtain

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Now repeat the process to get $p_2 = q_2$ and, in turn,

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s$$

Continue in this fashion. If the inequality $r < s$ were to hold, we would eventually arrive at

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

which is absurd, because each $q_j > 1$. Hence, $r = s$ and

$$p_1 = q_1 \qquad p_2 = q_2, \cdots, p_r = q_r$$

making the two factorizations of n identical. The proof is now complete. $\square$

Corollary 2.1.6. *Any positive integer $n > 1$ can be written uniquely in a canonical form*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_3^{k_r}$$

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

Theorem 2.1.7 (Pythagoras)**.** *The number $\sqrt{2}$ is irrational.*

Proof. Suppose, to the contrary, that $\sqrt{2}$ is a rational number, say, $\sqrt{2} = a/b$, where a and b are both integers with $gcd(a, b) = 1$. Squaring, we get $a^2 = 2b^2$, so that $b|a^2$. If $b > 1$, then the Fundamental Theorem of Arithmetic guarantees the existence of a prime p such that $p|b$. It follows that $p|a^2$ and, by Theorem 2.1.2, that $p|a$; hence, $gcd(a, b) \geq p$. We therefore arrive at a contradiction, unless $b = 1$. But if this happens, then $a^2 = 2$, which is impossible (we assume that the reader is willing to grant that no integer can be multiplied by itself to give 2). Our supposition that $\sqrt{2}$ is a rational number is untenable, and so $\sqrt{2}$ must be irrational. $\square$

2.2 The Sieve of Eratosthenes

Example 2.2.1. The foregoing technique provides a practical means for determining the canonical form of an integer, say $a = 2093$. Because $45 < \sqrt{2093} < 46$, it is enough to examine the primes $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$. By trial, the first of these to divide 2093 is 7, and $2093 = 7.299$. As regards the integer 299, the seven primes that are less than 18 (note that $17 < \sqrt{299} < 18$) are $2, 3, 5, 7, 11, 13, 17$. The first prime divisor of 299 is 13 and, carrying out the required division, we obtain $299 = 13 \cdot 23$. But 23 is itself a prime, whence 2093 has exactly three prime factors, $7, 13, and 23$:

$$2093 = 7 \cdot 13 \cdot 23$$

Theorem 2.2.2 (Euclid)**.** *There is an infinite number of primes.*

Proof. Euclid's proof is by contradiction. Let $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \cdots$ be the primes in ascending order, and suppose that there is a last prime, called p_n. Now consider the positive integer

$$P = p_1 p_2 \cdots p_{n+1}$$

Because $P > 1$, we may put Theorem 2.1.5 to work once again and conclude that P is divisible by some prime p. But $p_1, p_2, \cdots, p_n$ are the only prime numbers, so that p must be equal to one of $p_1, p_2, \cdots, p_n$. Combining the divisibility relation $p | p_1 p_2 \cdots p_n$ with $p | P$, we arrive at $p | P - p_1 p_2 \cdots p_n$ or, equivalently, $p | 1$. The only positive divisor of the integer 1 is 1 itself and, because $p > 1$, a contradiction arises. Thus, no finite list of primes is complete, whence the number of primes is infinite. $\square$

Theorem 2.2.3. *If p_n is the nth prime number, then $p_n \leq 2^{2^{n-l}}$.*

Proof. Let us proceed by induction on n, the asserted inequality being clearly true when $n = 1$. As the hypothesis of the induction, we assume that $n > 1$ and that the result holds for all integers up to n. Then

$$\begin{aligned} p_{n+1} &\leq p_1 p_2 \cdots p_{n+1} \\ &\leq 2.2^2 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\cdots+2^{n-1}} + 1 \end{aligned}$$

Recalling the identity $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^{n-1}$, we obtain

$$p_{n+1} \leq 2^{2^n-1} + 1$$

However, $1 \leq 2^{2^n-l}$ for all n; whence

$$\begin{aligned} p_{n+1} &\leq 2^{2^n-1} + 2^{2^n-1} \\ &= 2.2^{2^n-1} = 2^{2^n} \end{aligned}$$

completing the induction step, and the argument. $\square$

Corollary 2.2.4. *For $n \geq 1$, there are at least $n+1$ primes less than 2^{2^n}.*

Proof. From the theorem, we know that $p_1, p_2, \cdots, p_{n+1}$ are all less than 2^{2^n}. $\square$

2.3 The Goldbach Conjecture

Lemma 2.3.1. *The product of two or more integers of the form $4n+1$ is of the same form.*

Proof. It is sufficient to consider the product of just two integers. Let us take $k = 4n+1$ and $k' = 4m+1$. Multiplying these together, we obtain

$$\begin{aligned} kk' &= (4n+1)(4m+1) \\ &= 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1 \end{aligned}$$

which is of the desired form. $\square$

Theorem 2.3.2. *There are an infinite number of primes of the form $4n+3$.*

Proof. In anticipation of a contradiction, let us assume that there exist only finitely many primes of the form $4n+3$; call them $q_1, q_2, \cdots, q_s$. Consider the positive integer

$$N = 4q_1q_2\cdots q_s - 1 = 4(q_1q_2\cdots q_s - 1) + 3$$

and let $N = r_1r_2\cdots r_t$ be its prime factorization. Because N is an odd integer, we have $r_k \neq 2$ for all k, so that each r_k is either of the form $4n+1$ or $4n+3$. By the lemma, the product of any number of primes of the form $4n+1$ is again an integer of this type. For N to take the form $4n+3$, as it clearly does, N must contain at least one prime factor r_i of the form $4n+3$. But r_i cannot be found among the listing $q_1, q_2, \cdots, q_s$, for this would lead to the contradiction that $r_i|1$. The only possible conclusion is that there are infinitely many primes of the form $4n+3$. $\square$

Theorem 2.3.3 (Dirichlet). *If a and b are relatively prime positive integers, then the arithmetic progression*

$$a, a+b, a+2b, a+3b, \cdots$$

contains infinitely many primes.

Theorem 2.3.4. *If all the $n > 2$ terms of the arithmetic progression*

$$p, p+d, p+2d, \cdots, p+(n-1)d$$

are prime numbers, then the common differenced is divisible by every prime $q < n$.

Proof. Consider a prime number $q < n$ and assume to the contrary that $q \nmid d$. We claim that the first q terms of the progression

$$p, p+d, p+2d, \cdots, p+(q-1)d \tag{2.1}$$

will leave different remainders when divided by q. Otherwise there exist integers j and k, with $0 \leq j < k \leq q-1$, such that the numbers $p+jd$ and $p+kd$ yield the same remainder upon division by q. Then q divides their difference $(k-j)d$. But $gcd(q,d) = 1$, and so Euclid's lemma leads to $q|k-j$, which is nonsense in light of the inequality $k - j \leq q - 1$.

Because the q different remainders produced from Equation (2.1) are drawn from the q integers $0, 1, \cdots, q-1$, one of these remainders must be zero. This means that $q|p + td$ for some t satisfying $0 \leq t \leq q-1$. Because of the inequality $q < n \leq p \leq p + td$, we are forced to conclude that $p + td$ is composite. (If p were less than n, one of the terms of the progression would be $p + pd = p(l + d)$.) With this contradiction, the proof that $q|d$ is complete. □

Chapter 3

UNIT III

3.1 Basic properties of congruence

Definition 3.1.1. 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.

Theorem 3.1.2. *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.*

Proof. First take $a \equiv b(mod\ n)$, so that $a = b + kn$ for some integer k. Upon division by n, b leaves a certain remainder r; that is, $b = qn + r$, where $0 \leq r < n$. Therefore,

$$a = b + kn = (qn + r) + kn = (q + k)n + r$$

which indicates that a has the same remainder as b.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$$

whence $n|a-b$. In the language of congruences, we have $a \equiv b(mod\ n)$. □

Example 3.1.3. Because the integers -56 and -11 can be expressed in the form

$$-56 = (-7)9 + 7 \qquad -11 = (-2)9 + 7$$

with the same remainder 7, Theorem 3.1.2 tells us that $-56 \equiv -11(mod\ 9)$. Going in the other direction, the congruence $-31 \equiv 11(mod\ 7)$ implies that -31 and 11 have the same remainder when divided by 7; this is clear from the relations

$$-31 = (-5)7 + 4 \qquad 11 = 17 + 4$$

Theorem 3.1.4. *Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:*

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

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

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

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

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

(f) If $a \equiv b(mod\ n)$, *then* $ak \equiv bk(mod\ n)$ *for any positive integer* k.

Proof. For any integer a, we have $a - a = 0 \cdot n$, so that $a \equiv a(mod\ n)$. Now if $a \equiv b(mod\ n)$, then $a - b = kn$ for some integer k. Hence, $b - a = -(kn) = (-k)n$ and because $-k$ is an integer, this yields property (b).

Property (c) is slightly less obvious: Suppose that $a \equiv b(mod\ n)$ and also $b \equiv c(mod\ n)$. Then there exist integers h and k satisfying $a - b = hn$ and $b - c = kn$. It follows that

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n$$

which is $a \equiv c(mod\ n)$ in congruence notation.

In the same vein, if $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$, then we are assured that $a - b = k_1 n$ and $c - d = k_2 n$ for some choice of k_1 and k_2. Adding these equations, we obtain

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= k_1 n + k_2 n = (k_1 + k_2)n\end{aligned}$$

or, as a congruence statement, $a + c \equiv b + d(mod\ n)$. As regards the second assertion of property (d), note that

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

Because $bk_2 + dk_1 + k_1 k_2 n$ is an integer, this says that $ac - bd$ is divisible by n, whence $ac \equiv bd(mod\ n)$.

The proof of property (e) is covered by (d) and the fact that $c \equiv c(mod\ n)$. Finally, we obtain property (f) by making an induction argument. The statement certainly holds for $k = 1$, and we will assume it is true for some fixed k. From (d), we know that $a \equiv b(mod\ n)$ and $a^k \equiv b^k(mod\ n)$ together imply that $aa^k \equiv bb^k(mod\ n)$, or equivalently $a^{k+1} \equiv b^{k+1}(mod\ n)$. This is the form the statement should take for $k + 1$, and so the induction step is complete. □

Example 3.1.5. Show that 41 divides $220 - 1$. We begin by noting that $2^5 \equiv -9(mod\ 41)$, whence $(2^5)^4 \equiv (-9)^4(mod\ 41)$ by Theorem 3.1.4(f); in other words, $2^{20} \equiv 81 \cdot 81(mod\ 41)$. But $81 \equiv -1(mod\ 41)$, and so $81 \cdot 81 \equiv 1(mod\ 41)$. Using parts (b) and (e) of Theorem 3.1.4, we finally arrive at

$$2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0(mod\ 41)$$

Thus, $41|2^{20} - 1$, as desired.

Example 3.1.6. For another example in the same spirit, suppose that we are asked to find the remainder obtained upon dividing the sum

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

by 12. Without the aid of congruences this would be an awesome calculation. The observation that starts us off is that $4! \equiv 24 \equiv 0(mod 12)$; thus, for $k \geq 4$,

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k \equiv 0(mod\ 12)$$

In this way, we find that

$$1! + 2! + 3! + 4! + \cdots + 100! \equiv 1! + 2! + 3! + 0 + \cdots + 0 \equiv 9(mod\ 12)$$

Accordingly, the sum in question leaves a remainder of 9 when divided by 12.

Theorem 3.1.7. *If $ca \equiv cb(mod\ n)$, then $a \equiv b(mod\ n/d)$, where $d = gcd(c, n)$.*

Proof. By hypothesis, we can write

$$c(a - b) = ca - cb = kn$$

for some integer k. Knowing that $gcd(c, n) = d$, there exist relatively prime integers r and s satisfying $c = dr$, $n = ds$. When these values are substituted in the displayed equation and the common factor d canceled, the net result is

$$r(a - b) = ks$$

Hence, $s|r(a - b)$ and $gcd(r, s) = 1$. Euclid's lemma yields $s|a - b$, which may be recast as $a \equiv b(mod\ s)$; in other words, $a \equiv b(mod\ n/d)$. □

Corollary 3.1.8. *If $ca \equiv cb(mod\ n)$ and $gcd(c, n) = 1$, then $a \equiv b(modn)$.*

Corollary 3.1.9. *If $ca \equiv cb(mod\ p)$ and $p \nmid c$, where p is a prime number, then $a \equiv b(mod\ p)$.*

Proof. The conditions $p \nmid c$ and p a prime imply that $gcd(c, p) = 1$. □

Example 3.1.10. Consider the congruence $33 \equiv 15(mod\ 9)$ or, if one prefers, $3 \cdot 11 \equiv 3 \cdot 5(mod\ 9)$. Because $gcd(3,9) = 3$, Theorem 3.1.7 leads to the conclusion that $11 \equiv 5(mod\ 3)$.
A further illustration is given by the congruence $-35 \equiv 45(mod\ 8)$, which is the same as $5 \cdot (-7) \equiv 5 \cdot 9(mod\ 8)$. The integers 5 and 8 being relatively prime, we may cancel the factor 5 to obtain a correct congruence $-7 \equiv 9(mod\ 8)$.

3.2 Binary and Decimal Representations of Integers

Example 3.2.1. To calculate $5^{110}(mod\ 131)$, first note that the exponent 110 can be expressed in binary form as

$$110 = 64 + 32 + 8 + 4 + 2 = (110110)_2$$

Thus, we obtain the powers $5^{2^j}(mod\ 131)$ for $0 \leq j \leq 6$ by repeatedly squaring while at each stage reducing each result modulo 131:

$$\begin{array}{cc} 52 \equiv 25(mod\ 131) & 516 \equiv 27(mod\ 131) \\ 54 \equiv 101(mod\ 131) & 532 \equiv 74(mod\ 131) \\ 58 \equiv 114(mod\ 131) & 564 \equiv 105(mod\ 131) \end{array}$$

When the appropriate partial results-those corresponding to the 1's in the binary expansion of 110—are multiplied, we see that

$$\begin{aligned} 5^{110} &= 5^{64+32+8+4+2} \\ &= 5^{64} \cdot 5^{32} \cdot 5^{8} \cdot 5^{4} \cdot 5^{2} \\ &\equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60(mod\ 131) \end{aligned}$$

As a minor variation of the procedure, one might calculate, modulo 131, the powers $5, 5^2, 5^3, 5^6, 5^{12}, 5^{24}, 5^{48}, 5^{96}$ to arrive at

$$5^{ll0} = 5^{96} \cdot 5^{12} \cdot 5^{2} \equiv 41 \cdot 117 \cdot 25 \equiv 60(mod\ 131)$$

which would require two fewer multiplications.

Theorem 3.2.2. *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 $P(a) \equiv P(b)(mod\ n)$.*

Proof. Because $a \equiv b(mod\ n)$, part(f) of Theorem 3.1.4 can be applied to give $a^k \equiv b^k(mod\ n)$ for $k = 0, 1, \cdots, m$. Therefore,

$$c_k a^k \equiv c_k b^k (mod\ n)$$

for all such k. Adding these $m + 1$ congruences, we conclude that

$$\sum_{k=0}^{m} c_k a^k = \sum_{k=0}^{m} c_k b^k (mod\ n)$$

or, in different notation, $P(a) \equiv P(b)(mod\ n)$. □

Corollary 3.2.3. *If a is a solution of $P(x) \equiv 0(mod\ n)$ and $a \equiv b(mod\ n)$, then b also is a solution.*

Proof. From the last theorem, it is known that $P(a) \equiv P(b)(mod\ n)$. Hence, if a is a solution of $P(x) \equiv 0(mod\ n)$, then $P(b) \equiv P(a) \equiv 0(mod\ n)$, making b a solution. □

Theorem 3.2.4. *Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ 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 $9|N$ if and only if $9|S$.*

Proof. Consider $P(x) = \sum_{k=0}^{m} a_k x^k$, a polynomial with integral coefficients. The key observation is that $10 \equiv 1(mod\ 9)$, whence by Theorem 3.2.2, $P(10) \equiv P(l)(mod\ 9)$. But $P(10) = N$ and $P(1) = a_0 + a_1 + \cdots + a_m = S$, so that $N \equiv S(mod\ 9)$. It follows that $N \equiv 0(mod\ 9)$ if and only if $S \equiv 0(mod\ 9)$, which is what we wanted to prove. □

Theorem 3.2.5. *Let* $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ *be the decimal expansion of the positive integer* N, $0 \leq a_k < 10$, *and let* $T = a_0 - a_1 + a_2 - \cdots + (-l)^m a_m$. *Then* $11|N$ *if and only if* $11|T$.

Proof. As in the proof of Theorem 3.2.4, put $P(x) = \sum_{k=0}^{m} a_k x^k$. Because $10 \equiv -1(mod\ 11)$, we get $P(10) \equiv P(-1)(mod\ 11)$. But $P(10) = N$, whereas $P(-1) = a_0 - a_1 + a_2 - \cdots + (-l)^m a_m = T$, so that $N = T(mod\ 11)$. The implication is that either both N and T are divisible by 11 or neither is divisible by 11. $\square$

Example 3.2.6. To see an illustration of the last two results, take the integer $N = 1,571,724$. Because the sum

$$1 + 5 + 7 + 1 + 7 + 2 + 4 = 27$$

is divisible by 9, Theorem 3.2.4 guarantees that 9 divides N. It also can be divided by 11; for, the alternating sum

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

is divisible by 11.

3.3 Linear Congruence and The Chinese Remainder Theorem

Theorem 3.3.1. *The linear congruence* $ax = b(mod\ n)$ *has a solution if and only if* $d|b$, *where* $d = gcd(a, n)$. *If* $d|b$, *then it has* d *mutually incongruent solutions modulo* n.

Proof. We already have observed that the given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. From Theorem 1.6.1, it is known that the latter equation can be solved if and only if $d|b$; moreover, if it is solvable and x_0, y_0 is one specific solution, then any other solution has the form

$$x = x_0 + \tfrac{n}{d}t \quad y = y_0 + \tfrac{a}{d}t$$

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 $t = 0, 1, 2, \cdots, d-1$:

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

We claim that these integers are incongruent modulo n, and all other such integers x are congruent to some one of them. If it happened that

$$x_0 + \tfrac{n}{d}t_1 \equiv x_0 + \tfrac{n}{d}t_2 (mod\ n)$$

where $0 \leq t_1 < t_2 \leq d-1$, then we would have

$$\tfrac{n}{d}t_1 \equiv \tfrac{n}{d}t_2 (mod\ n)$$

Now $gcd(n/d, n) = n/d$, and therefore by Theorem 2.1.7 the factor n/d could be canceled to arrive at the congruence

$$t_1 \equiv t_2 (mod\ d)$$

which is to say that $d|t_2 - t_1$. But this is impossible in view of the inequality $0 < t_2 - t_1 < d$.

It remains to argue that any other solution $x_0 + (n/d)t$ is congruent modulo n to one of the d integers listed above. The Division Algorithm permits us to write t as $t = qd + r$, where $0 \leq r \leq d-1$. Hence

$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &= x_0 + \frac{n}{d}r (mod\ n) \end{aligned}$$

with $x_0 + (n/d)r$ being one of our d selected solutions. This ends the proof. □

Corollary 3.3.2. *If $gcd(a, n) = 1$, then the linear congruence $ax \equiv b(mod\ n)$ has a unique solution modulo n.*

Example 3.3.3. First consider the linear congruence $18x \equiv 30(mod\ 42)$. Because $gcd(18, 42) = 6$ and 6 surely divides 30, Theorem 3.3.1 guarantees the existence of exactly six solutions, which are incongruent modulo 42. By inspection, one solution is found to be $x = 4$. Our analysis tells us that the six solutions are as follows:

$$x \equiv 4 + (42/6)t \equiv 4 + 7t(mod\ 42) \qquad t = 0, 1, \cdots, 5$$

or, plainly enumerated,

$$x \equiv 4, 11, 18, 25, 32, 39(mod 42)$$

Example 3.3.4. Let us solve the linear congruence $9x \equiv 21(mod\ 30)$. At the outset, because $gcd(9, 30) = 3$ and $3|21$, we know that there must be three incongruent solutions.

One way to find these solutions is to divide the given congruence through by 3, thereby replacing it by the equivalent congruence $3x \equiv 7(mod\ 10)$. The relative primeness of 3 and 10 implies that the latter congruence admits a unique solution modulo 10. Although it is not the most efficient method, we could test the integers $0, 1, 2, \cdots, 9$ in turn until the solution is obtained. A better way is this: Multiply both sides of the congruence $3x \equiv 7(mod\ 10)$ by 7 to get

$$21x \equiv 49(mod\ 10)$$

which reduces to $x \equiv 9(mod\ 10)$. (This simplification is no accident, for the multiples $0 \cdot 3, 1 \cdot 3, 2 \cdot 3, \cdots, 9 \cdot 3$ form a complete set of residues modulo 10; hence, one of them is necessarily congruent to 1 modulo 10.) But the original congruence was given modulo 30, so that its incongruent solutions are sought among the integers $0, 1, 2, \cdots, 29$. Taking $t = 0, 1, 2$, in the formula

x=9+10t

we obtain $9, 19, 29$, whence

$$x \equiv 9(mod\ 30) \qquad x \equiv 19(mod\ 30) \qquad x \equiv 29(mod\ 30)$$

are the required three solutions of $9x \equiv 21(mod\ 30)$.

A different approach to the problem is to use the method that is suggested in the proof of Theorem 3.3.1. Because the congruence $9x \equiv 21(mod 30)$ is equivalent to the linear Diophantine equation

$$9x - 30y = 21$$

we begin by expressing $3 = gcd(9, 30)$ as a linear combination of 9 and 30. It is found, either by inspection or by using the Euclidean Algorithm, that $3 = 9(-3) + 30 \cdot 1$, so that

$$21 = 7 \cdot 3 = 9(-21) - 30(-7)$$

Thus, $x = -21$, $y = -7$ satisfy the Diophantine equation and, in consequence, all solutions of the congruence in question are to be found from the formula

$$x = -21 + (30/3)t = -21 + 10t$$

The integers $x = -21 + 10t$, where $t = 0, 1, 2$, are incongruent modulo 30 (but all are congruent modulo 10); thus, we end up with the incongruent solutions

$$x \equiv -21(mod\ 30) \quad x \equiv -11(mod\ 30) \quad x \equiv -1(mod\ 30)$$

or, if one prefers positive numbers, $x \equiv 9, 19, 29(mod\ 30)$.

Theorem 3.3.5 (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*

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

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

Proof. We start by forming the product $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \cdots, r$, let

$$N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r,$$

In words, N_k is the product of all the integers n_i with the factor n_k omitted. By hypothesis, the n_i are relatively prime in pairs, so that $gcd(N_k, n_k) = 1$. According to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 (mod\ n_k)$; call the unique solution x_k. Our aim is to prove that the integer

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

is a simultaneous solution of the given system.

First, observe that $N_i \equiv 0 (mod\ n_k)$ for $i \neq k$, because $n_k | N_i$ in this case. The result is

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k (mod\ nk)$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 (mod\ n_k)$, which forces

$$\bar{x} \equiv a_k \cdot 1 \equiv a_k (mod\ n_k)$$

This shows that a solution to the given system of congruences exists.

As for the uniqueness assertion, suppose that x' is any other integer that satisfies these congruences. Then

$$\bar{x} \equiv a_k \equiv x' (mod\ n_k) \quad k = 1, 2, \cdots, r$$

and so $n_k | \bar{x} - x'$ for each value of k. Because $gcd(n_i, n_j) = 1$, Corollary 2 to Theorem 1.4.8 supplies us with the crucial point that $n_1 n_2 \cdots n_r | \bar{x} - x'$; hence $\bar{x} \equiv x' (mod\ n)$. With this, the Chinese Remainder Theorem is proven. $\square$

Example 3.3.6. The problem posed by Sun-Tsu corresponds to the system of three congruences

$$\begin{aligned} x &\equiv 2(mod\ 3) \\ x &\equiv 3(mod\ 5) \\ x &\equiv 2(mod\ 7) \end{aligned}$$

In the notation of Theorem 3.3.5, we have $n = 3 \cdot 5 \cdot 7 = 105$ and

$$N_1 = \tfrac{n}{3} = 35 \quad N_2 = \tfrac{n}{5} = 21 \quad N_3 = \tfrac{n}{7} = 15$$

Now the linear congruences

$$35x \equiv 1(mod\ 3) \quad 21x \equiv 1(mod\ 5) \quad 15x \equiv 1(mod\ 7)$$

are satisfied by $x_1 = 2$, $x_2 = 1$, $x_3 = 1$, respectively. Thus, a solution of the system is given by

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

Modulo 105, we get the unique solution $x = 233 = 23(mod\ 105)$.

Example 3.3.7. For a second illustration, let us solve the linear congruence

$$17x \equiv 9(mod\ 276)$$

Because $276 = 3 \cdot 4 \cdot 23$, this is equivalent to finding a solution for the system of congruences

$$\begin{array}{cc} 17x \equiv 9(mod\ 3) & x \equiv 0(mod\ 3) \\ 17x \equiv 9(mod\ 4) & x \equiv 1(mod\ 4) \\ 17x \equiv 9(mod\ 23) & 17x \equiv 9(mod\ 23) \end{array}$$

Note that if $x \equiv 0(mod\ 3)$, then $x = 3k$ for any integer k. We substitute into the second congruence of the system and obtain

$$3k \equiv 1(mod\ 4)$$

Multiplication of both sides of this congruence by 3 gives us

$$k \equiv 9k \equiv 3(mod\ 4)$$

so that $k = 3 + 4j$, where j is an integer. Then

$$x = 3(3 + 4j) = 9 + 12j$$

For x to satisfy the last congruence, we must have

$$17(9 + 12j) \equiv 9(mod\ 23)$$

or $204j \equiv -144(mod\ 23)$, which reduces to $3j \equiv 6(mod\ 23)$; in consequence, $j \equiv 2(mod\ 23)$. This yields $j = 2 + 23t$, with t an integer, whence

$$x = 9 + 12(2 + 23t) = 33 + 276t$$

All in all, $x \equiv 33(mod\ 276)$ provides a solution to the system of congruences and, in turn, a solution to $17x \equiv 9(mod\ 276)$.

Theorem 3.3.8. *The system of linear congruences*

$$\begin{aligned} ax + by &\equiv r(mod\ n) \\ cx + dy &\equiv s(mod\ n) \end{aligned}$$

has a unique solution modulo n *whenever* $gcd(ad - bc, n) = 1$.

Proof. Let us multiply the first congruence of the system by d, the second congruence by b, and subtract the lower result from the upper. These calculations yield

$$(ad - bc)x \equiv dr - bs(mod\ n) \tag{3.1}$$

The assumption $gcd(ad - bc, n) = 1$ ensures that the congruence

$$(ad - bc)z \equiv 1(mod\ n)$$

possess a unique solution; denote the solution by t. When congruence (3.1) is multiplied by t, we obtain

$$x \equiv t(dr - bs)(mod\ n)$$

A value for y is found by a similar elimination process. That is, multiply the first congruence of the system by c, the second one by a, and subtract to end up with

$$(ad - bc)y \equiv as - cr(mod\ n) \tag{3.2}$$

Multiplication of this congruence by t leads to

$$y \equiv t(as - cr)(mod\ n)$$

A solution of the system is now established. □

Example 3.3.9. Consider the system

$$\begin{aligned} 7x + 3y &\equiv 10(mod 16) \\ 2x + 5y &\equiv 9(mod 16) \end{aligned}$$

Because $gcd(7 \cdot 5 - 2 \cdot 3, 16) = gcd(29, 16) = 1$, a solution exists. It is obtained by the method developed in the proof of Theorem 3.3.8. Multiplying the first congruence by 5, the second one by 3, and subtracting, we arrive at

$$29x \equiv 5 \cdot 10 - 3 \cdot 9 \equiv 23(mod\ 16)$$

or, what is the same thing, $13x \equiv 7(mod\ 16)$. Multiplication of this congruence by 5 (noting that $5 \cdot 13 \equiv 1(mod\ 16)$) produces $x = 35 = 3(mod\ 16)$. When the variable x is eliminated from the system of congruences in a like manner, it is found that

$$29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43(mod\ 16)$$

But then $13y \equiv 11 (mod\ 16)$, which upon multiplication by 5, results in $y \equiv 55 \equiv 7 (mod\ 16)$. The unique solution of our system turns out to be

$$x \equiv 3 (mod\ 16) \qquad y \equiv 7 (mod\ 16)$$

Chapter 4

UNIT IV

4.1 Fermat's Little Theorem and Pseudo primes

Theorem 4.1.1 (Fermat's theorem)**.** *Let p be a prime and suppose that $p|a$. Then $a^{p-1} \equiv 1(mod\ p)$.*

Proof. We begin by considering the first $p-1$ positive multiples of a; that is, the integers

$$a, 2a, 3a, \cdots, (p-1)a$$

None of these numbers is congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that

$$ra \equiv sa(mod\ p) \quad 1 \leq r < s \leq p-1$$

then a could be canceled to give $r \equiv s(mod\ p)$, which is impossible. Therefore, the previous set of integers must be congruent modulo p to $1, 2, 3, \cdots, p-1$, taken in some order. Multiplying all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)(mod\ p)$$

whence

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

Once $(p-1)!$ is canceled from both sides of the preceding congruence (this is possible because since $p|(p-1)!$), our line of reasoning culminates in the statement that $a^{p-l} \equiv 1(mod\ p)$, which is Fermat's theorem. □

Corollary 4.1.2. *If p is a prime, then $a^p \equiv a(mod\ p)$ for any integer a.*

Proof. When $p|a$, the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a(mod\ p)$. If $p \nmid a$, then according to Fermat's theorem, we have $a^{p-1} \equiv 1(mod\ p)$. When this congruence is multiplied by a, the conclusion $a^p \equiv a(mod\ p)$ follows. □

Lemma 4.1.3. *If p and q are distinct primes with $a^p \equiv a(mod\ q)$ and $a^q \equiv a(mod\ p)$, then $a^{pq} \equiv a(mod\ pq)$.*

Proof. The last corollary tells us that $(a^q)^p \equiv a^q(mod\ p)$, whereas $a^q \equiv a(mod\ p)$ holds by hypothesis. Combining these congruences, we obtain $a^{pq} \equiv a(mod\ p)$ or, in different terms, $p|a^{pq} - a$. In an entirely similar manner, $q|a^{pq} - a$. Corollary 2 to Theorem 1.4.8 now yields $pq|a^{pq} - a$, which can be recast as $a^{pq} \equiv a(mod\ pq)$. □

Theorem 4.1.4. *If n is an odd pseudo prime, then $M_n = 2^n - 1$ is a larger one.*

Proof. Because n is a composite number, we can write $n = rs$, with $1 < r \leq s < n$. Then, according to Problem 21, Section 2.3, $2^r - 1|2^n - 1$, or equivalently $2^r - 1|M_n$, making M_n composite. By our hypotheses, $2^n \equiv 2(mod\ n)$; hence $2^n - 2 = kn$ for some integer k. It follows that

$$2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}$$

This yields

$$\begin{aligned} 2^{M_n - 1} &= 2^{kn} - 1 \\ &= (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &= M_n(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &= 0(mod\ M_n) \end{aligned}$$

We see immediately that $2^{M_n} - 2 \equiv 0(mod\ M_n)$, in light of which M_n is a pseudo prime. □

Theorem 4.1.5. *Let n be a composite square-free integer, say, $n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes. If $p_i - 1|n - 1$ for $i = 1, 2, \cdots, r$, then n is an absolute pseudo prime.*

Proof. Suppose that a is an integer satisfying $gcd(a, n) = 1$, so that $gcd(a, p_i) = 1$ for each i. Then Fermat's theorem yields $p_i|a^{p_i - l} - 1$. From the divisibility hypothesis $p_i - 1|n - 1$, we have $p_i|a^{n-1} - 1$, and therefore $p_i|a^n - a$ for all a and $i = 1, 2, \cdots, r$. As a result of Corollary 2 to Theorem 1.4.8, we end up with $n|a^n - a$, which makes n an absolute pseudo prime. □

4.2 Wilson's Theorem

Theorem 4.2.1 (Wilson)**.** *If p is a prime, then $(p - 1)! \equiv -1(mod\ p)$.*

Proof. Dismissing the cases $p = 2$ and $p = 3$ as being evident, let us take $p > 3$. Suppose that a is any one of the $p - 1$ positive integers

$$1, 2, 3, \cdots, p - 1$$

and consider the linear congruence $ax \equiv 1(mod\ p)$. Then $gcd(a, p) = 1$. By Theorem 3.3.1, this congruence admits a unique solution modulo p; hence, there is a unique integer a', with $1 \leq a' \leq p - 1$, satisfying $aa' \equiv 1(mod\ p)$.

Because p is prime, $a = a'$ if and only if $a = 1$ or $a = p - 1$. Indeed, the congruence $a^2 \equiv 1(mod\ p)$ is equivalent to $(a - 1) \cdot (a + 1) \equiv 0(mod\ p)$. Therefore, either $a - 1 \equiv 0(mod\ p)$, in which case $a = 1$, or $a + 1 \equiv 0(mod\ p)$, in which case $a = p - 1$.

If we omit the numbers 1 and $p - 1$, the effect is to group the remaining integers $2, 3, \cdots, p - 2$ into pairs a, a', where $a \neq a'$, such that their product $aa' \equiv 1(mod\ p)$. When these $(p - 3)/2$ congruences are multiplied together and the factors rearranged, we get

$$2 \cdot 3 \cdots (p-2) \equiv 1(mod\ p)$$

or rather

$$(p-2)! \equiv 1(mod\ p)$$

Now multiply by $p-1$ to obtain the congruence

$$(p-1)! \equiv p-1 \equiv -1(mod\ p)$$

as was to be proved. □

Example 4.2.2. A concrete example should help to clarify the proof of Wilson's theorem. Specifically, let us take $p = 13$. It is possible to divide the integers $2, 3, \cdots, 11$ into $(p-3)/2 = 5$ pairs, each product of which is congruent to 1 modulo 13. To write these congruences out explicitly:

$$\begin{aligned} 2 \cdot 7 &= 1(mod\ 13) \\ 3 \cdot 9 &= 1(mod\ 13) \\ 4 \cdot 10 &= 1(mod\ 13) \\ 5 \cdot 8 &= 1(mod\ 13) \\ 6 \cdot 11 &= 1(mod\ 13) \end{aligned}$$

Multiplying these congruences gives the result

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

and so

$$12! \equiv 12 \equiv -1(mod\ 13)$$

Thus, $(p-1)! \equiv -1(mod\ p)$, with $p = 13$.

Theorem 4.2.3. *The quadratic congruence $x^2 + 1 \equiv 0(mod\ p)$, where p is an odd prime, has a solution if and only if $p \equiv 1(mod\ 4)$.*

Proof. Let a be any solution of $x^2+1 \equiv 0(mod\ p)$, so that $a^2 \equiv -1(mod\ p)$. Because $p \nmid a$, the outcome of applying Fermat's theorem is

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}(mod\ p)$$

The possibility that $p = 4k+3$ for some k does not arise. If it did, we would have

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$$

hence, $1 \equiv -1(mod\ p)$. The net result of this is that $p|2$, which is patently false. Therefore, p must be of the form $4k+1$.

Now for the opposite direction. In the product

$$(p-1)! = 1 \cdot 2 \cdots \tfrac{p-1}{2} \cdot \tfrac{p+1}{2} \cdots (p-2)(p-1)$$

we have the congruences

$$\begin{aligned} p-1 &\equiv -1(mod\ p) \\ p-2 &\equiv -2(mod\ p) \\ &\ \ \vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2}(mod\ p) \end{aligned}$$

Rearranging the factors produces

$$\begin{aligned} (p-1)! &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right)(mod\ p) \\ &\equiv (-1)^{(p-l)/2}\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 (mod\ p) \end{aligned}$$

because there are $(p-1)/2$ minus signs involved. It is at this point that Wilson's theorem can be brought to bear; for, $(p-1)! \equiv -1(mod\ p)$, whence

$$-1 \equiv (-1)^{(p-1)/2}\left[(\tfrac{p-1}{2})!\right]^2 (mod\ p)$$

If we assume that p is of the form $4k+1$, then $(-1)^{(p-1)/2} = 1$, leaving us with the congruence

$$-1 \equiv \left[\left(\tfrac{p-1}{2}\right)!\right]^2 (mod\ p)$$

The conclusion is that the integer $[(p-1)/2]!$ satisfies the quadratic congruence $x^2 + 1 \equiv 0(mod\ p)$. $\square$

4.3 The Fermat-Kraitchik Factorization Method

Example 4.3.1. To illustrate the application of Fermat's method, let us factor the integer $n = 119143$. From a table of squares, we find that $345^2 < 119143 < 346^2$; thus it suffices to consider values of $k^2 - 119143$ for those k that satisfy the inequality $346 \leq k < (119143+1)/2 = 59572$. The calculations begin as follows:

$$\begin{aligned}
3462 - 119143 &= 119716 - 119143 = 573 \\
3472 - 119143 &= 120409 - 119143 = 1266 \\
3482 - 119143 &= 121104 - 119143 = 1961 \\
3492 - 119143 &= 121801 - 119143 = 2658 \\
3502 - 119143 &= 122500 - 119143 = 3357 \\
3512 - 119143 &= 123201 - 119143 = 4058 \\
3522 - 119143 &= 123904 - 119143 = 4761 = 692
\end{aligned}$$

This last line exhibits the factorization

$$119143 = 352^2 - 69^2 = (352+69)(352-69) = 421 \cdot 283$$

the two factors themselves being prime. In only seven trials, we have obtained the prime factorization of the number 119143. Of course, one does not always fare so luckily; it may take many steps before a difference turns out to be a square.

Example 4.3.2. Suppose we wish to factor the positive integer $n = 2189$ and happen to notice that $579^2 \equiv 18^2 (mod\ 2189)$. Then we compute

$$gcd(579 - 18, 2189) = gcd(561, 2189) = 11$$

using the Euclidean Algorithm:

$$\begin{aligned} 2189 &= 3 \cdot 561 + 506 \\ 561 &= 1 \cdot 506 + 55 \\ 506 &= 9 \cdot 55 + 11 \\ 55 &= 5 \cdot 11 \end{aligned}$$

This leads to the prime divisor 11 of 2189. The other factor, namely 199, can be obtained by observing that

$$gcd(579 + 18, 2189) = gcd(597, 2189) = 199$$

Example 4.3.3. Let $n = 12499$ be the integer to be factored. The first square just larger than n is $112^2 = 12544$. So we begin by considering the sequence of numbers $x^2 - n$ for $x = 112, 113, \cdots$. As before, our interest is in obtaining a set of values $x_1, x_2, \cdots, x_k$ for which the product $(x_i - n) \cdots (x_k - n)$ is a square, say y^2. Then $(x_1 \cdots x_k)^2 \equiv y^2 (mod\ n)$, which might lead to a nontrivial factor of n.

A short search reveals that

$$\begin{aligned} 112^2 - 12499 &= 45 \\ 117^2 - 12499 &= 1190 \\ 121^2 - 12499 &= 2142 \end{aligned}$$

or, written as congruences,

$$\begin{aligned} 112^2 &\equiv 3^2 \cdot 5 (mod\ 12499) \\ 117^2 &\equiv 2 \cdot 5 \cdot 7 \cdot 17 (mod\ 12499) \\ 121^2 &\equiv 2.3^2 \cdot 7 \cdot 17 (mod\ 12499) \end{aligned}$$

Multiplying these together results in the congruence

$$(112 \cdot 117 \cdot 121)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17)^2 (mod\ 12499)$$

that is,

$$1585584^2 \equiv 10710^2 (mod\ 12499)$$

But we are unlucky with this square combination. Because

$$1585584 \equiv 10710 (mod\ 12499)$$

only a trivial divisor of 12499 will be found. To be specific,

$$\begin{aligned} gcd(1585584 + 10710, 12499) &= 1 \\ gcd(1585584 - 10710, 12499) &= 12499 \end{aligned}$$

After further calculation, we notice that

$$\begin{aligned} 113^2 &\equiv 2 \cdot 5 \cdot 3^3 (mod\ 12499) \\ 127^2 &\equiv 2 \cdot 3 \cdot 5 \cdot 11^2 (mod\ 12499) \end{aligned}$$

which gives rise to the congruence

$$(113 \cdot 127)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 11)^2 (mod\ 12499)$$

This reduces modulo 12499 to

$$1852^2 \equiv 990^2 (mod\ 12499)$$

and fortunately $1852 \neq \pm 990 (mod\ 12499)$. Calculating

$$gcd(1852 - 990, 12499) = gcd(862, 12499) = 431$$

produces the factorization $12499 = 29 \cdot 431$.

Chapter 5

UNIT V

5.1 The sum and number of divisors

Definition 5.1.1. Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and a $\sigma(n)$ denote the sum of these divisors.

Theorem 5.1.2. *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*

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

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

Proof. Note that the divisor $d = 1$ is obtained when $a_1 = a_2 = \cdots = a_r = 0$, and n itself occurs when $a_1 = k_1, a_2 = k_2, \cdots, a_r = k_r$. Suppose that d divides n non trivially; say, $n = dd'$, where $d > 1$, $d' > 1$. Express both d and d' as products of (not necessarily distinct) primes:

$$d = q_1 q_2 \cdots q_s \qquad d' = t_1 t_2 \cdots t_u$$

with q_i, t_j prime. Then

$$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 \cdots q_s t_1 \cdots t_u$$

are two prime factorizations of the positive integer n. By the uniqueness of the prime factorization, each prime q_i must be one of the p_j. Collecting the equal primes into a single integral power, we get

$$d = q_1 q_2 \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where the possibility that $a_i = 0$ is allowed.

Conversely, every number $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ $(0 \le a_i \le k_i)$ turns out to be a divisor of n. For we can write

$$\begin{aligned} n &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \\ &= (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})(p_1^{k_1-a_1} p_2^{k_2-a_2} \cdots p_r^{k_r-a_r}) \\ &= dd' \end{aligned}$$

with $d' = p_1^{k_1-a_1} p_2^{k_2-a_2} \cdots p_r^{k_r-a_r}$ and $k_i - a_i \ge 0$ for each i. Then $d' > 0$ and $d|n$. □

Theorem 5.1.3. *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) $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \frac{p_2^{k_2+1}-1}{p_2-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}$.

Proof. According to Theorem 5.1.2, the positive divisors of n are precisely those integers

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

where $0 \le a_i \le k_i$. There are $k_1 + 1$ choices for the exponent a_1; $k_2 + 1$ choices for $a_2, \cdots$; and $k_r + 1$ choices for a_r. Hence, there are

$$(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

possible divisors of n.

To evaluate $\sigma(n)$, consider the product

$$(1 + p_1 + p_1^2 + \cdots + p_1^{k_1})(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$$

Each positive divisor of n appears once and only once as a term in the expansion of this product, so that

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{k_1}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$$

Applying the formula for the sum of a finite geometric series to the ith factor on the right-hand side, we get

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i} = \frac{p_i^{k_i+1}-1}{p_i-1}$$

It follows that

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

□

Example 5.1.4. The number $180 = 2^2 \cdot 3^2 \cdot 5$ has

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

positive divisors. These are integers of the form

$$2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$$

where $a_1 = 0, 1, 2$; $a_2 = 0, 1, 2$; and $a_3 = 0, 1$. Specifically, we obtain

$$1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180$$

The sum of these integers is

$$\sigma(180) = \frac{2^3-1}{2-1}\frac{3^3-1}{3-1}\frac{5^2-1}{5-1} = \frac{7}{1}\frac{26}{2}\frac{24}{4} = 7 \cdot 13 \cdot 6 = 546$$

Definition 5.1.5. A number-theoretic function f is said to be *multiplicative* if

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

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

Theorem 5.1.6. *The functions τ and σ are both multiplicative functions.*

Proof. Let m and n be relatively prime integers. Because the result is trivially true if either m or n is equal to 1, we may assume that $m > 1$ and $n > 1$. If

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad \text{and} \quad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of m and n, then because $gcd(m, n) = 1$, no p_i can occur among the q_j. It follows that the prime factorization of the product mn is given by

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}$$

Appealing to Theorem 5.1.3, we obtain

$$\begin{aligned} \tau(mn) &= [(k_i + 1) \cdots (k_r + 1)][(j_1 + 1) \cdot (j_s + 1)] \\ &= \tau(m)\tau(n) \end{aligned}$$

In a similar fashion, Theorem 5.1.3 gives

$$\begin{aligned} \sigma(mn) &= \left[\frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}\right] \left[\frac{q_1^{j_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{j_s+1} - 1}{q_s - 1}\right] \\ &= \tau(m)\sigma(n) \end{aligned}$$

Thus, τ and σ are multiplicative functions. □

Lemma 5.1.7. *If $gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 | m$, $d_2 | n$ and $gcd(d_1, d_2) = 1$; furthermore, these products are all distinct.*

Proof. It is harmless to assume that $m > 1$ and $n > 1$; let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ be their respective prime factorizations. Inasmuch as the primes $p_1, \cdots, p_r, q_1, \cdots, q_s$ are all distinct, the prime factorization of mn is

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}$$

Hence, any positive divisor d of mn will be uniquely representable in the form

$$d = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} \qquad 0 \le a_i \le k_i, 0 \le b_i \le j_i$$

This allows us to write d as $d = d_1 d_2$, where $d_1 = p_1^{a_1} \cdots p_r^{a_r}$ divides m and $d_2 = q_1^{b_1} \cdots q_s^{b_s}$ divides n. Because no p_i is equal to any q_j. we surely must have $gcd(d_1, d_2) = 1$. □

Theorem 5.1.8. *If f is a multiplicative function and F is defined by*

$$F(n) = \sum_{d|n} f(d)$$

then F is also multiplicative.

Proof. Let m and n be relatively prime positive integers. Then

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) \end{aligned}$$

because every divisor d of mn can be uniquely written as a product of a divisor d_1 of m and a divisor d_2 of n, where $gcd(d_1, d_2) = 1$. By the definition of a multiplicative function,

$$f(d_1 d_2) = f(d_1) f(d_2)$$

It follows that

$$\begin{aligned} F(mn) &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) \\ &= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) \\ &= F(m) F(n) \end{aligned}$$

□

Corollary 5.1.9. *The functions τ and σ are multiplicative functions.*

Proof. We have mentioned that the constant function $f(n) = 1$ is multiplicative, as is the identity function $f(n) = n$. Because τ and σ may be represented in the form

$$\tau(n) = \sum_{d|n} 1 \quad \textit{and} \quad \sigma(n) = \sum_{d|n} d$$

the stated result follows immediately from Theorem 5.1.8. □

5.2 The Mobius Inversion Formula

Definition 5.2.1. For a positive integer n, define μ by the rules

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2|n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1p_2\cdots p_r, \text{where } p_i \text{ are distinct primes} \end{cases}$$

Theorem 5.2.2. *The function μ is a multiplicative function.*

Proof. We want to show that $\mu(mn) = \mu(m)\mu(n)$, whenever m and n are relatively prime. If either $p^2|m$ or $p^2|n$, p a prime, then $p^2|mn$; hence, $\mu(mn) = 0 = \mu(m)\mu(n)$, and the formula holds trivially. We therefore may assume that both m and n are square-free integers. Say, $m = p_1p_2\cdots p_r$, $n = q_1q_2\cdots q_s$, with all the primes p_i and q_j being distinct. Then

$$\begin{aligned} \mu(mn) = \mu(p_1\cdots p_rq_1\cdots q_s) &= (-l)^{r+s} \\ &= (-1)^r(-1)^s = \mu(m)\mu(n) \end{aligned}$$

which completes the proof. □

Theorem 5.2.3. *For each positive integer* $n \leq 1$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

where d *runs through the positive divisors of* n.

Theorem 5.2.4 (Mobius inversion formula)**.** *Let* F *and* f *be two number-theoretic functions related by the formula*

$$F(n) = \textstyle\sum_{d|n} f(d)$$

Then

$$f(n) = \textstyle\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

Proof. The two sums mentioned in the conclusion of the theorem are seen to be the same upon replacing the dummy index d by $d' = n/d$; as d ranges over all positive divisors of n, so does d'.

Carrying out the required computation, we get

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{c|(n/d)} f(c) \right) = \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d) f(c) \right) \tag{5.1}$$

It is easily verified that $d|n$ and $c|(n/d)$ if and only if $c|n$ and $d|(n/c)$. Because of this, the last expression in Equation (5.1) becomes

$$\sum_{d|n} \left(\sum_{c|(n/d)} \mu(d) f(c) \right) = \sum_{c|n} \left(\sum_{d|(n/c)} f(c) \mu(d) \right) = \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right) \tag{5.2}$$

In compliance with Theorem 5.2.3, the sum $\sum_{d|(n/c)} \mu(d)$ must vanish except when $n/c = 1$ (that is, when $n = c$), in which case it is equal to 1; the upshot is that the right-hand side of Equation (5.2) simplifies to

$$\begin{aligned}
\sum_{c|n}\left(f(c)\sum_{d|(n/c)}\mu(d)\right) &= \sum_{c=n} f(c)\cdot 1\\
&= f(n)
\end{aligned}$$

giving us the stated result. □

Theorem 5.2.5. *If F is a multiplicative function and*

$$F(n) = \textstyle\sum_{d|n} f(d)$$

then f is also multiplicative.

Proof. Let m and n be relatively prime positive integers. We recall that any divisor d of mn can be uniquely written as $d = d_1 d_2$, where $d_1|m$, $d_2|n$, and $gcd(d_1, d_2) = 1$. Thus, using the inversion formula,

$$\begin{aligned}
f(mn) &= \sum_{d|mn}\mu(d)F\left(\frac{mn}{d}\right)\\
&= \sum_{\substack{d_1|m\\ d_2|n}}\mu(d_1d_2)F\left(\frac{mn}{d_1d_2}\right)\\
&= \sum_{\substack{d_1|m\\ d_2|n}}\mu(d_1)\mu(d_2)F\left(\frac{m}{d_1}\right)F\left(\frac{n}{d_2}\right)\\
&= \sum_{d_1|m}\mu(d_1)F\left(\frac{m}{d_1}\right)\sum_{d_2|n}\mu(d_2)F\left(\frac{n}{d_2}\right)\\
&= f(m)f(n)
\end{aligned}$$

which is the assertion of the theorem. Needless to say, the multiplicative character of μ and of F is crucial to the previous calculation. □

5.3 The Greatest Integer Function

Definition 5.3.1. 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 $x - 1 < [x] \leq x$.

Theorem 5.3.2. *If n is a positive integer and p a prime, then the exponent of the highest power of p that divides $n!$ is*

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

where the series is finite, because $[n/p^k] = 0$ for $p^k > n$.

Proof. Among the first n positive integers, those divisible by p are $p, 2p, \cdots, tp$, where t is the largest integer such that $tp \leq n$; in other words, t is the largest integer less than or equal to n/p (which is to say $t = [n/p]$). Thus, there are exactly $[n/p]$ multiples of p occurring in the product that defines $n!$, namely,

$$p, 2p, \cdots, \left[\frac{n}{p}\right] p \tag{5.3}$$

The exponent of p in the prime factorization of $n!$ is obtained by adding to the number of integers in Equation (5.3), the number of integers among $1, 2, \cdots, n$ divisible by p^2, and then the number divisible by p^3, and so on. Reasoning as in the first paragraph, the integers between 1 and n that are divisible by p^2 are

$$p^2, 2p^2, \cdots, \left[\frac{n}{p^2}\right] p^2 \tag{5.4}$$

which are $[n/p^2]$ in number. Of these, $[n/p^3]$ are again divisible by p:

$$p^3, 2p^3, \cdots, \left[\frac{n}{p^3}\right] p^3 \tag{5.5}$$

After a finite number of repetitions of this process, we are led to conclude that the total number of times p divides $n!$ is

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

$\square$

Example 5.3.3. We would like to find the number of zeros with which the decimal representation of 50! terminates. In determining the number of times 10 enters into the product 50!, it is enough to find the exponents of 2 and 5 in the prime factorization of 50!, and then to select the smaller figure.

By direct calculation we see that

$$\begin{aligned}[50/2] + [50/2^2] + [50/2^3] + [50/2^4] + [50/2^5] \\ = 25 + 12 + 6 + 3 + 1 \\ = 47\end{aligned}$$

Theorem 6.9 tells us that 2^{47} divides 50!, but 2^{48} does not. Similarly,

$$[50/5] + [50/5^2] = 10 + 2 = 12$$

and so the highest power of 5 dividing 50! is 12. This means that 50! ends with 12 zeros.

Theorem 5.3.4. *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.

Proof. The argument rests on the observation that if a and b are arbitrary real numbers, then $[a+b] \leq [a]+[b]$. In particular, for each prime factor p of $r!(n-r)!$,

$$\left[\frac{n}{p^k}\right] \geq \left[\frac{r}{p^k}\right] + \left[\frac{(n-r)}{p^k}\right] \qquad k = 1, 2, \cdots$$

Adding these inequalities, we obtain

$$\sum_{k\geq 1} \left[\frac{n}{p^k}\right] \geq \sum_{k\geq 1} \left[\frac{r}{p^k}\right] + \sum_{k\geq 1} \left[\frac{(n-r)}{p^k}\right] \tag{5.6}$$

The left-hand side of Equation (5.6) gives the exponent of the highest power of the prime p that divides $n!$, whereas the right-hand side equals the highest power of this prime contained in $r!(n-r)!$. Hence, p appears in the numerator of $n!/r!(n-r)!$ at least as many times as it occurs in the denominator. Because this holds true for every prime divisor of the denominator, $r!(n-r)!$ must divide $n!$, making $n!/r!(n-r)!$ an integer. $\square$

Corollary 5.3.5. *For a positive integer r, the product of any r consecutive positive integers is divisible by $r!$.*

Proof. The product of r consecutive positive integers, the largest of which is n, is

$$n(n-1)(n-2)\cdots(n-r+1)$$

Now we have

$$n(n-1)\cdots(n-r+1) = \left(\frac{n!}{r!(n-r)}!\right) r!$$

Because $n!/r!(n-r)!$ is an integer by the theorem, it follows that $r!$ must divide the product $n(n-1)\cdots(n-r+1)$, as asserted. $\square$

Theorem 5.3.6. *Let f and F be number-theoretic functions such that*

$$F(n) = \sum_{d|n} f(d)$$

Then, for any positive integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

Proof. We begin by noting that

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d|n} f(d) \tag{5.7}$$

The strategy is to collect terms with equal values of $f(d)$ in this double sum. For a fixed positive integer $k \leq N$, the term $f(k)$ appears in $\sum_{d|n} f(d)$ if and only if k is a divisor of n. (Because each integer has itself as a divisor, the right-hand side of Equation (5.7) includes $f(k)$, at least once.) Now, to calculate the number of sums $\sum_{d|n} f(d)$ in which $f(k)$ occurs as a term, it is sufficient to find the number of integers among $1, 2, \cdots, N$, which are divisible by k. There are exactly $[N/k]$ of them:

$$k, 2k, 3k, \cdots, \left[\frac{N}{k}\right] k$$

Thus, for each k such that $1 \leq k \leq N$, $f(k)$ is a term of the sum $\sum_{d|n} f(d)$ for $[N/k]$ different positive integers less than or equal to N. Knowing this, we may rewrite the double sum in Equation (5.7) as

$$\sum_{n=1}^{N} \sum_{d|n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

and our task is complete. □

Corollary 5.3.7. *If N is a positive integer, then*

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$$

Proof. Noting that $\tau(n) = \sum_{d|n} 1$, we may writer for F and take f to be the constant function $f(n) = 1$ for all n. $\square$

Corollary 5.3.8. *If N is a positive integer, then*

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \left[\frac{N}{n}\right]$$

Example 5.3.9. *Consider the case $N = 6$. The definition of τ tells us that*

$$\sum_{n=1}^{6} \tau(n) = 14$$

By above Corollary,

$$\begin{aligned} \sum_{n=1}^{6} \left[\frac{6}{n}\right] &= [6] + [3] + [2] + [3/2] + [6/5] + [1] \\ &= 6 + 3 + 2 + 1 + 1 + 1 \\ &= 14 \end{aligned}$$

as it should. In the present case, we also have

$$\sum_{n=1}^{6} \sigma(n) = 33$$

and a simple calculation leads to

$$\begin{aligned} \sum_{n=1}^{6} n \left[\frac{6}{n}\right] &= 1[6] + 2[3] + 3[2] + 4[3/2] + 5[6/5] + 6[1] \\ &= 16 + 23 + 32 + 41 + 51 + 61 \\ &= 33 \end{aligned}$$