,2,3,4

Number Theory Olympiad Training Notes **Academic Year 2023/2024**

Lecture 1,2,3,4

Lecturer: Mahadi Ddamulira, B.Sc. M.Sc. Ph.D. Dept of Mathematics, Makerere University

This document is not official guidance!, rather a first approximation based upon one person's experience. There is no promise that the International Mathematical Olympiad (IMO), much less any particular country's exams, will follow this syllabus.

§1. Number Theory Olympiad Training

Outline

- Divisibility properties of the integers.
- Euclidean Algorithm and adjacent ideas, e.g. $\gcd(a, b) = \gcd(a - b, b)$.
- Basic results about primes like the Fundamental Theorem of Arithmetic.
- Modular arithmetic, and basic results like Fermat's Little Theorem, Chinese Remainder Theorem, modular inverses, orders modulo n.
- Exponents in prime factorization, and basic properties, such as $v_p(xy) = v_p(x) + v_p(y)$ or $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.
- Etc...

1.1 What is Number Theory?

Number Theory is primarily the **theory of numbers**. The theory of numbers is concerned, at least in its elementary aspects, with properties of the **integers**, $\mathbb{Z}$ and more particularly with the positive integers $1, 2, 3, 4, \ldots$ (also known as the **natural numbers**, $\mathbb{N}$). It is, arguably, believed that Number Theory is the oldest branch of mathematics.

1.2 The Integers, $\mathbb{Z}$

The set $\mathbb{Z}$ of all integers, which this course is all about, consists of all positive and negative integers as well as 0. Thus, $\mathbb{Z}$ is the set given by

$$\mathbb{Z} = \{\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\},$$

while the set of all *positive integers* $\mathbb{N}$, is given by

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}.$$

On $\mathbb{Z}$, there are two basic binary operations: **addition** (denoted $+$) and **multiplication** (denoted $\cdot$), that satisfy some basic properties from which every other property for $\mathbb{Z}$ emerges.

- **Commutativity property for addition and multiplication**:

$$a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a.$$

- **Associativity property for addition and multiplication**:

$$(a + b) + c = a + (b + c) \quad \text{and} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

- **Distributivity property of multiplication over addition**:

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

- In $\mathbb{Z}$ there are **identity elements** for the operations $+$ and $\cdot$; these are the elements 0 and 1, that satisfy the basic properties: $0 + a = a + 0 = a$ and $1 \cdot a = a \cdot 1 = a$, for every $a \in \mathbb{Z}$.
- The set $\mathbb{Z}$ allows **additive inverses** for its elements, in the sense that for every $a \in \mathbb{Z}$ there exists another integer in $\mathbb{Z}$, denoted by $-a$, such that $a + (-a) = (-a) + a = 0$.
- For multiplication in $\mathbb{Z}$, only the integer 1 has a **multiplicative inverse** in the sense that 1 is the only integer a such that there exists another integer, denoted by a^{-1} or by $1/a$, (namely 1 itself in this case) such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
- From the operations $+$ and $\cdot$ one can define two operations on $\mathbb{Z}$, namely **subtraction** (denoted $-$) and **division** (denoted $/$). Subtraction is a *binary operation* on $\mathbb{Z}$, that is, defined for any two integers in $\mathbb{Z}$, while division is not a binary operation and thus is defined only for some specific couple of integers in $\mathbb{Z}$.
- Subtraction and division are defined as follows:
  1. $a - b$ is defined by $a + (-b)$, that is, $a - b = a + (-b)$ for every $a, b \in \mathbb{Z}$.
  2. a/b is defined by the integer c if and only if $a = b \cdot c$.

1.3 Mathematical Induction

We begin this section with a very interesting property that will be useful in proving many other results.

Theorem 1.1 (Well-Ordering Principle (WOP)) *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 $b \in S$.*

We use the Well-Ordering Principle to show that the set of positive integers has what is known as the **Archimedean Property**.

Theorem 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,

$$S = \{b - na \mid n \text{ is a positive integer}\}$$

consists entirely of positive integers. By the Well-Ordering Principle, S possesses a least element, say, $b - ma$. Notice that $b - (m+1)a$ also lies in S, because S contains 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 does not hold; hence the property is proven true. ■

With the Well-Ordering Principle available, it is an easy mattter to derive the First Principle of Finite Induction, which provides a basis of proof called **mathematical induction**.

Theorem 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 the 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-Ordering Principle tells us that T possesses a least element, which we denote by a. Since $1 \in S$, certainly $a > 1$, and so $0 < a - 1 < a$. The choice of a as the smallest positive integer in T implies that $a - 1 \notin T$, or equivalently $a - 1 \in S$. By hypothesis, S must also contain $(a-1)+1 = a$, which contradicts the fact that $a \in T$. We conclude that the set T is empty and in consequence that the set S contain s all the positive integers. ■

Some important remark:

The First Principle of Finite Induction is also refereed to as the **Weak Principle of Finite Induction**.

Example 1.4 *We establish the following formula*

$$1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1), \tag{1.1}$$

for $n = 1, 2, 3, \ldots$, using the Weak Principle of Finite Induction.

Solution*: Let S denote the set of all positive integers n for which (1.1) is true.*

- *When $n = 1$, the formula becomes $1 = \frac{1}{2} \cdot 1 \cdot (1+1) = \frac{1}{2} \cdot 1 \cdot 2 = 1$. This means that $1 \in S$.*
- *Next, assume that the integer k belongs to S, so that*

$$1 + 2 + 3 + \cdots + k = \frac{1}{2}k(k+1). \tag{1.2}$$

- *To obtain the sum of the first $k+1$ integers, we merely add the next one, $(k+1)$ on both sides of (1.2). This gives,*

$$1 + 2 + 3 + \cdots + k + (k+1) = \frac{1}{2}k(k+1) + (k+1). \tag{1.3}$$

- *After some algebraic manipulation, the right-hand side of (1.3) becomes:*

$$\frac{1}{2}k(k+1) + (k+1) = (k+1)\left(\frac{1}{2}k + 1\right) = \frac{1}{2}(k+1)(k+2),$$

  which is precisely the right-hand side of (1.1) when $n = k+1$.

- *Our reasoning shows that $k+1 \in S$ whenever $k \in S$. By the Weak Principle of Finite Induction, S must be the set of all positive integers, that is, the given formula in (1.1) is true for $n = 1, 2, 3, \ldots$.*

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

Theorem 1.5 (Second Principle of Finite Induction) *Let S be a set of positive integers with the following properties:*

(a) The integer 1 belongs to S.

(b) If k is a positive integer such that the integers $1, 2, \ldots, k$ lie in S, then $k+1$ must also be in S.

Then S is the 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-Ordering Principle tells us that T has a least element, which we denote by n. Since $1 \in S$, certainly $n > 1$. The choice of n as the smallest positive integer in T implies that the integers $1, 2, \ldots, n-1 \notin T$, or equivalently $1, 2, \ldots, n-1 \in S$. By (b), S must also contain $(n-1)+1 = n$, which contradicts the fact that $n \in T$. We conclude that the set T is empty and in consequence that the set S contain s all the positive integers. ■

Some important remark:

The Second Principle of Finite Induction is also refereed to as the **Strong Principle of Finite Induction**.

Remark: The First Principle of Finite Induction is used more often than the Second Principle of Finite Induction, however, there are occasions when the second one is favored and thus, the reader should be familiar with both versions. It sometimes happens that in attempting to show that $k+1 \in S$, we require proof of the fact that not only $k \in S$, but all positive integers that precede k lie in S.

Example 1.6 *To illustrate a proof that requires the Second Principle of Finite Induction, we consider the so-called* **Lucas Sequence**, *whose first few terms are given by:*

$$\{L_n\}_{n\geq 1} = 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, \ldots.$$

This sequence, can also be defined recursively by

$$L_1 = 1, \quad L_2 = 3, \quad \text{and} \quad L_n = L_{n-1} + L_{n-2} \quad \text{for all} \quad n \geq 3.$$

We prove that the inequality

$$L_n < 2^n, \tag{1.4}$$

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

- *First of all, for $n = 1$ and $n = 2$, we have $L_1 = 1 < 2^1 = 2$ and $L_2 = 3 < 2^2 = 4$.*

  Hence, the inequality holds in these two cases. This provides the base case for this induction.

- *For the induction step, choose an integer $k \geq 3$ and assume that the inequality if true for $n = 1, 2, 3, \ldots, k-1$. Then, in particular, $L_{k-1} < 2^{k-1}$ and $L_{k-2} < 2^{k-2}$.*

- *By the way the Lucas sequence is defined, it follows that*

$$L_k = L_{k-1} + L_{k-2} < 2^{k-1} + 2^{k-2} = 2^{k-2}(2+1) = 3 \cdot 2^{k-2} < 2^2 \cdot 2^{k-2} = 2^k.$$

- *Because the inequality is true for $n = k$ whenever it is true for the integers $n = 1, 2, 3, \ldots, k-1$, we conclude by the Second Principle of Finite Induction that the inequality (1.4) is true for all $n \geq 1$.*

There is another version for induction!

Theorem 1.7 (Principle of Mathematical Induction) *Suppose that the proposition $P(n)$ satisfies:*

(a) $P(1)$ is true; and

(b) for every positive integer n, whenever $P(n)$ is true, then $P(n+1)$ is true.

Then $P(n)$ is true for all positive integers n.

Remarks:

1. Why is this sufficient? Well, suppose we have proved (i) and (ii) above. Then we know that $P(1)$ is true. Since $P(1) \Rightarrow P(2)$, we know that $P(2)$ is true. Since $P(2) \Rightarrow P(3)$, we know that $P(3)$ is true. Since $P(3) \Rightarrow P(4)$, we know that $P(4)$ is true. We can continue this indefinitely, so we see that $P(n)$ is true for every positive integer n.
2. A proof by induction consists of two parts. In the first part, called the **base case**, we show that $P(1)$ is true. In the second part, called the **induction step**, we assume that n is a positive integer such that $P(n)$ is true, and we deduce that $P(n+1)$ is true. The assumption that $P(n)$ is true is called the **induction hypothesis**.

The principle of mathematical induction can be proved from the Well-Ordering Principle. To see this:

Proof: Let us assume that the Well-Odering Principle is true and suppose that P is any proposition about positive integers such that $P(1)$ is true; and for every positive integer n, whenever $P(n)$ is true, then $P(n+1)$ is true. (These are the requirements for induction.) Write S for the set of positive integers n such that $P(n)$ is not true. In order to prove that induction works, we need to show that S is empty. If S is non-empty, then by the Well-Ordering Principle, S has a smallest element, say x. So, $P(x)$ is false. We know that $P(1)$ is true, so $x \neq 1$. But x is a positive integer, so $x-1$ is a positive integer, and $P(x)$ must be true–otherwie $x-1$ would be a member of S, asnd smaller than x. But this means that $P((x-1)+1)$ is true, that is, $P(x)$ is both true and false! This can't happen, so our original assumption, that S is non-empty, must have been wrong. So induction is proved. ■

Example 1.8 *Applications of Mathematical Induction.*

1. *Prove by induction that the sum of the first positive integers is:* $\sum_{i=1}^{n} i = 1+2+\cdots+n = \frac{1}{2}n(n+1)$.

   Proof: *The case $n=1$ is $\frac{1}{2}\cdot 1\cdot(1+1)=1$, which is obviously true, so the formula gives the correct answer when $n=1$. Suppose it is true for $n=k$; that is, $1+2+\cdots+k=\frac{1}{2}k(k+1)$, then we show that it also holds for $n=k+1$. That is,*

   $1+2+\cdots+k+(k+1)=\frac{1}{2}k(k+1)+(k+1)=\frac{1}{2}(k+1)(k+2)=\frac{1}{2}(k+1)((k+1)+1)$,

   and the formula is proved correct for $n=k+1$. So, by induction, we have the result. ■

2. *(Exercise) Use mathematical induction to prove that* $\sum_{i=1}^{n} i^2 = 1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$.

3. *Use mathematical induction to prove that $n! \leq n^n$ for all positive integers n.*

   Proof: *First note that, $1! = 1 \leq 1^1 = 1$, the statement holds for $n=1$.*

   Induction step, suppose that $n! \leq n^n$ for some n, then we show that $(n+1)! \leq (n+1)^{n+1}$.

   Indeed, $(n+1)! = (n+1)n! \leq (n+1)n^n < (n+1)(n+1)^n = (n+1)^{n+1}$.

   This completes the proof. ■

4. *Prove that* $n! \geq 2^n$ *whenever* $n \geq 4$.

   Proof: *Suppose that the proposition* $P(n)$ *means* $n! \geq 2^n$. *Then* $P(4)$ *means* $4! \geq 2^4$, *or* $24 \geq 16$, *which is true. That is,* $P(4)$ *is true. Now, suppose that* k *is an integer such that* $k \geq 4$; *and* $P(k)$ *is true; that is,* $k! \geq 2^k$. *Multiplying through by* $(k+1)$ *gives:*

   $$(k+1)! = (k+1)k! \geq (k+1) \cdot 2^k \geq 2 \cdot 2^k = 2^{k+1},$$

   so $P(k)$ *implies that* $P(k+1)$ *is true, and the result follows by induction.* ■

5. *Prove by induction that* $5^n - 2^n$ *is divisible by* 3 *whenever* n *is a positive integer.*

   Proof: *Suppose that* $P(n)$ *means* $5^n - 2^n$ *is divisible by* 3. *Then* $P(1)$ *is true, because* $5^1 - 2^1 = 5 - 2 = 3$. *Now suppose that* k *is any positive integer and that* $P(k)$ *is true; say* $5^k - 2^k = 3x$, *where* x *is an integer. Then,*

   $5^{k+1} - 2^{k+1} = 5 \cdot 5^k - 2 \cdot 2^k = 3 \cdot 5^k + 2 \cdot 5^k - 2 \cdot 2^k = 3 \cdot 5^k + 2(5^k - 2^k) = 3 \cdot 5^k + 2 \cdot 3x = 3(5^k + 2x)$, *which is divisible by* 3. *So,* $P(k+1)$ *is also true and the result follows by induction.* ■

6. *(Exercise) Prove that* $3^{2n} - 2^n$ *is divisible by* 7 *whenever* n *is a positive integer.*

7. *(Exercise) Suppose that the numbers* a_n *are defined recursively by* $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, *and* $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ *for all* $n \geq 4$. *Use the Strong Principle of Mathematical induction to prove that* $a_n < 3^n$ *for every positive integer* n.

8. *(Exercise) If the numbers* b_n *are defined recursively by* $a_1 = 11$, $a_2 = 21$, *and* $a_n = 3a_{n-1} - 2a_{n-2}$ *for all* $n \geq 3$, *prove that* $a_n = 5 \cdot 2^n + 1$ *for all* $n \geq 1$.

1.4 Divisibility Theory

1.4.1 Integer divisibility

Integer **divisibility** is the starting point of the theory of numbers.

Definition 1.9 (Integer Divisibility) *If a and b are integers, we say that a* **divides** *b (or a is a* **factor** *of b or a is a* **divisor** *of b or b is a* **multiple** *of a), if there exists an integer k such that $b = ka$. We denote this by $a|b$. If a does not divide b, then we write $a \nmid b$. E.g. $2|4$ and $5|35$, but $7 \nmid 34$.*

Some important remarks:

1. Any **even** integer has the form $2k$ for some integer k, while any **odd** integer has the form $2k+1$ for some integer k. Thus, $2|n$ if n is even and $2 \nmid n$ if n is odd.
2. For any $a \in \mathbb{Z}$, we always have that $a|0$.
3. If $b \in \mathbb{Z}$ is such that $|b| < a$, and $b \neq 0$, then $a \nmid b$.

Theorem 1.10 *If a, b, c are integers such that $a|b$ and $b|c$, then $a|c$.*

Proof: Since $a|b$ and $b|c$, then by definition there exist integers k_1 and k_2 such that $b = k_1 a$ and $c = k_2 b$. As a result, we get that $c = k_1 k_2 a$ and hence, $a|c$ since $k_1 k_2$ is also an integer. ■

Example 1.11 *Since $3|9$ and $9|45$, then $3|45$.*

Theorem 1.12 *If a, b, c, x, y are integers such that $c|a$ and $c|b$, then $c|(ax + by)$.*

Proof: Since $c|a$ and $c|b$, then by definition there exist integers k_1 and k_2 such that $a = k_1 c$ and $b = k_2 c$. Thus, $ax + by = (k_1 c)x + (k_2 c)y = k_1 cx + k_2 cy = (k_1 x + k_2 y)c$, and hence, $c|(ax + by)$ since $k_1 x + k_2 y$ is also an integer. ■

Some important remark:

1. If a, b, x, y are integers, then the integer $ax + by$ is called a **linear combination** of a and b.
2. Thus, Theorem 1.12 says that if c is a **common divisor** of a and b, then c divides any linear combination of a and b.

1.4.2 Some Olympiad questions involving the divisibility concept

- (**BMO 1, 2024**) The sequence of integers $a_0, a_1, \ldots$ has the property that for each $i \geq 2$, a_i is either $2a_{i-1} - a_{i-2}$ or $2a_{i-2} - a_{i-1}$. Given that a_{2023} and a_{2024} are consecutive integers, prove that a_0 and a_1 are consecutive integers. (Note that 6 & 7 are consecutive integers, as are 7 & 6).
- (**BMO 1, 2024**) Find all positive integers n such that $n \times 2^n + 1$ is a perfect square. (Note that an integer x is a **perfect square** if there is an integer y such that $x = y^2$).
- (**CMO 1, 2020**) Find all positive integers n, which can be subtracted from the numerator and the denominator of the factor $\frac{1234}{6789}$ to obtain (possibly after reduction) a proper fraction $\frac{a}{b}$, where a and b are integers.

Theorem 1.13 (Division Algorithm (DA)) *If a and b are integers such that $b > 0$, then there exist unique integers q and r such that $a = qb + r$, where $0 \leq r < b$.*

Remark: The integer q is called the **quotient**, while the integer r is called the **remainder**.

Example 1.14 *If $a = 76$ and $b = 6$, then $76 = 12 \cdot 6 + 4$. Here, $q = 12$ and $r = 4$.*

We give the proof of the Divison Algorithm. It consists of two parts: **existence** and **uniqueness**.

Proof: Existence: Consider the set $S = \{a - kb \geq 0 \mid k \in \mathbb{Z}\}$. Then S is a nonempty set of nonnegative integers since for $k < a/b$, we have $a - kb > 0$. By the Well-Ordering Principle, S has a least element, say $r = a - qb$ for some integer q. Note that $r \geq 0$ by construction. Now if $r \geq b$, then (since $b > 0$):

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

This contradicts the fact that $r = a - qb$ is a least element of S. As a result, we have that $0 \leq r < b$.

Uniqueness: We now show that q and r are unique. Suppose that $a = q_1 b + r_1$ and $a = q_2 b + r_2$ with $0 \leq r_1 < b$ and $0 \leq r_2 < b$. Then, we have $q_1 b + r_1 = q_2 b + r_2$ or $(q_1 - q_2)b + (r_1 - r_2) = 0$. As a result, we get that $(q_1 - q_2)b = r_2 - r_1$. Thus, we get that $b|(r_2 - r_1)$. And since, $-\max\{r_1, r_2\} \leq |r_2 - r_1| \leq \max\{r_1, r_2\}$ and $b > \max\{r_1, r_2\}$, then we must have that $r_2 - r_1 = 0$. That is, $r_1 = r_2$. Since $q_1 b + r_1 = q_2 b + r_2$, we also get that $q_1 = q_2$. This completes the proof. ■

1.4.3 A few applications of the Division Algorithm

1. If $b = 2$, according to the Division Algorithm, the possible remainders $r = 0$ and $r = 1$. When $r = 0$, the integer a has the form $2q$ and is called **even**; when $r = 1$, the integer a has the form $a = 2q + 1$ and is called **odd**. Now a^2 is either of the form $a^2 = (2q)^2 = 4k$ or $a^2 = (2q + 1)^2 = 4(q^2 + q) + 1 = 4k + 1$. The point made is that the square of an integer leaves remainder 0 or 1 upon division by 4.

2. The square of any odd integer is of the form $8k + 1$. By the Division Algorithm, any integer is representable as one of the forms: $4q$, $4q + 1$, $4q + 2$, or $4q + 3$. In this classification, only those integers of the forms $4q + 1$ and $4q + 3$ are odd. When $4q + 1$ is squared, we get:

   $$(4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8k + 1.$$

   On the other hand, when $4q + 3$ is squared, we also get:

   $$(4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1 = 8k + 1.$$

   E.g., the square of the odd integer 7 is $7^2 = 49 = 8 \cdot 6 + 1$, and the square of 13 is $13^3 = 169 = 8 \cdot 21 + 1$.

Example 1.15 *A few more applications of the Division Algorithm.*

1. *Show that the expression $a(a^2 + 2)/3$ is an integer for all positive integer $a \geq 1$.*

   Solution*: According to DA, every integer a is of one of the forms: $3q$, $3q + 1$, or $3q + 2$. Then:*

   - *For $a = 3q$; we have $\dfrac{a(a^2 + 2)}{3} = \dfrac{3q((3q)^2 + 2)}{3} = q(9q^2 + 2)$, which is clearly an integer.*
   - *For $a = 3q + 1$; we have $\dfrac{a(a^2 + 2)}{3} = \dfrac{(3q + 1)((3q + 1)^2 + 2)}{3} = (3q + 1)(3q^2 + 2q + 1)$, which is also clearly an integer.*

- *Finally, for* $a = 3q+2$*; we have* $\dfrac{a(a^2+2)}{3} = \dfrac{(3q+2)((3q+2)^2+2)}{3} = (3q+2)(3q^2+4q+2)$*, which is also an integer.*

Consequently, the result is established in all the three cases.

2. *(Exercise) For any integer* $n \geq 1$*, prove that* $n(n+1)(2n+1)/6$ *is an integer.*
3. *(Exercise) If* n *is an odd integer, show that* $n^4 + 4n^2 + 11$ *is an integer of the form* $16k$*.*

1.4.4 Representation of integers in different bases

An integer a written in base b expansion is denoted as $(a)_b$.

Theorem 1.16 *Let* b *be a positive integer with* $b > 1$*. Then any positive integer* m *can be written uniquely as*

$$m = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_1 b + a_0,$$

where ℓ *is a positive integer,* $0 \leq a_j < b$ *for* $j = 0, 1, \ldots, \ell$ *and* $a_\ell \neq 0$*.*

Proof: Exercise: An easy repeated application of the Division Algorithm. ■

Example 1.17 *Find the expansion of* 214 *in base* 3*.*

- *We apply the Division Algorithm as follows:*

$$\begin{aligned} 214 &= 3 \cdot 71 + 1 \\ 71 &= 3 \cdot 23 + 2 \\ 23 &= 3 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 3 \cdot 0 + 2. \end{aligned}$$

- *As a result, to obtain the expansion of* 214 *in base* 3*, we take the remainders of the divisions to get:* $(214)_{10} = (21221)_3$*.*

Example 1.18 *Find the base* 10 *expansion of* $(364)_7$*.*

- *We use place values to complete the computation:*

1.4.5 Greatest common divisor (gcd)

Definition 1.19 (gcd) *Let* a *and* b *be given integers, with at least one different from zero. The Greatest Common Divisor (gcd) of* a *and* b*, denoted* $\gcd(a, b)$ *or simply* (a, b)*, is the positive integer* d *satisfying the following:*

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

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

Example 1.20 *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* $\gcd(-12, 30) = 6$.

Theorem 1.21 (GCD) *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:

$$S = \{au + bv > 0 \mid u, v \in \mathbb{Z}\}.$$

Notice that S is nonempty. E.g. if $a \neq 0$, then the integer $|a| = au + b \cdot 0$ lies in S, where we choose $u = 1$ or $u = -1$ depending on whether a is positive or negative.

By the Well-Ordering Principle, S has a least element, say d. Thus, from the way S is defined, there exist integers x and y such that $d = ax + by$. We claim that $d = \gcd(a, b)$.

Applying 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

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

If $r > 0$, then this would imply that $r \in S$, contradicting the fact that d is the least integer in S, since $r < d$. Thus, $r = 0$, and so $a = qd$, or $d|a$. By a similar argument, $d|b$, the effect of which makes d a common divisor of a and b.

Now, if c is an arbitrary positive common divisor of a and b, then we also know that $c|(ax + by)$, that is, $c|d$. So, d is greater than every positive common divisor of a and b. Thus, $d = \gcd(a, b)$, which implies that $\gcd(a, b) = ax + by$. ■

Definition 1.22 *Twe integers* a *and* b *are* **relatively prime** *(or* **coprime***) if* $\gcd(a, b) = 1$.

Example 1.23 $\gcd(9, 16) = 1$*, thus* 9 *and* 16 *are relatively prime.*

Theorem 1.24 *Let* a *and* b *be integers, not both zero. Then* a *and* b *are relatively prime if and only f there exist integers* x *and* y *such that* $1 = ax + by$.

Proof: ($\Rightarrow$) If a and b are relatively prime, then $\gcd(a, b) = 1$, by Theorem (GCD) there exist integers x and y such that $1 = ax + by$.

($\Leftarrow$) Conversely, suppose that $1 = ax+by$ from some choice of integers x and y, and that $\gcd(a, b) = d$. Since $d|a$ and $d|b$, then certainly $d|(ax + by)$, which in turn implies that $d|1$. Since d is a positive integer, the condition $d|1$ implies that $d = 1$. Thus, a and b are relatively prime. ■

Corollary 1.25 *If* $\gcd(a, b) = d$*, then* $\gcd(a/d, b/d) = 1$.

Proof: First, we observe that although a/d and b/d have fractional appearance, in fact, they are integers because d is a divisor of both a and b. Now, knowing that $\gcd(a, b) = d$, it is possible to find integers x and y such that $d = ax + by$. Upon dividing through each side by d, we obtain $1 = \left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y$. Since a/d and b/d are both integers, we conclude that a/d and b/d are coprime. That is, $\gcd(a/d, b/d) = 1$. ■

Example 1.26 $\gcd(-12, 30) = 6$ *and* $\gcd(-12/6, 30/6) = \gcd(-2, 5) = 1$.

Corollary 1.27 *If $a|c$ and $b|c$, with $\gcd(a,b)=1$, then $ab|c$.*

Proof: Since $a|c$ and $b|c$, then there exist integers r and s such that $c=ar$ and $c=bs$.

Note that the relation $\gcd(a,b)=1$ implies that there exist integers x and y such that $1=ax+by$.

Now, multiplying through this equation by c gives: $c=c\cdot 1=c\cdot(ax+by)=acx+bcy$.

Then making appropriate substitution for c gives: $c=a(bs)x+b(ar)y=ab(sx+ry)$.

From this, it follows that $ab|c$.

■

Theorem 1.28 (Euclid's Lemma) *If $a|bc$, with $\gcd(a,b)=1$, then $a|c$.*

Proof: From $\gcd(a,b)=1$, there exist integers x and y such that

$$1=ax+by. \tag{1.5}$$

Multiplying through (1.5) by c gives:

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

Since $a|ac$ and $a|bc$, it follows that $a|(acx+bcy)$, which in turn implies that $a|c$. ■

Theorem 1.29 *Let a,b,c be integers. Then $\gcd(a,b)=\gcd(a+bc,b)$.*

Proof: This an interesting easy exercise! ■

Example 1.30 $\gcd(14,4)=\gcd(14-3\cdot 4,4)=\gcd(2,4)=2$.

1.4.6 Euclidean Algorithm (EA)

The **Euclidean Algorithm** provides a technique for both finding the gcd of two integers and expressing the gcd as a linear combination of the two integers.

Lemma 1.31 *Let a,b,q,r be integers. 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 $d|(a-qb)$, and hence this implies that $d|r$. 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 $c|(qb+r)$, and hence $c|a$. This makes c a common divisor of a and b, so $c|d$. It follows by definition that $\gcd(b,r)=d$. Thus, $\gcd(a,b)=\gcd(b,r)$. ■

Theorem 1.32 (Euclidean Algorithm) *Let $a=r_0$ and $b=r_1$ be two positive integers where $a\geq b$. If we apply the Division Algorithm successively to obtain that*

$$r_j=q_{j+1}r_{j+1}+r_{j+2},\quad 0\leq r_{j+2}<r_{j+1}$$

for all $j=0,1,\ldots,n-2$ and $r_{n+1}=0$. Then $\gcd(a,b)=r_n$.

Proof: By applying the Division Algorithm, we see that

$$\begin{aligned} r_0 &= q_1 r_1 + r_2, \quad 0 \le r_2 < r_1, \\ r_1 &= q_2 r_2 + r_3, \quad 0 \le r_2 < r_2 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, \quad 0 \le r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + 0. \end{aligned}$$

Notice that, we will have remainder 0 eventually since the remainders are integers and every remainder in the next step is less than the remainder in the previous one. By Lemma 1.31, we see that

$$\gcd(a, b) = \gcd(b, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_n, 0) = r_n.$$

■

Example 1.33 *Find the* gcd *of* 270 *and* 2412 *and express it as a linear combination of* 270 *and* 2412.

- *We apply the Euclidean Algorithm:*

$$2412 = 8 \cdot 270 + 252 \tag{1.6}$$
$$270 = 1 \cdot 252 + 18 \tag{1.7}$$
$$252 = 14 \cdot 18 + 0.$$

- *The last nonzero remainder is* 18. *Thus,* $\gcd(270, 2412) = 18$.
- *Next, we express* 18 *as a linear combination of* 270 *and* 2412. *From* (1.6), *we have*

$$252 = 2412 - 8 \cdot 270,$$

which on substitution in (1.7), *gives:*

$$270 = 1 \cdot (2412 - 8 \cdot 270) + 18.$$

- *This implies that*

$$18 = 9 \cdot 270 + (-1) \cdot 2412,$$

which is the desired linear combination.

Example 1.34 *Use the Euclidean Algorithm to find* $\gcd(12378, 3054)$.

Solution*: We apply the Euclidean Algorithm as follows.*

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

Since the last nonzero remainder in these divisions is 6, *it follows that* $\gcd(12378, 3054) = 6$.

Example 1.35 *Represent* 6 *as a linear combination of the integers* 12378 *and* 3054.

Solution*: We start with the second-last of the displayed equations in EA and successfully eliminate the remainders* $18, 24, 138$*, and* 162.

$$\begin{aligned} 6 &= 24 - 1 \cdot 18 \\ &= 24 - 1 \cdot (138 - 24 \cdot 5) \\ &= 6 \cdot 24 - 138 \\ &= 6 \cdot (162 - 1 \cdot 138) - 138 \\ &= 6 \cdot 162 - 7 \cdot 138 \\ &= 6 \cdot 162 - 7 \cdot (3054 - 18 \cdot 162) \\ &= 132 \cdot 162 - 7 \cdot 3054 \\ &= 132 \cdot (12378 - 4 \cdot 3054) - 7 \cdot 3054 \\ \therefore 6 &= 132 \cdot 12378 + (-535) \cdot 3054. \end{aligned}$$

Corollary 1.36 *If* $k > 0$*, then* $\gcd(ka, kb) = k \gcd(a, b)$.

Proof: If each of the equations in EA for a and b is multiplied by k, we get:

$$\begin{aligned} ka &= q_1(kb) + kr_1, \quad 0 < kr_1 < bk \\ kb &= q_2(kr_1) + kr_2, \quad 0 < kr_2 < kr_1 \\ &\vdots \\ kr_{n-2} &= q_n(kr_{n-1}) + kr_n, \quad 0 < kr_n < kr_{n-1} \\ kr_{n-1} &= q_{n+1}(kr_n) + 0. \end{aligned}$$

But this is clearly the EA applied to the integers ka and kb, so that their gcd is the last nonzero remainder kr_n, that is, $\gcd(ka, kb) = kr_n = k \gcd(a, b)$. ■

1.4.7 Least common multiple (lcm)

Definition 1.37 (lcm) *The* **least common multiple** *of two nonzero integers* a *and* b*, denoted* $lcm(a, b)$ *or simply* $[a, b]$*, 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* $m|c$.

Example 1.38 *The positive common multiples of the integers* -12 *and* 30 *are:* $60, 120, 180, \ldots$*, hence* $lcm(-12, 30) = 60$.

Theorem 1.39 *Let* a *and* b *be positive integers, then* $\gcd(a, b)lcm(a, b) = ab$.

Proof: To begin, let $d = \gcd(a, b)$. Since $d|a$ and $d|b$, there exist integers r and s such that $a = dr$ and $b = ds$. If $m = ab/d$, then $m = as = br$, the effect of which is to make m a positive common multiple of both a and b. Now let c be any positive integer that is a common multiple of both a and b; say $c = au = bv$. 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 shows that $m|c$. Thus, $m = \text{lcm}(a, b)$; that is, $\text{lcm}(a, b) = \dfrac{ab}{d} = \dfrac{ab}{\gcd(a, b)}$. Hence, $\gcd(a, b)\text{lcm}(a, b) = ab$. ■

Corollary 1.40 *For any choice of positive integers a and b, $lcm(a,b) = ab$ if and only if* $\gcd(a,b) = 1$.

Proof: Easy exercise. ■

Example 1.41 *Consider the following examples relating the* gcd *and the lcm.*

1. *Since* $\gcd(270, 2412) = 18$ *by Example 1.33, then*

$$lcm(270, 2412) = \frac{270 \cdot 2412}{\gcd(270, 2412)} = \frac{270 \cdot 2412}{18} = 36180.$$

2. *Since* $\gcd(12378, 3054) = 6$ *by Example 1.34, then*

$$lcm(12378, 3054) = \frac{12378 \cdot 3054}{\gcd(12378, 3054)} = \frac{12378 \cdot 3054}{6} = 6300402.$$

1.4.8 Linear Diophantine equations $ax + by = c$

The name honours the mathematician *Diophantus*, who initiated the study of such equations. He lived in *Alexandria* around 250 A.D.

The epigram-problem for Diophantus of Alexandria: His boyhood lasted $\frac{1}{6}$ of his life; his beard grew after $\frac{1}{12}$ more; after $\frac{1}{7}$ more he married; and his son was born 5 years later. The son lived to half of his father's age and the father dies 4 years after his son.

Solution: If x was the age at which Diophantus dies, the data leads to the equation

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x,$$

with solution $x = 84$. Thus, Diophantus must have reached an age of 84 years, but in what year or even what century is not known.

The great work of Diophantus of Alexandria is documented in his work *Arithmetica*, which may be described as the earliest book on Algebra. The simplest tupe of Diophantine equation that we shall consider is the *linear Diophantine equation* in two unknowns:

$$ax + by = c,$$

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, that is, x_0 and y_0 satisfy

$$ax_0 + by_0 = c.$$

Theorem 1.42 *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*

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

where t is an arbitrary integer.

Proof:

- The first condition is known as the condition for solvability.

- ($\Rightarrow$) We know that since $d|a$ and $d|b$, then there exist integers r and s, such that $a = dr$ and $b = ds$. If a solution of $ax + by = c$ exists, so that $ax_0 + by_0 = c$ for suitable x_0 and y_0, then $c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$. This implies that $d|c$.

- ($\Leftarrow$) Assume that $d|c$, say $c = dt$. Then by the GCD Theorem, there exist integers x_0 and y_0 such that $d = ax_0 + by_0$. Multiplying by t, we get that $c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0)$. Hence, has the equations $x = tx_0$ and $y = ty_0$ as a particular solution.

- To establish the second assertion, let us suppose that a solution x_0 and y_0 of the Diophantine equation $ax + by = c$ is known.

- If x' and y' is any other solution, then

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

which is equivalent to $a(x' - x_0) = b(y_0 - y')$. We know that $d = \gcd(a, b)$ implies that there exist relatively prime integers r and s such that $a = dr$ and $b = ds$.

- With this substitution, we get that $r(x' - x_0) = s(y_0 - y')$. This implies that $r|s(y_0 - y')$, with $\gcd(r, s) = 1$. By Euclid's Lemma, it must be the case that $r|(y_0 - y')$. That is, $y_0 - y' = rt$ for some integer t. Similarly, $x' - x_0 = st$.

- Thus, $x' = x_0 + st = x_0 + \left(\frac{b}{d}\right) t$ and $y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right) t$.

■

Example 1.43 *Solve the linear Diophantine equation* $172x + 20y = 1000$.

- *We apply the EA to evaluate* $\gcd(172, 20)$. *We find that*

$$\begin{aligned} 172 &= 20 \cdot 8 + 12 \\ 20 &= 12 \cdot 1 + 8 \\ 12 &= 8 \cdot 1 + 4 \\ 8 &= 4 \cdot 2 + 0, \end{aligned}$$

hence $\gcd(172, 20) = 4$. *Since* $4|1000$, *it follows that a solution to the linear Diophantine equation* $172x + 20y = 1000$ *exists.*

- *We express the integer* 4 *as a linear combination of* 172 *and* 20 *by working backward through a previous EA. One should verify that*

$$4 = 172 \cdot 2 + 20 \cdot (-17).$$

- *Multiplying through by* 250 *gives*

$$1000 = 4 \cdot 250 = 172 \cdot 500 + 20 \cdot (-4250),$$

so that $x = 500$ *and* $y = -4250$ *provide a particular solution to the linear Diophantine equation* $172x + 20y = 1000$.

- *All the other solutions are given by*

$$x = 500 + \left(\frac{20}{4}\right) t = 500 + 5t, \quad \textit{and} \quad y = -4250 - \left(\frac{172}{4}\right) t = -4250 - 43t,$$

for some integer t.

- *(Optional!) A little further effort produces the solutions in the positive integers, if any exists. For this, t must be chosen to satisfy simultaneously, the inequalities: $500+5t > 0$ and $-4250-43t > 0$; and this amounts to the same thing as $-98\frac{36}{43} > t > -100$. Since t must be an integer, we must have that $t = -99$. Thus, our Diophantine equation has a unique positive integer solution: $x = 5, y = 7$ corresponding to the value of $t = -99$.*

Corollary 1.44 *If $\gcd(a, b) = 1$ and if x_0, y_0 is a particular solution to the linear Diophantine equation $ax + by = c$, then all solutions are given by $x = x_0 + bt, \quad y = y_0 - at$, for some integer t.*

Example 1.45 *The linear Diophantine equation $5x + 22y = 18$ has $x_0 = 8$, $y_0 = -1$ as a particular solution; from Corollary 1.44, since $\gcd(5, 22) = 1$, a complete solution is given by $x = 8 + 22t$, $y = -1 - 5t$, for some integer t.*

Example 1.46 *The linear Diophantine equation $3x + 6y = 7$ has no solution because $\gcd(3, 6) = 3$ does not divide 7.*

Diophantine equations also frequently arise when solving traditional word problems.

Example 1.47 *A customer bought a dozen pieces of fruit, apples and ornages, 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 of fruit were bought?*

Solution*: To set up 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,*

$$3x + (x + y)z = 132. \tag{1.8}$$

Since $x + y = 12$, then (1.8) becomes: $3x + 12z = 132$, which in turn simplifies to:

$$x + 4z = 44. \tag{1.9}$$

Then, we solve the Diophantine equation (1.9) as follows: since $\gcd(1, 4) = 1$ is a divisor of 44, then there is an integer solution to (1.9). Upon multiplying the relation $1 = 1 \cdot (-3) + 4 \cdot 1$ by 44 to get: $44 = 1 \cdot (-132) + 4 \cdot 44$, it follows that $x_0 = -132$ and $z_0 = 44$ serves as one solution. All other solutions to (1.9) are of the form:

$$x = -132 + 4t \quad \text{and} \quad y = 44 - t,$$

where t is an integer. Only values of t that ensure that $6 < x \leq 12$ should be considered. This requires obtaining integer values of t such that: $6 < -132 + 4t \leq 12$, which implies that $34\frac{1}{2} < t \leq 36$. The only possible integer values of t are: $t = 35$ and $t = 36$. Thus, there are two possible purchases:

- *$x = -132 + 4 \cdot 35 = 8$ and $y = 12 - 8 = 4$, with $z = 44 - 35 = 9$. That is, 8 apples at 12 cents each and 4 oranges at 9 cents each (the case where $t = 35$).*
- *$x = -132 + 4 \cdot 36 = 12$ and $y = 0$, with $z = 44 - 36 = 8$. That is, 12 apples at 11 cents each and no oranges (the case where $t = 36$).*

Example 1.48 (First solved by Chinese Mathematician - Chang in the 6th Century) *If a cock is worth 5 coins, a hen worth 3 coins and three chicks together worth 1 coin, how many cocks, hens, and chicks, totaling 100, can be bought for 100 coins?*

Solution: *To set up a Diophantine equation for this problem, let x be the number of cocks, y be the number of hens, and z be the number of chicks. Then, the problem can be written as follows:*

$$5x + 3y + \frac{1}{3}z = 100 \quad \textit{and} \quad x + y + z = 100.$$

Eliminating one of the unknowns, we are left with a linear Diophantine equation in the other two unknowns: Specifically, because $z = 100 - x - y$, we have $5x + 3y + \frac{1}{3}(100 - x - y) = 100$, which simplifies to:

$$7x + 4y = 100. \tag{1.10}$$

The Diophantine equation (1.10) *has the general solution:*

$$x = -100 + 4t, \quad y = 200 - 7t, \quad \textit{so that} \quad z = 3t,$$

where t is an arbitrary integer. A little effort produces all solutions in the positive integers. For this, the integer t must be chosen to satisfy simultaneously, the inequalities:

$$-100 + 4t > 0, \quad 200 - 7t > 0, \quad \textit{and} \quad 3t > 0.$$

The last two of these inequalities are equivalent to the requirement: $25 < t < 28\frac{1}{50}$. Since t must have a positive integer value, we conclude that $t = 26, 27, 28$; leading to the solutions:

$$\begin{aligned} x = 4, \quad y = 14, \quad z = 78 \\ x = 8, \quad y = 11, \quad z = 81 \\ x = 12, \quad y = 4, \quad z = 84. \end{aligned}$$

1.5 Non-linear Diophantine equations

1.5.1 Some Olympiad problems

- **(CMO 4, 2020)** Out of three expressions $\frac{x}{y}$, $\frac{x^2+4}{y^2+4}$ and $\frac{x^3+8}{y^3+8}$ for some integers x, y, two take the same value and the remaining one takes a different value. Find all pairs of integers (x, y) for which this is possible.
- **(CMO 4, 2019)** Out of three expressions $\frac{x}{y}$, $\frac{x^2+x}{y^2+y}$ and $\frac{x^2+2}{y^2+2}$ for some integers x, y, all the three are defined, two take the same integer value and the remaining one takes a different integer value. Find all pairs of integers (x, y) for which this is possible.

1.6 Primes and their Distribution

Prime numbers are the building blocks of integers. They are also known as **primes**.

Definition 1.49 *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 as* **composite**.

Example 1.50 *The integers $2, 3, 5, 7, 11, 13$ are all prime numbers. The integers $4, 6, 8, 9, 10, 12, 14, 15$ are all composite numbers. Note that the integer 2 is the only even prime integer. The rest are odd primes.*

Theorem 1.51 *If p is a prime and $p|ab$, then either $p|a$ or $p|b$.*

Proof: If $p|a$, then we not go further. So, let us assume that $p \not| a$. Since the only positive divisors of p are 1 and p itself, it follows that $\gcd(p, a) = 1$. Hence, by Euclid's Lemma, we get that $p|b$. ■

Corollary 1.52 *If p is a prime and $p|a_1a_2 \cdots a_n$, then $p|a_k$ for some k, $1 \leq k \leq n$.*

Proof: Easy exercise. Proceed by induction on n. ■

Corollary 1.53 *If $p, q_1, q_2, \ldots, q_n$ are primes and $p|q_1q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.*

Proof: By Corollary 1.52, 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 and q_k itself. Because $p > 1$, we are forced to conclude that $p = q_k$. ■

Lemma 1.54 *Every integer greater than 1 has a prime divisor.*

Proof: Let $S = \{m \in \mathbb{Z} \mid m > 1 \quad \text{and} \quad n \quad \text{has no prime divisors}\}$. Suppose that S is nonempty. Then by the Well-Ordering Principle, S has a least element, say n. Since $n > 1$ and n has no prime divisors, then n is composite, and there exist integers a and b such that $n = ab$, where $1 < a < n$ and $1 < b < n$. However, since $a < a < n$ and n is the smallest element in S, then $a \notin S$, which implies that a has a prime divisor, say $p|a$, but then $p|n$ also, which is a contradiction. Thus, S is empty so that every positive integer $n > 1$ has a prime divisor. ■

1.6.1 Fundamental Theorem of Arithmetic (FTA)

Theorem 1.55 (Fundamental Theorem of Arithmetic (FTA)) *Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order of occurrence.*

Proof: Existence:

- If n is a prime integer, then n itself stands as a product of primes with a single factor.
- If n is composite, we use a proof by contradiction. Suppose now that there is some composite integer n that cannot be written as a product of primes.
- Let n be the smallest such integer. Let $n = ab$ with $1 < a < n$ and $1 < b < n$. As a result, a and b are products of primes since both integers are less than n.
- As a result, $n = ab$ is a product of primes. This contradicts the assumption that it is not.
- Thus, every integer can be written as a product of primes. This completes the existence proof.

  Uniqueness:
- Suppose that there is an integer n with two different factorizations: $n = p_1p_2 \cdots p_s = q_1q_2 \cdots q_r$, where $p_1, p_2, \ldots, p_s$ and $q_1, q_2, \ldots, q_r$ are primes with $p_1 \leq p_2 \leq \cdots \leq p_s$ and $q_1 \leq q_2 \leq \cdots \leq q_r$.
- Cancelling out all common primes from the factorizations above, we get that $p_{j_1}p_{j_2} \cdots p_{j_u} = q_{i_1}q_{i_2} \cdots q_{i_v}$.
- Thus, all primes on L.H.S are different from all primes on R.H.S.

- Since any prime p_{j_l} for some $1 \leq j \leq u$, must divide $p_{j_1}p_{j_2}\cdots p_{j_u}$, then p_{j_l} must divide $q_{i_1}q_{i_2}\cdots q_{i_v}$, and hence, p_{j_1} must divide q_{j_k} for some $1 \leq k \leq v$, which is impossible since the primes are different. Hence the representation is unique. This completes the uniqueness proof.

■

Corollary 1.56 *Any positive integer $n > 1$ can be written uniquely in the (canonical) form*

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

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

Proof: Easy exercise. ■

Example 1.57 $360 = 2\cdot 2\cdot 2\cdot 3\cdot 3\cdot 5 = 2^3\cdot 3^2\cdot 5$, $4725 = 3^3\cdot 5^2\cdot 7$, *and* $17640 = 2^3\cdot 3^2\cdot 5\cdot 7^2$.

1.6.2 Prime factorization with the gcd and the lcm

Prime factorization provides another means of calculating the $\gcd(a, b)$ and $\text{lcm}(a, b)$ for some integers a and b. First suppose that $p_1, p_2, \ldots, p_n$ are the distinct primes that divide either a or b. Allowing zero exponents, we can write:

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

Then,

$$\gcd(a,b) = p_1^{r_1}p_2^{r_2}\cdots p_n^{r_n} \text{ and } \text{lcm}(a,b) = p_1^{s_1}p_2^{s_2}\cdots p_n^{s_n}, \quad \text{where} \quad r_i = \min\{k_i, j_i\} \text{ and } s_i = \max\{k_i, j_i\}.$$

Example 1.58 *When $a = 4725$ and $b = 17640$, we would have that $a = 4725 = 2^0\cdot 3^3\cdot 5^2\cdot 7$ and $b = 17640 = 2^3\cdot 3^2\cdot 5\cdot 7^2$. Thus,* $\gcd(a, b) = \gcd(4725, 17640) = 2^0\cdot 3^2\cdot 5\cdot 7 = 315$ *and* $lcm(a, b) = lcm(4725, 17640) = 2^3\cdot 3^3\cdot 5^2\cdot 7^2 = 264600$.

Theorem 1.59 (Pythagoras) *The number $\sqrt{2}$ is irrational.*

Proof: Suppose by contradiction 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 by the Fundamental Theorem of Arithmetic there exists a prime p such that $p|b$. It follows that since $p|b$ and $b|a^2$, then $p|a^2$ and thus, $p|a$; hence, $\gcd(a, b) \geq p$. This is a contradiction to our original assumption that $\gcd(a, b) = 1$, unless $b = 1$. But if this happens, then $a^2 = 2$, which is obviously impossible. Our assumption that $\sqrt{2}$ is a rational number is wrong, so $\sqrt{2}$ must be irrational. ■

Alternative proof.

Proof: Suppose by contradiction that $\sqrt{2}$ is a rational number, say $\sqrt{2} = a/b$, where a and b are both integers with $\gcd(a, b) = 1$. Then by the GCD theorem, there exist integers r and s such that $1 = ar + bs$. Thus, multiplying through by $\sqrt{2}$, gives:

$$\sqrt{2} = \sqrt{2}(ar + bs) = (\sqrt{2}a)r + (\sqrt{2}b)s = 2br + as.$$

The above representation of $\sqrt{2}$ leads us to conclude that $\sqrt{2}$ is an integer, which is obviously a contradiction. Thus, our assumption that $\sqrt{2}$ is a rational number is wrong, so $\sqrt{2}$ must be irrational.
■

Theorem 1.60 *If an integer $n > 1$ is composite, then n has a prime factor not exceeding $\sqrt{n}$.*

Proof: If an integer $n > 1$ is composite, then it may be written as $n = ab$, where a and b are integers with $1 < a < n$ and $1 < b < n$. Suppose that $a \leq b$, then $a^2 \leq ab = n$ and as a result $a \leq \sqrt{n}$. By Lemma 1.54, a must have a prime divisor, say p. Then $p \leq a \leq \sqrt{n}$; furthermore, since $p|a$ and $a|n$, it follows that $p|n$. Thus, every integer $n > 1$ that is composite, will always have a prime divisor p satisfying $p \leq \sqrt{n}$. ■

Some important remarks:

- In testing the **primality** (that is, whether a given integer is a prime or not) of a specific integer $n > 1$, it suffices to divide n by those primes not exceeding $\sqrt{n}$.
- Theorem 1.60 also provides the practical means for determining the canonical form of an integer.

Example 1.61 *Use Theorem 1.60 to investigate whether the integer $n = 509$ is a prime or not.*

Solution*: Considering the integer $n = 509$. Since $22 < \sqrt{509} < 23$, we need only try out the primes that are not larger than 22 as possible divisors, namely, $2, 3, 5, 7, 11, 13, 17, 19$. Dividing 509 by each of these primes, we find out that none of them serves as a divisor of 509. Therefore, the conclusion is that 509 must be a prime number.*

Example 1.62 *Use Theorem 1.60 to determine the canonical form of the integer $n = 2093$.*

Solution*: For the integer $n = 2093$, since $45 < \sqrt{2093} < 46$, it is enough to examine the primes: $2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, 43$ as the possible divisors of 2093. By trial, the first of these primes to divide 2093 is 7, and $2093 = 7 \cdot 299$. As regards to the integer 299, we know that since $17 < \sqrt{299} < 18$, then we investigate the primes: $2, 3, 5, 7, 11, 13, 17$ as the possible divisors of 299. By trial, the first prime to divide 299 is 13, and $299 = 13 \cdot 23$. But 23 is itself a prime, hence $n = 2093$ has exactly three prime divisors $7, 13$, and 23. So, its canonical form is given as: $2093 = 7 \cdot 13 \cdot 23$.*

1.6.3 The Sieve of Eratosthenes

This is an ancient method of finding prime numbers up to a specified integer. This method was invented by ancient Greek mathematician *Eratosthenes*. There are several other methods used to determine whether a number is prime or composite

Definition 1.63 *The function $\pi(x)$, where x is a positive real number, denotes the number of primes less than or equal to x.*

The Algorithm for the Sieve of Eratosthenes for $\pi(n)$

1. List down all the numbers from 2 to the largest number n you want to test.
2. Strike off all multiples of 2 greater than 2 from the list.
3. Strike off all multiples of 3 greater than 3 from the list.
4. Repeat the above step un til no more multiples of prime integers are found that are less than $\sqrt{n}$.

Example 1.64 *Use the Sieve of Eratosthenes to compute $\pi(10)$ and $\pi(100)$.*

Solution: Chalkboard illustration.

1.6.4 Infinitude of Primes

We now show that there are infinitely many primes. There are several ways to prove this result. We shall provide two proofs:

- one due to **Euclid** (a contradiction by divisibility methods), and
- one due to **Euler** (a contradiction by analytic methods).

Theorem 1.65 (Euclid) *There exist an infinite number of primes.*

Proof: [Euclid's Proof]

- Let $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots$ be a list of primes in ascending order, and suppose that there is a last prime, called p_n.
- Now consider the positive integer $P = p_1 p_2 \cdots p_n + 1$.
- Since $P > 1$, we know that P has some prime divisor, say p. But $p_1, p_2, \ldots, p_n$ are the only primes, so that p must be one of $p_1, p_2, \ldots, p_n$.
- Combining the divisibility relation $p|p_1 p_2 \cdots p_n$ with $p|P$, we get that $p|P - p_1 p_2 \cdots p_n$ or, equivalently $p|1$. The only positive disor of integer 1 is 1 itself, since $p > 1$, we get a contradiction.
- Thus, no finite list of primes exists, hence the number of primes is infinite.

■

Proof:[Euler's Proof*]

- Suppose that $2 \leq p_1 < p_2 < \cdots < p_n$ are all the primes.
- Since each $p_i > 1$, then the sum $\displaystyle\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1 - \frac{1}{p_i}}$ converges.
- Hence $\displaystyle\prod_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}} = \prod_{i=1}^{n} \sum_{k=0}^{\infty} \frac{1}{p_i^k}$.
- The R.H.S is the sum of all positive integers, each counted at least once, since $p_1, p_2, \ldots, p_n$ are all the primes.
- Therefore, $\displaystyle\sum_{n=1}^{n} \frac{1}{n} \leq \prod_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}}$ must be finite. However, it is well–known that the series $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$ is divergent (Harmonic series). This leads to a contradiction.

■

1.6.5 Further results on primes

Let p_n denote the nth prime in their natural order. Euclid's proof shows that the expression $p_1 p_2 \cdots p_n +$ 1 is divisible by at least one prime. If there are several such prime divisors, then p_{n+1} cannot exceed the smallest of these so that $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$ for $n \geq 1$.

Theorem 1.66 *If p_n is the nth prime, $p_n \leq 2^{2^{n-1}}$.*

Proof:

- Let us proceed by induction on n. The asserted inequality is clearly true for $n = 1$. That is, $p_1 = 2 \leq 2^{2^{1-1}} = 2^{2^0} = 2^1 = 2$.
- As the hyposthesis of the induction, we assume that $n > 1$ and that the result holds for all integers up to n.
- Thus, we get that $p_{n+1} \leq p_1 p_2 \cdots p_n + 1 \leq 2 \cdot 2^2 \cdots 2^{2^{n-1}} = 2^{1+2+2^2+\cdots+2^{n-1}} + 1$.
- Recalling the identity, $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, we obtain that $p_{n+1} \leq 2^{2^n-1} + 1$.
- However, since $1 \leq 2^{2^n-1}$ for all n, we get that $p_{n+1} \leq 2^{2^n-1} + 2^{2^n-1} = 2 \cdot 2^{2^n-1} = 2^{2^n}$. Hence, $p_{n+1} \leq 2^{2^n}$.
- This completes the induction step, and hence the proof.

■

Corollary 1.67 *For $n \geq 1$, there are at least $n + 1$ primes less than 2^{2^n}.*

Proof: By the proof of the previous Theorem, we know that all primes $p_1, p_2, \ldots, p_n, p_{n+1}$ are less than 2^{2^n}. ■

Theorem 1.68 (Prime Number Theorem (PNT)) *Let $\pi(x)$ be the prime counting function. Then $\pi(x) \sim \dfrac{x}{\log x}$ as $x \to \infty$. Alternatively, $\lim\limits_{x\to\infty} \left(\dfrac{\pi(x)}{\frac{x}{\log x}} \right) = 1$.*

1.6.6 Conjectures on Primes

1. (**Twin Prime Conjecture**) There are infinitely many pairs of primes p and $p + 2$.
   E.g. $(3, 5), (5, 7), (11, 13), (17, 19), \ldots$.
2. (**Goldbach's Conjecture**) Every even positive integer greater than 2 can be written as the sum of two primes. E.g. $4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 3 + 7 = 5 + 5, \ldots$.
3. (**The $n^2 + 1$ Conjecture**- Hardy and Littlewood) There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer. E.g. $5 = 2^2 + 1, 17 = 4^2 + 1, 37 = 6^2 + 1, 101 = 10^2 + 1 \ldots$.
4. (**Polignac Conjecture**) For every even number $2n$ are there infinitely many pairs of consecutive primes which differ by $2n$.

Lemma 1.69 *The product of two integers of the form $4n + 1$ is also of the form $4n + 1$.*

Proof: Let $N_1 = 4n_1 + 1$ and $N_2 = 4n_2 + 1$ for some integers n_1 and n_2. Then,

$$N = N_1 N_2 = (4n_1 + 1)(4n_2 + 1) = 16n_1 n_2 + 4n_1 + 4n_2 + 1 = 4(4n_1 n_2 + n_1 + n_2) + 1 = 4n + 1,$$

where $n = 4n_1 n_2 + n_1 + n_2$. This completes the proof. ■

Theorem 1.70 *There is an infinite number of primes of the form $4n+3$, where n is a positive integer.*

Proof: Easy exercise! Use Euclid's Proof ideas together with the arguments from Lemma 1.69. ■

Theorem 1.71 (Dirichlet) *If a and b are relatively prime integers, then the arithmetic progression $a, a+b, a+2b, a+3b, \ldots$, contains infinitely many primes.*

Proof: Hard exercise! ■

Theorem 1.72 *If all the $n > 2$ terms of the arithmetic progression $p, p+d, p+2d, \ldots, p+(n-1)d$, then the common difference d is divisible by every prime $q < n$.*

Proof: Easy exercise! ■

1.6.7 Attempts to find a general formula for primes

For centuries, mathematicians have sought a simple formula that would yield every prime number or if this fails, a formula that would produce nothing else but primes. A request that seems modest enough, is to find a function $f(n)$ whose domain is, say, the nonnegative integers and whose range is some infinite subset of the set of all primes.

It was widely believed several years ago that the quadratic polynomial: $f(n) = n^2 + n + 41$ assumed only prime values. This claim was shown to be false by the Swiss Mathematician **Euler** in 1772. The claim is correct for the values $n = 0, 1, 2, 3, \ldots, 39$. However, it fails for $n = 40$ and $n = 41$, that is,

$$f(4) = 40^2 + 40 + 41 = 1681 = 41 \cdot 41 = 41^2 \quad \text{and} \quad f(41) = 41^2 + 41 + 41 = 1763 = 41 \cdot 43.$$

The next value $f(42) = 1847$ turns out to be prime. In fact, for the first 100 nonnegative integer values of n, the so-called Euler polynomial represents 86 primes. Although $f(n)$ starts off very well in the production of primes, there are other quadratic polynomials such as $g(n) = n^2 + n + 27941$ that begin to be better than $f(n)$ as the values of n become larger. For example, $g(n)$ is prime for 286129 values on n in $0 \leq n \leq 10^6$, while its famous rival $f(n)$ yields 261081 primes in this range.

It has been shown that no polynomial of the form $n^2 + n + q$, where q is a prime can do better than the Euler polynomial in giving primes for successive values of n. Indeed, until recently no other quadratic polynomial of any kind was known to produce more than 40 successive prime values. In 1988, it was found out that the polynomial $h(n) = 103n^2 - 3945n + 34381$, produces prime values for $n = 0, 1, 2, \ldots, 42$. The current record holder in this regard is the polynomial $k(n) = 36n^2 - 810n + 2753$ does slightly better by giving a string of 45 prime values. The failure to find prime-producing functions if not by accident, for it is easy to prove that there is no nonconstant polynomial $f(n)$ with integer coefficients that takes on just prime values for all integers $n \geq 0$. This is left as an easy exercise to prove!

1.6.8 Some Olympiad questions involving primes, composites and divisibility concepts

- (**IMO 2023, Japan**) Determine all composite integers $n > 1$ that satisfy the following property: $d_1, d_2, \ldots, d_k$ are all the positive divisors of n with $1 = d_1 < d_2 < \cdots < d_k = n$, then d_i divides $d_{i+1} + d_{i+2}$ for every $1 \leq i \leq k-2$.
- (**SAMO 2 2022**) Find all pairs of positive prime numbers (p, q) such that $p^5 + p^3 + 2 = q^2 - q$.

  Solution: We are given that $p^5 + p^3 = q^2 - q - 2$ which is equivalent to $p^3(p^2+1) = (q+1)(q-2)$. Thus, if p divides both $q+1$ and $q-2$, then $p = 3$, giving us a solution $(p, q) = (3, 17)$.

  Now, suppose that $p \neq 3$. Then either $q+1$ or $q-2$ is a multiple of p^3, whereas the other divides $p^2 + 1$. It follows that $q + 1 \geq p^3$ and $p^2 + 1 \geq q - 2$, so $p^3 \geq p^2 + 4$, which holds only for $p = 2$, giving a solution $(p, q) = (2, 7)$.
- (**PAMO 2023**) Find all pairs of positive integers (m, n) with no common divisors greater than 1 such that $m^3 + n^3$ divides $m^2 + 20mn + n^2$.

1.7 Theory of Congruences

The theory of congruences is an approach to divisibility questions through the arithmetic of remainders. This theory was introduced by the famous German mathematician - **Carl Friedrich Gauss**.

Definition 1.73 *Let n be a fixed integer. Two integers a and b are said to be* **congruent modulo** *n, denoted by $a \equiv b \pmod{n}$, if $n \mid (a-b)$; that is, provided $a - b = kn$ for some integer k.*

Example 1.74 *When $n = 7$, we see that $3 \equiv 24 \pmod{7}$, $-31 \equiv 11 \pmod{7}$, and $-15 \equiv -64 \pmod{7}$. This is because $3 - 24 = -21 = (-3) \cdot 7$, $-31 - 11 = -42 = (-6) \cdot 7$, and $-15 - (-64) = 49 = 7 \cdot 7$.*

When $n \not| (a-b)$, we say that a is **incongruent to b modulo n**, and in this case we write $a \not\equiv b \pmod{n}$. E.g. $25 \not\equiv 12 \pmod{7}$ because $7 \not| (25-12)$ or $7 \not| 13$.

Remark: Any two integers are congruent modulo 1, while two integers are congruent modulo 2 when then are both even or both odd. In usual practice, we shall assume that $n > 1$.

Given an integer a, let q and r be its quotient and remainder, respectively, upon division by n, so that $a = qn + r$, $0 \le r < n$. Then, by definition of the congruence, $a \equiv r \pmod{n}$.

Since there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values $0, 1, 2, \ldots, n-1$; in particular, $a \equiv 0 \pmod{n}$ if and only if $n|a$. The set of n integers $0, 1, 2, \ldots, n-1$ is called the **set of least nonnegative residues modulo** n.

In general, a collection of n integers $a_1, a_2, \ldots, a_n$ is said to form a **complete set of residues modulo** n if every integer is congruent modulo n to one and only one of the a_k. To put it in another way, $a_1, a_2, \ldots, a_n$ are congruent modulo n to $0, 1, 2, \ldots, n-1$, taken in some order.

Example 1.75 *The integers $-12, -4, 11, 13, 22, 82, 91$ constitute a complete set of residues modulo 7; here we have $-12 \equiv 2$, $-4 \equiv 3$, $11 \equiv 4$, $13 \equiv 6$, $22 \equiv 1$, $82 \equiv 5$, $91 \equiv 0 \pmod{7}$.*

Observation: Any n integers form a complete set of residues modulo n if and only if no two of the integers are congruent modulo n.

Theorem 1.76 *For any two integers a and b, we have $a \equiv b \pmod{n}$ if and only if both a and b leave the same nonegative remainder when divided by n.*

Proof: ($\Rightarrow$) Suppose that $a \equiv b \pmod{n}$, then $a = b + kn$ for some integer k. Upon division by n, b leaves a certain remainder r, that is, $b = qn + r$, where $0 \le r < n$. Therefore, $a = b + kn = (qn + r) + kn = (q + k)n + r$, which indicates that a leaves the same remainder as b upon division by n.

($\Leftarrow$) Suppose that both a and b leave the same remainder when divided by n, that is we can write $a = q_1 n + r$ and $b = q_2 n + r$, with $0 \le r < n$. Then $a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$. Hence $n|(a-b)$, that is, $a \equiv b \pmod{n}$. This completes the proof. ■

Example 1.77 *Consider the following few examples.*

- *Since the integers -56 and -11 can be expressed in the form: $-56 = (-7) \cdot 9 + 7$ and $-11 = (-2) \cdot 9 + 7$, with the same remainder 7, then by Theorem 1.76, we have $-56 \equiv -11 \pmod{9}$.*
- *The congruence $-31 \equiv 11 \pmod{7}$ implies that both -31 and 11 have the same remainder when divided by 7; this is clear from the relations: $-31 = (-5) \cdot 7 + 4$ and $11 = 1 \cdot 7 + 4$.*

Remark: Congruences may be viewed as a generalized form of equality, in the sense that its behavior with respect to addition and multiplication is reminiscent of ordinary equality.

Theorem 1.78 *Let $n > 1$ be a fixed integer and a, b, c, d be any given integers. Then the following properties hold.*

(i) (**Reflexivity**) $a \equiv a \pmod{n}$.

(ii) (**Symmetry**) *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$.

(iii) (**Transtivity**) *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.

(iv) If $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ab \equiv bd \pmod{n}$.

(v) If $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$.

(vi) If $a \equiv b \pmod{n}$, *than* $a^k \equiv b^k \pmod{n}$ *for some positive integer* k.

Proof:

(i) For any integer a, we have $a - a = 0 = 0 \cdot n$, so that $a \equiv a \pmod{n}$.

(ii) Suppose that $a \equiv b \pmod{n}$, then $a - b = kn$ for some integer k. Hence, $b - a = -kn = (-k)n$. Since $-k$ is also an integer, it immediately follows that $b \equiv a \pmod{n}$.

(iii) Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then there exist integers k_1 and k_2 such that $a - b = k_1 n$ and $b - c = k_2 n$. Thus, $a - c = (a - b) + (b - c) = k_1 n + k_2 n = (k_1 + k_2)n$, and since $k_1 + k_2$ is also an integer, it follows that $a \equiv c \pmod{n}$.

(iv) In the same spirit, suppose that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then there exist integers k_1 and k_2 such that $a - b = k_1 n$ and $c - d = k_2 n$. Adding these two equations gives: $(a + c) - (b + d) = (a - b) + (c - d) = k_1 n + k_2 n = (k_1 + k_2)n$. This implies that $a + c \equiv b + d \pmod{n}$. Furthermore, note that $ac = (b + k_1 n)(d + k_2 n) = bd + bk_2 n + dk_1 n + k_1 k_2 n^2 = bd + (bk_2 + dk_1 + k_1 k_2 n)n$ or $ac - bd = (bk_2 + dk_1 + k_1 k_2 n)n$. Since $bk_2 + dk_1 + k_1 k_2 n$ is also an integer, we get that $ac \equiv bd \pmod{n}$.

(v) Using $a \equiv b \pmod{n}$ and that fact that $c \equiv c \pmod{n}$, this property follows from (iv).

(vi) We prove this by induction on k. When $k = 1$, the statement certainly holds. Next we assume that it holds for a fixed integer $k > 1$. From (iv) we know that $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$ together imply that $aa^k \equiv bb^k \pmod{n}$ or, equivalently $a^{k+1} \equiv b^{k+1} \pmod{n}$. Thus, the statement is true for $k + 1$ whenever it is true for k, and the induction is complete.

This completes the proof. ∎

Example 1.79 *Let us show that* $41 \mid (2^{20} - 1)$.

Solution: *We begin by noting that* $2^5 \equiv 32 \equiv -9 \pmod{41}$. *Hence,* $(2^5)^4 \equiv (-9)^4$ *by Theorem 1.7 (vi). In otherwords,* $2^{20} \equiv 81 \cdot 81 \pmod{41}$. *But* $81 \equiv 40 \equiv -1 \pmod{41}$, *and so* $81 \cdot 81 \equiv (-1) \cdot (-1) \equiv 1 \pmod{41}$. *Using Theorem 1.7 (ii) and (v), we finally arrive at*

$$20^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}.$$

Thus, $41 \mid (2^{20} - 1)$ *as desired.*

Example 1.80 *Find the remainder obtained upon dividing the sum* $1! + 2! + 31 + \cdots + 99! + 100!$ *by* 12.

Solution*: Without the aid of congruences, this would be a very tough calculation! First, we observe that:* $4! \equiv 24 \equiv 0 \ (mod\ 12)$. *Thus, for* $k \geq 4$, *we have:*

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

In this way, we find that

$$1! + 2! + 3! + \cdots + 99! + 100! \equiv 1! + 2! + 3! + 0 + \cdots + 0 \equiv 9 \ (mod\ 9).$$

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

Remark: In Theorem 1.7, we say that if $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$ for any integer c. The converse, however, fails to hold. For example, note that $4 \cdot 2 \equiv 1 \cdot 2 (\text{mod } 6)$, whereas $4 \not\equiv 1 \pmod{6}$. In brief, one cannot unrestrictly cancel a common factor in the arithmetic of congruences. With suitable precautions, cancellation can be allowed; one step in this direction, and an important one, is provided by the following theorem.

Theorem 1.81 *If* $ac \equiv bc \ (mod\ n)$, *then* $a \equiv b \ (mod\ n/d)$, *where* $d = \gcd(c, n)$.

Proof: By hypothesis, we can write

$$(a - b)c = ac - bc = kn, \tag{1.11}$$

for some integer k. Knowing that $\gcd(c, n) = d$, there exist relatively prime integers r and s such that $c = dr$ and $n = ds$. Substituting these values in (1.11) and canceling out the common factor d yields: $(a - b)r = ks$. Hence, $s \mid (a - b)r$ and since $\gcd(r, s) = 1$, by Euclid's lemma, we have $s \mid (a - b)$. That is, $a \equiv b \pmod{s}$ or $a \equiv b \pmod{n/d}$, as required. ■

Corollary 1.82 *If* $ac \equiv bc \ (mod\ n)$ *and* $\gcd(c, n) = 1$, *then* $a \equiv b \ (mod\ n)$.

Corollary 1.83 *If* $ac \equiv bc \ (mod\ p)$ *and* $p \nmid c$, *where* p *is a prime, then* $a \equiv b \ (mod\ p)$.

Example 1.84 *Consider the following congruences:*

- $33 \equiv 15 \ (mod\ 9)$ *or if one preferes to write* $11 \cdot 3 \equiv 5 \cdot 3 \ (mod\ 9)$. *Since* $\gcd(3, 9) = 3$, *Theorem 1.81 leads to the conclusion that* $11 \equiv 5 \ (mod\ 3)$.
- $-33 \equiv 45 \ (mod\ 8)$ *or equivalently* $(-7) \cdot 5 \equiv 9 \cdot 5 \ (mod\ 8)$. *Since* $\gcd(5, 8) = 1$, *by Corollary 1.82, we can cancel out the common factor* 5, *to get* $-7 \equiv 9 \ (mod\ 8)$.

Remark: The product of two integers, neither of which is congruent to zero, may turn out to be congruent to zero. E.g. $4 \cdot 3 \equiv 0 \pmod{6}$ but $4 \not\equiv 0 \pmod{6}$ and $3 \not\equiv 0 \pmod{6}$. It is a simple matter to show that if $ab \equiv 0 \pmod{n}$ and $\gcd(a, n) = 1$, then $b \equiv 0 \pmod{n}$. In otherwords, if $ab \equiv 0 \pmod{p}$ with p a prime, then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

1.8 Binary and Decimal Representations; Divisibility Tests (9 and 11)

1.8.1 Binary and decimal representations

Example 1.85 *Consider the conversion from base* 10 *to binary and vice versa.*

- *The integer* 105 *can be written as:* $105 = 64+32+8+1 = 2^6+2^5+2^3+1 = 1\cdot 2^6+1\cdot 2^5+0\cdot 2^4+1\cdot 2^3+0\cdot 2^2+0\cdot 2+1 = (1101001)_2$, *or* $105 = (1101001)_2$.
- *In the other direction,* $(1001111)_2$ *translate into:* $(1001111)_2 = 1\cdot 2^6+0\cdot 2^5+0\cdot 2^4+1\cdot 2^3+1\cdot 2^2+1\cdot 2+1 = 64+8+4+2+1 = 79$.

The binary system is most convenient for use in modern electronic computing machines, because binary numbers are represented by strings of ones and zeros: 1 and 0 (or on and off).

We shall frequently calculate values of $a^k \pmod n$ when k is large. We use the **binary exponential algorithm** which relies on successive squaring.

Example 1.86 *Evaluate* 5^{110} *(mod* 131*).*

Solution*: First note that* $110 = 64+32+8+4+2 = 2^6+2^5+2^3+2^2+2 = 1\cdot 2^6+1\cdot 2^5+0\cdot 2^4+1\cdot 2^3+1\cdot 2^2+1\cdot 2+0\cdot 1 = (1101110)_2$.

Thus, we obtain the powers 5^{2^j} *(mod* 131*) for* $0 \le j \le 6$ *by repeatedly squaring while at each stage reducing each result modulo* 131*:* $5^2 \equiv 25$ *(mod* 131*),* $5^4 \equiv (5^2)^2 \equiv (25)^2 \equiv 625 \equiv 101$ *(mod* 131*),* $5^8 = (5^4)^2 \equiv (101)^2 \equiv 114$ *(mod* 131*),* $5^{16} \equiv (5^8)^2 \equiv (114)^2 \equiv 27$ *(mod* 131*),* $5^{32} \equiv (5^{16})^2 \equiv (27)^2 \equiv 74$ *(mod* 131*), and* $5^{64} \equiv (5^{32})^2 \equiv (74)^2 \equiv 105$ *(mod* 131*).*

From these, it follows that:

$$5^{110} \equiv 5^{64+32+8+4+2} \equiv 5^{64}\cdot 5^{32}\cdot 5^8\cdot 5^4\cdot 5^2 \equiv 105\cdot 74\cdot 114\cdot 101\cdot 25 \equiv 41\cdot 117\cdot 25 \equiv 60 \ (mod\ 131).$$

1.8.2 Polynomial congruences with integer coefficients

We are about ready to derive criteria for determining whether an integer is divisible by 9 or 11, without performing the actual division. For this, we need a result having to do with congruences involving polynomials with integer coefficients.

Theorem 1.87 *Let* $P(x) = \sum_{k=0}^{m} c_k x^k$ *be a polynomial function of* x *with integer coefficients* c_k*. If* $a \equiv b$ *(mod* n*), then* $P(a) \equiv P(b)$ *(mod* n*).*

Proof: Suppose that $a \equiv b \pmod n$, then by Theorem 1.78 (vi), we have $a^k \equiv b^k \pmod n$ for $k = 0, 1, 2, \ldots, m$. Therefore, $c_k a^k \equiv c_k b^k \pmod n$ for all such k. Summing up these $m+1$ congruences, we get that $\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod n$, or equivalently, $P(a) \equiv P(b) \pmod n$, as required. ■

Definition 1.88 *If* $P(x)$ *is a polynomial with integer 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 1.89 *If* a *is a solution of* $P(x) \equiv 0$ *(mod* n*) and* $a \equiv b$ *(mod* n*), then* b *is also a solution.*

Proof: By Theorem 1.87, it is known that if $a \equiv b \pmod n$, then $P(a) \equiv P(b) \pmod n$. Hence, if a is a solution of $P(x) \equiv 0 \pmod n$, then $P(b) \equiv P(a) \equiv 0 \pmod n$, making b a solution. ■

1.8.3 Divisibility test for 9

One divisibility test that we have in mind is this. A positive integer is divisible by 9 if and only if the sum of the digits in its decimal representation is divisible by 9.

Theorem 1.90 *Let $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$ be the decimal expansion of the positive integer N, with $0 \leq a_k < 10$, and let $S = a_0 + a_1 + \cdots + a_m$. Then $9|N$ if and only if $9|S$.*

Proof: Consider $P(x) = \sum_{k=0}^{m} c_k x^k$, a polynomial with integer coefficients. The key observation is that $10 \equiv 1 \pmod 9$, hence $P(10) \equiv P(1) \pmod 9$. But $P(10) = N$ and $P(1) = a_0 + a_1 + \cdots + a_m = S$. So, $N \equiv S \pmod 9$. It follows that $N \equiv 0 \pmod 9$ if and only if $S \equiv 0 \pmod 9$ or $9|N$ if and only if $9|S$. ■

1.8.4 Divisibility test for 11

Another divisibility test that we have in mind is this. A positive integer is divisible by 11 if and only if the alternating sum of the digits in its decimal representation is divisible by 11.

Theorem 1.91 *Let $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$ be the decimal expansion of the positive integer N, with $0 \leq a_k < 10$, and let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11|N$ if and only if $11|T$.*

Proof: Consider $P(x) = \sum_{k=0}^{m} c_k x^k$, a polynomial with integer coefficients. Observe that $10 \equiv -1 \pmod{11}$, hence $P(10) \equiv P(-1) \pmod{11}$. But $P(10) = N$ and $P(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m = T$. So, $N \equiv T \pmod{11}$. It follows that $N \equiv 0 \pmod{11}$ if and only if $T \equiv 0 \pmod{11}$ or $11|N$ if and only if $11|T$, as required. ■

Example 1.92 *Consider the integer $N = 1571724$. We show that N is divisible by both 9 and 11.*

- *Since the sum $1 + 5 + 7 + 1 + 7 + 2 + 4 = 27$ is divisible by 9, it follows that 1571724 is divisible by 9.*
- *Since the alternating sum $4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$ is divisible by 11, it also follows that 1571724 is divisible by 11.*

Remark: The theory of congruences is frequently used to append an extra check digit to identification numbers, in order to rcognise transmission errors or forgeries. Personal identification numbers of some kind appear on passports, credit cards, bank accounts, and a variety of other settings.

1.9 Linear Congruences and the Chinese Remainder Theorem

1.9.1 Linear congruences

Definition 1.93 *A* **linear congruence** *is an equation of the form $ax \equiv b \pmod n$ and a* **solution** *of such an equation means an integer x_0 for which $ax_0 \equiv b \pmod n$.*

By definition, $ax_0 \equiv b \pmod{n}$ if an only if $n \mid (ax_0 - b)$ or, if an only if $ax_0 - b = ny_0$ for some integer y_0. Thus, the problem of finding all integers that will satisfy the linear congruence $ax \equiv b \pmod{n}$ is identical to finding all solutions of the linear Diophantine equation $ax - ny = b$.

It is convenient to treat two solutions of $ax \equiv b \pmod{n}$ that are congruent modulo n as being **equal** even though they are not equal in the usual sense. E.g., $x = 3$ and $x = -9$ both satisfy the congruence $3x \equiv 9 \pmod{12}$; because $3 \equiv -9 \pmod{12}$, they are not counted as different solutions. In brief, when we refer to the number of solutions of $ax \equiv b \pmod{n}$, we mean the number of incongruent integers satisfying this congruence.

Theorem 1.94 *The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$, where $d = \gcd(a, n)$. If $d|b$, then the congruence has d mutually incongruent solutions modulo n.*

Proof: We already have observed that the given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. It is already 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

$$x = x_0 + \frac{n}{d}t \quad \text{and} \qquad y = y_0 - \frac{a}{d}t,$$

for some choice of an integer t. Among the various integers satisfying the first of these formulas, consider those that occur when t takes on the successive values $t = 0, 1, 2, \ldots, d-1$:

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

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

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}, \text{ where } 0 \le t_1 < t_2 \le d-1, \text{ then we would have } \frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}.$$

Now, $\gcd(n/d, d) = n/d$ and therefore the factor n/d could be canceled to get the congruence $t_1 \equiv t_2 \pmod{d}$, that is, $d \mid (t_2 - t_1)$. But this is impossible since $0 < t_2 - t_1 < d$.

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 $0 \le r < d - 1$. Hence,

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r) = x_0 + nq + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r \pmod{n},$$

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

Remark: Theorem 1.94 implicitly says that if x_0 is any solution of the linear congruence $ax \equiv b \pmod{n}$, then the $d = \gcd(a, n)$ incongruent solutions are given by

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

Corollary 1.95 *If a and n are relatively prime, that is, $\gcd(a, n) = 1$, then the congruence $ax \equiv b \pmod{n}$ has a unique solution modulo n.*

Remark: Given relatively prime integers a and n, the congruence $ax \equiv 1 \pmod{n}$ has a unique solution. This solution is called the **multiplicative inverse** of a modulo n.

Example 1.96 *Solve the linear congruence $18x \equiv 30 \pmod{42}$.*

Solution*: Since $\gcd(18, 42) = 6$ and $6|30$, then there are exactly six solutions, which are incongruent modulo 42. By inspection, one of the solutions is $x_0 = 4$. Our analysis tells us that the six solutions are as follows:*

$$x \equiv 4 + \left(\frac{42}{6}\right)t \equiv 4 + 7t \pmod{42}, \quad \text{where } t = 0, 1, 2, 3, 4, 5.$$

These solutions are plainly enumerated as $x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}$.

Example 1.97 *Solve the linear congruence* $9x \equiv 21 \pmod{30}$.

Solution*: Since* $\gcd(9, 30) = 3$ *and* $3|21$*, then we know that there are exactly three solutions, which are incongruent modulo* 30*. Using another approach, since the linear congruence* $9x \equiv 21 \pmod{30}$ *is equivalent to the linear Diophantine equation* $9x - 30y = 21$*, we begin by expressing the* $\gcd(9, 30) = 3$ *as a linear combination of* 9 *and* 30*. It is easily found out by inspection or by using the Euclidean Algorithm, that* $3 = (-3) \cdot 9 + 1 \cdot 30$*, so that* $21 = 7 \cdot 3 = (-21) \cdot 9 - (-7) \cdot 30$*. Thus,* $x_0 = -21$ *and* $y_0 = -7$ *satisfy the linear Diophantine equation, in consequence, all solutions of the linear congruence in question are found to be:* $x = -21 + (30/3)t = -21 + 10t$*. The integers* $x = -21 + 10t$*, where* $t = 0, 1, 2$*, are the three incongruent solutions modulo* 30*. These are*

$$x \equiv -21 \pmod{30}, \quad x \equiv -11 \pmod{30}, \quad \text{and} \quad x \equiv -1 \pmod{30},$$

or if one prefers positive numbers: $x \equiv 9, 19, 29 \pmod{30}$.

Chinese Remainder Theorem (CRT)

Having considered a single linear congruence, it is natural to turn to the problem of solving a system of simultaneous linear congruences:

$$a_1 x \equiv b_1 \pmod{m_1},\ a_2 x \equiv b_2 \pmod{m_2},\ \ldots,\ a_r x \equiv b_r \pmod{m_r}.$$

We shall assume that the moduli n_k are relatively prime in pairs. Evidently, the system will admit no solution unless each individual congruence is solvable; that is, unless $d_k | b_k$ for each k, where $d_k = \gcd(a_k, m_k)$. When these conditions are satisfied, the factor d_k can be canceled in the kth congruence to produce a new system having the same set of solutions as the original one:

$$a_1' x \equiv b_1' \pmod{n_1},\ a_2' x \equiv b_2' \pmod{n_2},\ \ldots,\ a_r' x \equiv b_r' \pmod{n_r},$$

where $n_k = m_k/d_k$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$; in addition, $\gcd(a_i', n_i) = 1$. The solutions of the individual congruences assume the form:

$$x \equiv c_1 \pmod{n_1},\ x \equiv c_2 \pmod{n_2},\ \ldots,\ x \equiv c_r \pmod{n_r}.$$

Thus, the problem is reduced to one of finding a simultaneous solution of a system of congruences of this simpler type. The kind of problem that can be solved by simultaneous congruences has a long history, appearing in the Chinese literature as early as the 1st century A.D. In honor of their early contributions, the rule for obtaining a solution usually goes by the name of the **Chinese Remainder Theorem**.

Theorem 1.98 (Chinese Remainder Theorem (CRT)) *Let* $n_1, n_2, \ldots, n_r$ *be positive integers such that* $\gcd(n_i, n_j) = 1$ *for* $i \neq j$*. Then the system of linear congruences*

$$x \equiv a_1 \pmod{n_1},\ x \equiv a_2 \pmod{n_2},\ \ldots,\ x \equiv a_r \pmod{n_r},$$

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

Proof: We start by forming the product $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \ldots, r$, let $N_k = n/n_k = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$. That is, N_k is the product of all integers n_i with the factor n_k omitted. By hypothesis, $\gcd(n_i, n_j) = 1$ for $i \neq j$, so we have $\gcd(N_k, n_k) = 1$.

According to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 \pmod{n_k}$; 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 of linear congruences.

First, we observe that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, since $n_k | N_i$ in this case. The result is,

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}.$$

But the integer x_k was chosen to satisfy the linear congruence $N_k x \equiv 1 \pmod{n_k}$, which forces: $\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}$. This shows that a solution to the given system of linear congruences exists.

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

$$\bar{x} \equiv a_k \equiv x^{'} \pmod{n_k}, \quad \text{for } k = 1, 2, \ldots, r,$$

and so $n_k \mid (\bar{x} - x^{'})$ for each value of k. Since $\gcd(n_i, n_j) = 1$ for $i \neq j$, then we get that $n_1 n_2 \cdots n_r \mid (\bar{x} - x^{'})$; hence $\bar{x} \equiv x^{'} \pmod{n}$. This completes the proof of CRT. ■

Example 1.99 *Solve the system of three linear congruences*

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

Solution*: First, we have* $n = 3 \cdot 5 \cdot 7 = 105$ *and* $N_1 = \frac{n}{3} = 35$, $N_2 = \frac{n}{5} = 21$, $N_3 = \frac{n}{7} = 15$. *Now, the linear congruences:*

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

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

$$\bar{x} = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233.$$

Reducing this modulo 105, *we get the unique solution* $\bar{x} \equiv 23 \ (mod\ 105)$.

Example 1.100 *Solve the linear congruence* $17x \equiv 9 \ (mod\ 276)$.

Solution*: Since* $276 = 3 \cdot 4 \cdot 23$, *his is equivalent to finding a solution for the system of congruences:*

$17x \equiv 9 \ (mod\ 3),\ 17x \equiv 9 \ (mod\ 4),\ 17x \equiv 9 \ (mod\ 23)$ *or*, $x \equiv 0 \ (mod\ 3),\ x \equiv 1 \ (mod\ 4),\ 17x \equiv 9 \ (mod\ 23)$.

Note that if $x \equiv 0 \ (mod\ 3)$, *thenx* $= 3k$ *for some integer* k. *We substitute into the second congruence of the system and obtain* $3k \equiv 1 \ (mod\ 4)$. *Multiplying both sides of this congruence by* 3 *gives:* $k \equiv 9k \equiv 3 \ (mod\ 4)$, *so that* $k = 3 + 4j$, *where* j *is an integer. Then,* $x = 3(3 + 4j) = 9 + 12j$. *For* x *to satisfy the third 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,* $j = 2 + 23t$, *for some integer* t. *Hence*

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

which implies that $x \equiv 33 \ (mod\ 276)$ *satisfies the system of the three linear congruences, and hence the linear congruence* $17x \equiv 9 \ (mod\ 276)$.

1.9.2 Systems of two linear congruences in two variables with the same modulus

The focus of our concern here is how to solve a system of two linear congruences in two variables with the same modulus. The proof of the coming theorem adopts the familiar procedure of eliminating one of the unknowns.

Theorem 1.101 *The system of linear congruences*

$$ax + by \equiv r \ (mod\ n)$$
$$cx + dy \equiv s \ (mod\ n),$$

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

$$(ad - bc)x \equiv dr - bs \pmod{n}. \tag{1.12}$$

The assumption that $\gcd(ad - bc, n) = 1$ ensures that the congruence $(ad - bc)z \equiv 1 \pmod{n}$ has a unique solution; denote this solution by t. When the congruence (1.12) is multiplied by t, we obtain:

$$x \equiv t(dr - bs) \pmod{n}.$$

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

$$(ad - bc)y \equiv as - cr \pmod{n}. \tag{1.13}$$

Multiplication of this congruence by t leads to

$$y \equiv t(as - cr) \pmod{n}.$$

A unique solution of the system is now established. This completes the proof. ■

Example 1.102 *Solve the system of linear congruences*

$$7x + 3y \equiv 10 \ (mod\ 16)$$
$$2x + 5y \equiv 9 \ (mod\ 16).$$

Solution*: Since* $\gcd(7 \cdot 5 - 2 \cdot 3, 16) = \gcd(29, 16) = 1$*, a unique solution to the system exists. We obtain the solution by elimination method established in the preceding theorem.*

Multiply 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* $13x \equiv 7 \ (mod\ 16)$*. Multiplying this last congruence by* 5*, since* $5 \cdot 13 \equiv 1 \ (mod\ 16)$*, produces* $x \equiv 35 \equiv 3 \ (mod\ 16)$*.*

When the variable x is eliminated from the system of congruences in a like manner, it is found that $29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43 \ (mod\ 16)$ *or,* $13y \equiv 11 \ (mod\ 16)$*. Multiplying this congruence by* 5*, since since* $5 \cdot 13 \equiv 1 \ (mod\ 16)$*, yields* $y \equiv 55 \equiv 7 \ (mod\ 16)$*.*

Therefore, the unique solution of our system turns out to be

$$x \equiv 3 \ (mod\ 16), \quad y \equiv 7 \ (mod\ 16).$$

1.10 Fermat's Little Theorem, Pseudoprimes, and Wilson's Theorem

1.10.1 Fermat's Little Theorem

Theorem 1.103 (Fermat's Little Theorem (FLT)) *Let p be a prime and suppose that $p \not| \ a$. Then, $a^{p-1} \equiv 1 \ (mod\ p)$ for any integer a.*

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

$$a,\ 2a,\ 3a, \ldots, (p-1)a. \tag{1.14}$$

None of these numbers is congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that $ra \equiv sa \pmod{p}$ for $1 \leq r < s \leq p-1$, then a could be canceled to give $r \equiv s \pmod{p}$, which is impossible. Therefore, the integers in (1.14) must be congruent modulo p to $1, 2, 3, \ldots, p-1$, taken in some order. Multiplying all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

Hence,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}. \tag{1.15}$$

Since $p \not| (p-1)!$, we can cancel out $(p-1)!$ on both sides of the congruence in (1.15) to get $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's Little Theorem. ■

FLT can be stated in a slightly more general way in which the requirement that $p \nmid a$ is dropped.

Corollary 1.104 *If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.*

Proof: When $p|a$, then the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, then according to FLT, we have $a^{p-1} \equiv 1 \pmod{p}$. When this congruence is multiplied through by a, the conclusion that $a^p \equiv a \pmod{p}$ follows. ■

Fermat's Little Theorem has many applications and is central to much of what is done in number theory. In the least, it can be a labour-saving device in certain calculations.

Example 1.105 *Verify that $5^{38} \equiv 4 \pmod{11}$.*

Solution*: From Fermat's Little Theorem, we know that $5^{10} = 5^{11-1} \equiv 1 \pmod{11}$. Thus, we have*

$$5^{38} = 5^{10 \cdot 3 + 8} = (5^{10})^3 \cdot (5^2)^4 \equiv 1^3 \cdot (25)^4 \equiv 3^4 \equiv 81 \equiv 4 \pmod{11}.$$

Thus, $5^{38} \equiv 4 \pmod{11}$ as required.

Another use of FLT is as a tool in testing the primality of a given integer n. If it could be shown that the congruence $a^n \equiv a \pmod{n}$ fails to hold for some choice of a, then n is necessarily composite

Example 1.106 *Verify that the integer 117 is composite (that is, not a prime). Hint! use $n = 117$ and $a = 2$ in Fermat's Little Theorem.*

Solution*: Since $2^7 = 128 \equiv 11 \pmod{117}$, we have*

$$2^{117} = 2^{7 \cdot 16 + 5} = (2^7)^{16} \cdot 2^5 \equiv (11)^{16} \cdot 2^5 \equiv ((11)^2)^8 \cdot 2^5 \equiv (121)^8 \cdot 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}.$$

But $2^{21} = 2^{7 \cdot 3} = (2^7)^3$, and this leads to

$$2^{117} \equiv 2^{21} \equiv (2^7)^3 \equiv (11)^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}.$$

Thus, $2^{117} \equiv 44 \not\equiv 2 \pmod{117}$, so that 117 must be composite. In fact, $117 = 9 \cdot 13$.

We investigate that the converse of FLT fails to hold. We first prove a technical lemma.

Lemma 1.107 *If p and q are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.*

Proof: By Corollary 1.104, we see that $a^{pq} = (a^q)^p \equiv a^q \pmod{p}$, whereas $a^q \equiv a \pmod{p}$ holds by hypothesis. Combining these congruences, we get that $a^{pq} \equiv a \pmod{p}$ or, in different terms, $p \mid (a^{pq} - a)$. In the same way, we find that $q \mid (a^{pq} - a)$. These divisibility conditions lead to $pq \mid (a^{pq} - a)$ or, in different terms $a^{pq} \equiv a \pmod{pq}$, as required. ■

Example 1.108 *We illustrate that the converse of FLT is false by showing that* $2^{340} \equiv \ (mod\ 341)$, *where* $341 = 11 \cdot 31$.

Solution*: Using the fact that* $2^{10} = 31 \cdot 33 + 1$, *we get that*

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2\ (mod\ 31) \quad and \quad 2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2\ (mod\ 11).$$

Now, applying Lemma 1.107, we get that

$$2^{11 \cdot 31} \equiv 2(mod\ 11 \cdot 31) \quad or \quad 2^{341} \equiv 2\ (mod\ 341). \tag{1.16}$$

Since $\gcd(2, 341) = 1$, *we cancel out the factor* 2 *in the last congruence in* (1.16) *to get* $2^{340} \equiv 1\ (mod\ 341)$, *so that the converse of FLT is false, as required.*

1.10.2 Pseudoprimes

The historical interest in the numbers of the form $2^n - 2$ resides in the claim made by Chinese mathematicians that "n **is a prime if and only if** $n \mid (2^n - 2)$". This criterion is only reliable for all integers $n \leq 340$. Example 1.108 shows that $341 \mid (2^{341} - 2)$, although $341 = 11 \cdot 31$, and this lays the claim to rest.

Definition 1.109 *A composite integer* n *is called a* **pseudoprime** *whenever* $n \mid (2^n - 2)$. *It can be shown there there are infinitely many pseudoprimes, the smallest four being* 341, 561, 645, *and* 1105.

The following theorem allows us to construct an increasing sequence of pseudoprimes.

Theorem 1.110 *If* n *is an odd pseudoprime, then* $M_n = 2^n - 1$ *is a larger one.*

Proof: Since n is composite, we can write $n = rs$, with $1 < r \leq s < n$. Then, from the fact that $(2^r - 1)|(2^n - 1)$ or, equivalently, $(2^r - 1)|M_n$, makes M_n composite. By our hypothesis, $n \mid (2^n - 2)$, that is, $2^n \equiv 2 \pmod{n}$. Hence, $2^n - 2 = kn$ for some integer k. It follows that $2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}$. This yields:

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

We immediately see that $M_n|(2^{M_n} - 2)$, which shows that M_n is a pseudoprime. ■

Remarks: More generally, a composite integer n for which $a^n \equiv a \pmod{n}$ is called a pseudoprime to the base a. (When $a = 2$, n is simply called a pseudoprime). For example, 91 is the smallest pseudoprime to base 3, whereas 217 is the smallest pseudoprime to base 5. It has been proved (1903) that there are infinitely many pseudoprimes to any given base. The first example of an even pseudoprime, namely, the number $161038 = 2 \cdot 73 \cdot 1103$ was found in 1950.

There exist composite numbers n that are pseudoprimes to every base a; that is, $a^{n-1} \equiv 1 \pmod{n}$ for all integers a with $\gcd(a, n) = 1$. The smallest such pseudoprime is the integer 561. These exceptional numbers are called **absolute pseudoprimes** or **Carmichael numbers** for R. D. Carmichael, who was the first to notice their existence.

In his first paper, Carmichael, indicated four absolute pseudoprimes including the well-known $561 = 3 \cdot 11 \cdot 17$. The others are $1105 = 5 \cdot 13 \cdot 17$, $2821 = 7 \cdot \cdot 31$, and $15841 = 7 \cdot 73$. Two years later he presented 11 more having three prime factors and discovered one absolute pseudoprime with four factors, specifically, $16046641 = 13 \cdot 37 \cdot 73 \cdot 457$.

Example 1.111 *We show that* $561 = 3 \cdot 11 \cdot 17$ *is indeed an absolute pseudoprime.*

Solution*: Note that* $\gcd(a, 561) = 1$ *gives* $\gcd(a, 3) = \gcd(a, 11) = \gcd(a, 17) = 1$*. An application of FLT leads to the congruences:*

$$a^2 = a^{3-1} \equiv 1 \ (mod\ 3), \quad a^{10} = a^{11-1} \equiv 1 \ (mod\ 11), \quad a^{16} = a^{17-1} \equiv 1 \ (mod\ 17),$$

and, in turn, leading to:

$$a^{560} = (a^2)^{280} \equiv 1^{280} \equiv 1 \ (mod\ 3), \quad a^{560} = (a^{10})^{56} \equiv 1^{56} \equiv 1 \ (mod\ 11), \quad a^{560} = (a^{16})^{35} \equiv 1^{35} \equiv 1 \ (mod\ 17).$$

These congruences lead to the single congruence $a^{560} \equiv 1 \ (mod\ 561)$*, where* $\gcd(a, 561) = 1$*. But then,* $a^{561} \equiv a \ (mod\ 561)$ *for all* a*, showing that* 561 *is an absolute pseudoprime.*

It can also be shown that any absolute pseudoprime is square-free. We prove the following theorem.

Theorem 1.112 *Any absolute pseudoprime is square-free.*

Proof: Suppose that $a^n \equiv a \pmod{n}$ for every integer a, but $k^2|n$ for some integer $k > 1$. If we let $a = k$, then $k^n \equiv k \pmod{n}$. Since $k^2|n$, this last congruence holds modulo k^2; that is, $k^n \equiv 0 \pmod{k^2}$, hence $k^2|k$, which is impossible. Thus, n must be square-free. ■

Next we present a theorem that furnishes a means for producing absolute pseudoprimes.

Theorem 1.113 *Let* n *be a composite square-free integer, say* $n = p_1 p_2 \cdots p_r$*, where* p_i *are distinct primes. If* $(p_i - 1)|(n - 1)$ *for* $i = 1, 2, \ldots, r$*, then* n *is an absolute pseudoprime.*

Proof: Suppose that a is an integer satisfying $\gcd(a, n) = 1$ so that $\gcd(a, p_i) = 1$ for $i = 1, 2, \ldots, r$. Then FLT yields $p_i \mid (a^{p_i - 1} - 1)$. From the divisibility hypothesis $(p_i - 1)|(n - 1)$, we have $p_i \mid (a^{n-1} - 1)$, and therefore $p_i \mid (a^n - a)$ for all a and $i = 1, 2, \ldots, r$. As a result, we end up with $n|(a^n - a)$, which makes n an absolute pseudoprime. ■

Remarks: Examples of integers that satisfy the conditions of Theorem 1.113 are $1729 = 7 \cdot 13 \cdot$, $6601 = 7 \cdot 23 \cdot 41$, and $10585 = 5 \cdot 29 \cdot 73$. It was proved in 1994 that infinitely many absolute pseudoprimes exist, but that they are fairly rare.

1.10.3 Wilson's Theorem

Mathematician John Wilson proved the property that if p is a prime, then p divides $(p - 1)! + 1$.

Theorem 1.114 (Wilson's Theorem) *If* p *is a prime, then* $(p - 1)! \equiv -1 \ (mod\ p)$*.*

Proof: Since the cases $p = 2$ and $p = 3$ are obviously satisfied, we omit them. So, let us take $p > 3$. Suppose that a is any one of the $p - 1$ positive integers: $1, 2, 3, \ldots, p - 1$, and consider the linear congruence $ax \equiv 1 \pmod{p}$. Since, $\gcd(a, p) = 1$, the congruence admits a unique solution modulo p; hence there is a unique integer a', with $1 \leq a' \leq p - 1$, satisfying $aa' \equiv 1 \pmod{p}$.

Since p is a prime, $a = a'$ if and only if $a = 1$ or $a = p - 1$. Indeed, the congruence $a^2 \equiv 1 \pmod{p}$ is equivalent to the congruence $(a - 1)(a + 1) \equiv 0 \pmod{p}$. Therefore, either $(a - 1) \equiv 0 \pmod{p}$, in this case $a = 1$, or $(a + 1) \equiv 0 \pmod{p}$, in this case $a = p - 1$.

If we omit the numbers 1 and $p - 1$, the effect is to group the remaining integers $2, 3, \ldots, p - 2$ into pairs a, a', where $a \neq a'$, such that $aa' \equiv 1 \pmod{p}$. When these $(p - 3)/2$ congruences are multiplied together and the factors re-arranged, we get that $2 \cdot 3 \cdots (p - 2) \equiv 1 \pmod{p}$, or rather

$$(p - 2)! \equiv 1 \pmod{p}. \tag{1.17}$$

Now, multiplying through the congruence (1.17) by $(p-1)$, we obtain the congruence:

$$(p-1)! \equiv (p-1)(p-2)! \equiv (p-1) \equiv -1 \pmod{p},$$

which is Wilson's Theorem, as required. ■

Example 1.115 *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* $2, 3, 4, 5, \ldots, 11$ *into* $(p-3)/2 = (13-3)/2 = 10/2 = 5$ *pairs, each product of which is congruent to* 1 *modulo* 13. *We write out these congruences explicitly:*

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

Multiplying these congruences together, gives the result

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

and so $12! \equiv 12 \equiv -1 \ (mod\ 13)$. *Thus,* $(p-1)! \equiv -1 \ (mod\ p)$, *with* $p = 13$.

Remark: The converse of Wilson's Theorem is also true. That is, if $(n-1)! \equiv -1 \pmod{n}$, then n must be a prime. **Proof:** Suppose by contradiction, that n is not a prime, then n has a divisor d with $1 < d < n$. Furthermore, since $d \leq n-1$, d occurs as one of the factors in $(n-1)!$, hence $d \mid (n-1)!$. Now, we are assuming that $n \mid ((n-1)!+1)$ and so $d \mid ((n-1)!+1)$ as well. The conclusion is that $d|1$, which is a contradiction. ■

An application of Wilson's theorem to the study of quadratic congruences. It is understood that **quadratic congruence** means a congruence of the form $ax^2+bx+c \equiv 0 \pmod{n}$, with $a \not\equiv 0 \pmod{n}$.

Theorem 1.116 *The quadratic congruence* $x^2 + 1 \equiv 0 \ (mod\ p)$, *where* p *is an odd prime if and only if* $p \equiv 1 \ (mod\ 4)$.

Proof: ($\Rightarrow$) Let a be any solution of the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$, so that $a^2 \equiv -1 \pmod{p}$. Since $p \nmid a$, the oucome of applying FLT is:

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

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

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

hence, $1 \equiv -1 \pmod{p}$. The net result of this is that $p|2$, which is false since p is an odd prime, that is, $p \geq 3$. Thus, p must be of the form $p = 4k+1$, or $p \equiv 1 \pmod{4}$.

($\Leftarrow$) In the product

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

we have the congruences

$$(p-1) \equiv -1 \pmod{p}, \quad (p-2) \equiv -2 \pmod{p}, \quad \ldots, \quad \frac{(p+1)}{2} \equiv -\frac{(p-1)}{2} \pmod{p}.$$

Re-arranging the factors gives:

$$(p-1)! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{(p-1)}{2} \cdot \left(-\frac{(p-1)}{2}\right) \equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \frac{(p-1)}{2}\right)^2 \pmod{p},$$

because there are $(p-1)/2$ minus signs involved. By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$, hence:

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

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

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

The conclusion is that the integer $\left[\frac{(p-1)}{2}!\right]$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$. ■

Example 1.117 *We take $p = 13$ which is a prime of the form $p = 4k+1$ for some integer $k = 3$. Here, we have $(p-1)/2 = (13-1)/2 = 12/2 = 6$, and it is easy to see that $6! = 720 \equiv 5 \pmod{13}$, and $5^1 + 1 = 26 \equiv 0 \pmod{13}$. Thus, the assertion that $\left[\frac{(p-1)}{2}!\right]^2 + 1 \equiv 0 \pmod{p}$ is correct for $p = 13$.*

Remark: Wilson's theorem implies that there exists an infinitude of composite numbers of the form $n! + 1$. On the other hand, it is an open question whether $n! + 1$ is prime for infinitely many values of n.

1.10.4 Fermat's factorization method

Fermat's factorization scheme involves the factorization of an odd integer n, and is equivalent to obtaining the integer solutions x and y of the equation $n = x^2 - y^2$. If n is the difference of two squares, then it is apparent that n is factored as:

$$n = x^2 - y^2 = (x+y)(x-y).$$

Conversely, when n has the factorization $n = ab$, with $a \geq b \geq 1$, then we may write

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

Moreover, because n is taken to be an odd integer, a and b are themselves odd; hence $(a+b)/2$ and $(a-b)/2$ will be nonnegative integers.

One begins the search for possible x and y satisfying the equation $n = x^2 - y^2$, or what is the same thing as the equation $x^2 - n = y^2$, by first determining the smallest integer k for which $k^2 \geq n$. Now look successively at the numbers

$$k^2 - n, \quad (k+1)^2 - n, \quad (k+2)^2 - n, \quad (k+3)^2 - n, \quad \ldots$$

until a value of $m \geq \sqrt{n}$ is found making $m^2 - n$ a square.

Example 1.118 *To illustrate the application of Fermat's method, let us factor the integer $n = 119143$.*

Solution*: Note that $345^2 < 119143 < 346^2$; thus, it suffices to consider the values of $k^2 - 119143$ for those k satisfying the inequality $346 \leq k < (119143+1)/2 = 59572$. The calculations are as follows:*

$$346^2 - 119143 = 119716 - 119143 = 573$$
$$347^2 - 119143 = 120409 - 119143 = 1266$$
$$348^2 - 119143 = 121104 - 119143 = 1961$$
$$349^2 - 119143 = 121801 - 119143 = 2658$$
$$350^2 - 119143 = 122500 - 119143 = 3357$$
$$351^2 - 119143 = 123201 - 119143 = 4058$$
$$352^2 - 119143 = 123904 - 119143 = 4761 = 69^2.$$

The last line gives the required factorization. That is,

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

and the two factors themselves being prime.

Example 1.119 *Fermat's method is most effective when the two factors of n are of nearly the same magnitude, for in this case a suitable square will appear quickly. E.g. let us suppose that $n = 23449$.*

Solution*: Note that $153^2 < 23449 < 154^2$, so the sequence $k^2 - n$ starts with:*

$$154^2 - 23449 = 23716 - 23449 = 267$$
$$155^2 - 23449 = 24025 - 23449 = 576 = 24^2.$$

Hence, the factors of 23449 are given by:

$$23449 = 155^2 - 24^2 = (155 + 24)(155 - 24) = 179 \cdot 131.$$

References

1. D. M. Burton (2007), *Elementary Number Theory*, McGraw-Hill, 6th Edition.
2. B. Fine and G. Rosenberger (2016), *Number Theory*, Birkhäuser, 2nd Edition.