Number theory lectures

By Dr. Mohammed M. AL-Ashker
Associated professor
Mathematics Department
E.mail:mashker @ mail.iugaza.edu
Islamic University of Gaza P.O.Box 108, Gaza, Palestine
Contents

1 Divisibility Theory of integers
   1.1 The Division Algorithm ........................................... 3
   1.2 The greatest common divisor ..................................... 4
   1.3 The Euclidean algorithm ......................................... 8
   1.4 The Diophantine equation $ax + by = c$ ........................ 11

2 Primes and their distributions ....................................... 14
   2.1 Fundamental theorem of arithmetics ............................ 14
   2.2 The sieve of Eratosthenes ....................................... 16
   2.3 The Goldbach conjecture ......................................... 17

3 The theory of congruences ............................................. 19
   3.1 Basic properties of congruence ................................ 19
   3.2 Special divisibility tests ....................................... 23
   3.3 Linear congruences ............................................... 25

4 Fermat’s theorem ..................................................... 31
   4.1 Fermat’s little theorem ......................................... 31
   4.2 Wilson’s theorem ................................................. 32
Chapter 1

Divisibility Theory of integers

1.1 The Division Algorithm

Theorem 1.1.1. Given integers $a$ and $b$, with $b > 0$, there exist unique integers $q$ and $r$ satisfying, $a = qb + r$, $0 \leq r < b$. The integers $q$ and $r$ are called, respectively, the quotient and remainder in the division of $a$ and $b$.

Proof. We first show $r$ and $q$ exist. Let $S = \{a - xb : a - xb \geq 0, \ x \in \mathbb{Z}\}$. We will show that $S \neq \emptyset$. Since $b > 0$ and $b \in \mathbb{Z} \implies b \geq 1 \implies |a|b \geq |a|$. Let $x = -|a| \implies a - xb \geq a + |a|b \geq a + |a| \geq 0 \implies S \neq \emptyset$ (since $S$ not empty), so $S$ contains a least non-negative integer call it $r$. Then $r$ will be in the form $r = a - qb$, then $r$ exists and also $q$ exists corresponding to $r$.

We will also show that $r < b$.

Suppose $r \geq b$ and $r = r' + b$ where $r' \geq 0$ and $r' + b = a - qb \implies r' = a - (q + 1)b \geq 0 \implies r' \in S$.

Contradiction, (because $r' < r$ and $r$ the smallest non-negative element in $S$) $\implies 0 \leq r < b$.

We will now prove the uniqueness of $r$ and $q$. Assume $\exists r_1, q_1$ satisfying the conditions of the theorem such that $r < r_1$ and $a = q_1b + r_1$ then $r_1 = a - q_1b$...(1) but $a = qb + r$ then $r = a - qb$...(2), from (1) and (2) by subtraction, we have $(r_1 - r) = (q - q_1)b \implies b|r_1 - r$.

Contradiction, because $r_1 < b$ and $r < b \implies r_1 - r = 0 \implies r_1 = r$ and $q_1 = q$. \hfill \Box

Example 1.1.1. If $a = 592$, $b = 7$ then $592 = 84(7) + 4$ then $q = 84$ and $r = 4$. 

3
Corollary 1.1.2. If $a$ and $b$ are integers, with $b \geq 0$, then there exist unique integers $q$ and $r$ such that,

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

Proof. If $b < 0$, then $|b| > 0$ and by the above theorem $\exists q'$ and $r \exists a = q'|b| + r, \quad 0 \leq r < |b|$.
Since $|b| = -b$, we may take $q = -q'$ to arrive $a = (−q)(−b) + r = qb + r$ with $0 \leq r < |b|$. \qed

Example 1.1.2. Let $b = -7, \quad a = 1$ then $1 = 0(−7) + 1, \quad \text{where } 0 \leq r = 1 < |b| = 7.$
Let $b = -7, \quad a = -2$ then $-2 = 1(−7) + 5, \quad \text{where } 0 \leq r = 5 < |b| = 7.$
Let $b = -7, \quad a = 61$ then $61 = (-8)(−7) + 5, \quad \text{where } 0 \leq r = 5 < |b| = 7.$
Let $b = -7, \quad a = -59$ then $-59 = 9(−7) + 4, \quad \text{where } 0 \leq r = 4 < |b| = 7.$

If $a$ is even integer then $a = 2q$ and $a^2 = 4q^2 = 4k$ where $k = q^2$. If $a$ is odd then $a = 2q+1$ and $a^2 = 4q^2+4q+1 = 4(q^2+q)+1 = 4k'+1$ where $k' = q^2+q$.

Example 1.1.3. The square of any odd integer is of the form $8k + 1$

Proof. By division algorithm, any integer is represented as one of the four following forms: $4q, \ 4q + 1, \ 4q + 2, \ 4q + 3$. In this classification, only those integers of the forms $4q + 1$ and $4q + 3$ are odd. Then $(4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8k + 1$, where $k = 2q^2 + q$, and $(4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1 = 8k' + 1$, where $k' = 2q^2 + 3q + 1$.

Let $a = 7$ then $a^2 = 49 = 8 \cdot 6 + 1$. \qed

1.2 The greatest common divisor

Definition 1.2.1. An integer $b$ is said to be divisible by an integer $a \neq 0$, in symbols $a | b$, if there exists some integer $c$ such that $b = ac$. We write $a \nmid b$ to indicate that such $b$ is not divisible by $a$.

Example 1.2.1. $3 | -12$ because $-12 = 4(-3)$ but $3 \nmid 10$ \exists $c \in Z \ni 10 = 3c$. If $a | b \implies -a | b$ because if $b = ac \implies b = -a(-c) \implies -a | b$.

Theorem 1.2.1. For integers $a, b$ and $c$ the following hold :
1) \( a \mid 0,\ 1 \mid a,\ a \mid a. \)

2) \( a \mid 1 \text{ if and only if } a = \pm 1. \)

3) If \( a \mid b \text{ and } c \mid d, \text{ then } ac \mid bd. \)

4) If \( a \mid b \text{ and } b \mid c, \text{ then } a \mid c. \)

5) \( a \mid b \text{ and } b \mid a \text{ if and only if } a = \pm b. \)

6) If \( a \mid b \text{ and } b \neq 0 \text{ then } |a| \leq |b|. \)

7) If \( a \mid b \text{ and } a \mid c \text{ then } a \mid bx + cy \text{ for arbitrary integers } x \text{ and } y. \)

**Proof.**

1) For \( a \mid 0, \text{ exists } x = 0 \Rightarrow x = \pm 1 \text{ or } a = \pm 1. \)

2) If \( a \mid 1, \text{ then } \exists x \in Z \Rightarrow 1 = ax \Rightarrow x = \pm 1 \text{ or } a = \pm 1. \)

3) If \( a \mid b \text{ and } c \mid d \), then \( \exists x, y \in Z \Rightarrow b = xa,\ d = cy \Rightarrow bd = xyca \Rightarrow ca \mid bd. \)

4) If \( a \mid b \text{ and } b \mid c \), then \( \exists x, y \in Z \Rightarrow b = xa,\ c = by \Rightarrow c = axy \Rightarrow a \mid c. \)

5) If \( a \mid b \text{ and } b \mid a \), then \( \exists x, y \in Z \Rightarrow b = xa,\ a = by \Rightarrow b = byx \Rightarrow 1 = yx \Rightarrow y = \pm 1,\ x = \pm 1 \Rightarrow b = \pm a. \)

6) If \( a \mid b \), then there exists \( c \in Z \) such that \( b = ac, \text{ also } b \neq 0 \text{ then } c \neq 0, \text{ and } |b| = |ac| = |a||c|, \text{ since } c \neq 0 \text{ then } |c| \geq 1 \text{ and } |b| \geq |a||c| \geq |a|. \)

7) If \( a \mid b \text{ and } a \mid c \), then there exists \( t \in Z, r \in Z, \exists b = at \text{ and } c = ar \Rightarrow bx = atx,\ cy = ary \Rightarrow bx + cy = a(tx + ry) \Rightarrow a \mid bx + cy. \)

In general if \( a \mid b_k \) for \( k = 1, 2, \ldots, n \) then \( a \mid bx_1 + b_2x_2 + \cdots + b_nx_n. \)

\[ \square \]

**Definition 1.2.2.** The integer \( d \) is a common divisor of \( a \) and \( b \) in case \( d \mid a, \) and \( d \mid b. \)

since \( 1 \mid a \) for any integer \( a \) then 1 is a common divisor of \( a \) and \( b, \) so the set of common divisors of any integers \( a \) and \( b \) is non-empty.

**Remark 1.2.1.** If \( a = b = 0, \) then every integer is a common divisor of \( a \) and \( b, \) so in this case the set of common divisors of \( a \) and \( b \) is infinite.

If at least one of \( a \) or \( b \) is not zero then there are only a finite number of positive common divisors.
Let \( d \) be the positive divisors of \( a \) and \( b \). If \( \text{gcd}(a, b) \) denotes by \(\text{gcd}(a, b)\), the greatest common divisor which is called the greatest common divisor which is denoted by \( \text{gcd}(a, b) \).

**Definition 1.2.3.** Let \( a \) and \( b \) be given integers with at least one of them different from zero. The \( \text{gcd}(a, b) \) is the positive integer \( d \) satisfying:

1. \( d \mid a \) and \( d \mid b \).
2. If \( c \mid a \) and \( c \mid b \), then \( c \leq d \).

**Example 1.2.2.** The positive divisors of \(-12\) are 1, 2, 3, 4, 6, 12 while those of 30 are 1, 2, 3, 5, 6, 10, 15, 30. the \( \text{gcd}(30, -12) = 6 \).

\( \text{gcd}(-5, 5) = 5, \text{gcd}(8, 17) = 1 \) and \( \text{gcd}(-8, -36) = 4 \).

If \( a = b = 0 \) there is no greatest common divisor.

If we have \( a_1, a_2, \ldots, a_n \) such that at least one of \( a_i \neq 0 \) for \( i = 1, 2, \ldots, n \) then \( \text{gcd} \) of \( a_i \neq 0 \) for \( i = 1, 2, \ldots, n \) is denoted by \( \text{gcd}(a_1, a_2, \ldots, a_n) \).

**Theorem 1.2.2.** Given integers \( a \) and \( b \) not both of which are zero, there exist integers \( x \) and \( y \) such that \( \text{gcd}(a, b) = ax + by \).

**Proof.** Let \( g = \text{gcd}(a, b) \), let \( S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0 \} \). Since \(-a+b, a-b, -a-b, a+b\) are integers, so at least one of them must be in \( S \implies S \neq \emptyset \). Let \( l = \) the smallest positive integer in \( S \) chose \( x_0, y_0 \). So that \( l = ax_0 + by_0 \) we will show that \( l \mid a \), and \( l \mid b \). Assume that \( l \nmid a \implies \exists q \text{ and } r \in \mathbb{Z} \exists a = lq + r, 0 < r < l \implies r = a - lq = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) \implies r \in S \), Contradiction, because \( r < l \) and \( l \) is the smallest integer in \( S \implies r = 0 \) and \( l \mid a \ldots(1) \).

By the same way we can prove that \( l \mid b \ldots(2) \) then from (1) and (2) \( l \) is a common divisor of \( a \) and \( b \).

Since \( g = \text{gcd}(a, b) \implies g \mid a \), \( g \mid b \implies g \mid ax_0 + by_0 = l \implies g \mid l, g \leq l \), but \( l \) is a common divisor of \( a \) and \( b \) cannot be greater than the \( \text{gcd} \) \( g \implies g = l \). \( \square \)

**Corollary 1.2.3.** If \( a \) and \( b \) are given integers, not both zeros, then the set \( T = \{ax + by : x, y \text{ are integers} \} \) is precisely the set of all multiples of \( g = \text{gcd}(a, b) \).

**Proof.** Since \( g \mid a \), and \( g \mid b \implies g \mid ax + by \) for all integers \( x, y \in \mathbb{Z} \). Then every member of \( T \) is a multiple of \( g \). If \( g = ax_0 + by_0 \) for suitable integers \( x_0 \) and \( y_0 \). So that any multiple \( ng \) of \( g \) is of the form \( ng = n(ax_0 + by_0) = a(nx_0) + b(ny_0) \).
If an integer \(g\) is expressible in the form \(g = ax + by\) then it is not necessary that \(g\) is the g.c.d of \((a, b)\). But it follows from such an equation g.c.d \((a, b)|g\).

If \(ax + by = 1\) for some integers \(x\) and \(y\) then g.c.d\((a, b) = 1\).

**Definition 1.2.4.** Two integers \(a\) and \(b\), not both of which are zeros, are said to be relatively prime whenever g.c.d\((a, b) = 1\).

**Example 1.2.3.** \(g.c.d(2, 5) = g.c.d(-9, 16) = g.c.d(-27, -35) = 1\)

**Theorem 1.2.4.** Let \(a\) and \(b\) integers not both zeros, then \(a\) and \(b\) are relatively prime if and only if there exist integers \(x\) and \(y\) such that \(1 = ax + by\).

**Proof.** If g.c.d\((a, b) = 1, then \(\exists x, y \in \mathbb{Z} \ni 1 = ax + by\). Conversely if \(1 = ax + by\) for some \(x, y \in \mathbb{Z},\) and \(g = g.c.d(a, b) \implies g|a, g|b \implies g|ax + by \implies g|1 \implies g = 1 \implies a \text{ and } b \text{ are relatively prime.} \)

**Corollary 1.2.5.** If g.c.d\((a, b) = d, then g.c.d\((\frac{a}{d}, \frac{b}{d}) = 1.

**Proof.** \(d|a, d|b \implies \frac{a}{d}, \frac{b}{d} \text{ are integers since } d = g.c.d(a, b) \implies \exists x, y \in \mathbb{Z} \ni d = ax + by \implies 1 = \frac{a}{d}x + \frac{b}{d}y, \text{ by previous theorem } (\frac{a}{d}, \frac{b}{d}) = 1 \).

**Example 1.2.4.** \(g.c.d(-12, 30) = 6 \implies g.c.d(-\frac{12}{6}, \frac{30}{6}) = g.c.d(-2, 5) = 1\)

**Remark 1.2.3.** It is not true that if \(a|c\) and \(b|c \implies ab|c.\) For example 6|24, and 8|24 \implies 48 \nmid 24.

**Corollary 1.2.6.** If \(a|c\) and \(b|c\) with g.c.d\((a, b) = 1 \implies ab|c.

**Proof.** If \(a|c, b|c, \exists r\) and \(s \in \mathbb{Z} \ni c = ar = bs, \text{ since } g.c.d(a, b) = 1 \text{ then there exist } x, y \in \mathbb{Z} \ni 1 = ax + by \implies c = cax + cby = acx + bcy \implies c = a(bs)x + b(ar)y = ab(ax + ry) \implies ab|c.\)

**Theorem 1.2.7.** If \(ab|c\) with g.c.d\((a, b) = 1, \text{ then } a|c.

**Proof.** Since \(g.c.d(a, b) = 1 \implies \exists x, y \in \mathbb{Z} \ni 1 + ax + by \implies c = acx + bcy\) since \(a|ac\) and \(a|bc \implies a|acx + bcx \implies a|c(ax + by) \implies a|c \cdot 1 \implies a|c.\)

**Remark 1.2.4.** If g.c.d\((a, b) \neq 1 \text{ then } a \nmid c.\)
Example 1.2.5. \(12|9 \cdot 8 \implies 12 \nmid 9, \ 12 \nmid 8\).

**Theorem 1.2.8.** Let \(a, b\) be integers, no both zero. For a positive integer \(d\), \(d = \gcd(a, b)\) if and only if

1. \(d|a\) and \(d|b\),
2. whenever \(c|a\) and \(c|b\), then \(c|d\).

**Proof.** Let \(d = \gcd(a, b) \implies d|a\) and \(d|b\), so (1) holds. Also \(\exists x, y \in \mathbb{Z} \mid d = ax + by\). If \(c|a\), \(c|b\) then \(c|ax + by \implies c|d \implies \) condition (2) holds.

Conversely, let \(d\) be any positive integer satisfying the stated conditions and let \(c\) be any common divisor of \(a\) and \(b\) then \(c|d\) by condition (2). This implies that \(d \geq c\), so \(d\) is the greatest common divisor of \(a\) and \(b\). \(\square\)

### 1.3 The Euclidean algorithm

**Lemma 1.3.1.** If \(a = qb + r\), then \(\gcd(a, b) = \gcd(b, r)\).

**Proof.** If \(d = \gcd(a, b) \implies d|a, d|b \implies d|a−qb = r, \implies d|r \implies d|\gcd(b, r)\), let \(c = \gcd(b, r) \implies d|c\ldots (1)\).

\(c|b, c|r \implies c|bq+r \implies c|a \implies c|\gcd(b, a) = d \implies c|d\ldots (2)\). From (1), (2) \implies \ c = d. \(\square\)

**Theorem 1.3.2. The Euclidean algorithm.**

Let \(a\) and \(b\) be two integers whose greatest common divisor is desired. Assume that \(a \geq b > 0\). Apply the division algorithm to \(a\) and \(b\) to get,

\[ a = q_1b + r_1, \ 0 \leq r_1 < b. \]

If \(r_1 = 0 \implies b|a\) and \(\gcd(a, b) = b\).

If \(r_1 \neq 0\) divide \(b\) by \(r_1\) to produce integers \(q_2\) and \(r_2\) satisfying

\[ b = q_2r_1 + r_2, \ 0 \leq r_2 < r_1. \]

If \(r_2 = 0\), then we stop; otherwise, proceed as before to obtain

\[ r_1 = q_3r_2 + r_3, \ 0 \leq r_3 < r_2. \]

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

The result is the following system of equations.

\[
\begin{align*}
 a &= q_1 b + r_1, \quad 0 < r_1 < b \\
 b &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \\
 r_1 &= q_3 r_2 + r_3, \quad 0 < r_3 < r_2 \\
 &\vdots \\
 r_{n-2} &= q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\
 r_{n-1} &= q_{n+1} r_n + 0.
\end{align*}
\]

We argue that \( r_n \), the last nonzero remainder which appears in this manner is equal to \( \text{g.c.d}(a, b) \).

**Proof.** By lemma

\[
\text{g.c.d}(a, b) = \text{g.c.d}(b, r_1) = \cdots = \text{g.c.d}(r_{n-1}, r_n) = \text{g.c.d}(r_n, 0) = r_n.
\]

The \( \text{g.c.d}(a, b) \) can be expressed in the form \( ax + by \). For this, we fall back on Euclidean algorithm. Starting with the next-to-last equation arising from the algorithm, we write

\[
r_n = r_{n-2} - q_n r_{n-1}.
\]

Now solve the proceeding equation in the algorithm for \( r_{n-1} \) and substitute to obtain,

\[
r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) = (1 + q_n q_{n-1})r_{n-2} + (-q_n)r_{n-3}.
\]

This represents \( r_n \) as a linear combination of \( r_{n-2} \) and \( r_{n-3} \). Continuing backwards through the system of equations, we successively eliminate the remainders \( r_{n-1}, r_{n-2}, \cdots, r_2, r_1 \) until a stage is reached where \( r_n = \text{g.c.d}(a, b) \) is expressed as a linear combination of \( a \) and \( b \).

**Example 1.3.1.** Use Euclidean algorithm to find the greatest common divisor of 7469 and 2464.

**solution:**

\[
\begin{align*}
7469 &= 3(2464) + 77 \\
2464 &= 32(77) + 0
\end{align*}
\]

\[\therefore \text{g.c.d}(7469, 2464) = 77.\]

Also \( 77 = 7469 - 3(2464) \), so \( x = 1, \ y = -3. \)
Theorem 1.3.3. If \( k > 0 \), then \( \gcd(ka, kb) = k \gcd(a, b) \).

Proof. Let \( g = \gcd(a, b) \) then \( g = \) the least positive value of \( ax + by \). So for \( k > 0 \), \( \gcd(ka, kb) = \) least positive value of \( (kax + kby) = k \) (least positive value of \( ax + by \)) = \( k \gcd(a, b) = kg \).

\[ \square \]

Corollary 1.3.4. For any integer \( k \neq 0 \), \( \gcd(ka, kb) = \lvert k \rvert \gcd(a, b) \).

Proof. If \( k < 0 \implies \lvert k \rvert = -k \implies \gcd(ak, bk) = \gcd(-ak, -bk) = \gcd(a|k|, b|k|) = \lvert k \rvert \gcd(a, b) \).

\[ \square \]

Example 1.3.2. \( \gcd(12, 30) = 3 \gcd(4, 10) = (3) \cdot 2 \gcd(2, 5) = 6 \).

Definition 1.3.1. An integer \( c \) is said to be a common multiple of two nonzero integers \( a \) and \( b \) whenever \( a|c \) and \( b|c \). Evidently \( 0 \) is a common multiple of \( a \) and \( b \).

Example 1.3.3. For \( a = -12, b = 30 \), all of the integers \( 0, 60, 120, 180, \cdots \) are common multiple of \(-12 \) and \( 30 \). The least positive common multiple \( \text{l.c.m}(-12, 30) = 60 \).

Definition 1.3.2. The Least common multiple of two nonzero integers \( a \) and \( b \), denoted by \( \text{l.c.m}(a, b) \), is the positive integer \( m \) satisfying:

1. \( a|m \) and \( b|m \).
2. if \( a|c \) and \( b|c \), with \( c > 0 \), then \( m \leq c \).

Remark 1.3.1. If \( a, b \neq 0 \) then \( \text{l.c.m}(a, b) \) exists and \( \text{l.c.m}(a, b) \leq \lvert ab \rvert \).

Theorem 1.3.5. For positive integers \( a \) and \( b \), \( \gcd(a, b) \text{l.c.m}(a, b) = ab \).

Proof. Let \( d = \gcd(a, b) \implies d|a, d|b \implies \exists r, s \in \mathbb{Z} \ni a = dr, b = ds \). If \( m = \frac{ab}{d} \), then \( m = as = br \) because \( m = \frac{dcds}{d} = as = br \implies a|m, b|m \implies m \) is a common multiple of \( a \) and \( b \).

Now let \( c \) be any positive integer that is a common multiple of \( a \) and \( b \) then \( a|c \) and \( b|c \implies c = au = bv \) for some \( u, v \in \mathbb{Z} \implies u = \frac{c}{a}, v = \frac{c}{b} \).

Since \( d = \gcd(a, b) \implies \exists x, y \in \mathbb{Z} \ni d = ax + by \), then \( \frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \frac{cax + cby}{ab} = \frac{vx + uy}{x} \in \mathbb{Z} \implies m|c \implies m \leq c \implies m = \text{l.c.m}(a, b) \) and \( m = \frac{ab}{d} = \frac{ab}{\gcd(a, b)} \implies ab = md = \text{l.c.m}(a, b)\gcd(a, b) \).

\[ \square \]

Corollary 1.3.6. Given positive integers \( a \) and \( b \), \( \text{l.c.m}(a, b) = ab \) if and only if \( \gcd(a, b) = 1 \).
Proof. \( \text{l.c.m}(a, b) \cdot \text{g.c.d}(a, b) = ab \) if \( \text{g.c.d}(a, b) = 1 \) then \( \text{l.c.m}(a, b) \cdot 1 = ab \).

Conversely, let \( \text{l.c.m}(a, b) \cdot \text{g.c.d}(a, b) = ab \) and \( \text{l.c.m}(a, b) = ab \) then \( ab \cdot \text{g.c.d}(a, b) = ab \implies \text{g.c.d}(a, b) = 1. \)

\[ \square \]

Example 1.3.4. Find \( \text{l.c.m}(7469, 2464) \).

 SOLUTION: \( \text{g.c.d}(7469, 2464) \) by Euclidean algorithm is equal 77

So \( \text{l.c.m}(7469, 2464) = \frac{(7469)(2464)}{\text{g.c.d}(7469, 2464)} = 239008 \)

Definition 1.3.3. If \( a, b, c \in \mathbb{Z} \) not all zero then the \( \text{g.c.d}(a, b, c) \) is defined to be the positive integer \( d \) having the properties:

1. \( d \) is a divisor of each \( a, b, c \)
2. If \( e \) divides the integers \( a, b, c \) then \( e \leq d \).

Example 1.3.5. \( \text{g.c.d}(39, 42, 54) = 3 \).

Definition 1.3.4. Three integers are said to be relatively prime as a triple if \( \text{g.c.d}(a, b, c) = 1 \), yet not relatively primes in pairs.

1.4 The Diophantine equation \( ax + by = c \)

Theorem 1.4.1. The linear diophantine equation \( ax + by = c \) has a solution if and only if \( d|c \), where \( d = \text{g.c.d}(a, b) \). If \( x_0, y_0 \) is any particular solution of this equation, then all other solutions are given by

\[ x = x_0 + \frac{b}{d} t, \quad y = y_0 - \frac{a}{d} t \quad \text{for varying integer } t. \]

Proof. Let \( d = \text{g.c.d}(a, b) \implies d|a, \quad d|b \implies \exists r, s \in \mathbb{Z} \ni a = dr, \quad b = ds \).

If \( ax + by = c \) has a solution then there exists \( x_0, y_0 \) such that \( ax_0 + by_0 = c \implies drx_0 + dsy_0 = c \implies d(rx_0 + sy_0) = c \implies d|c. \)

Conversely if \( d|c \implies \exists t \in \mathbb{Z} \ni c = dt \), but \( d = \text{g.c.d}(a, b) \implies \exists x_0, y_0 \in \mathbb{Z} \ni ax_0 + by_0 = d \implies atx_0 + bty_0 = td \implies a(tx_0) + b(ty_0) = c. \) If \( x = tx_0, \quad y = ty_0 \), then the diophantine equation \( ax + by = c \) has a solution \( x = tx_0, \quad y = ty_0. \)

To proof the second assertion of the theorem, let \( x_0, y_0 \) be a solution of the diophantine equation \( ax + by = c \implies ax_0 + by_0 = c \).

Let \( x', y' \) be any other solution, then \( ax' + by' = c \implies ax_0 + by_0 = ax' + by' = c \implies a(x' - x_0) = b(y_0 - y'). \)
But $d|a,$ and $d|b \iff \exists r, s \in Z, \exists a = rd, b = ds \implies d = g.c.d(a, b) = g.c.d(dr, ds) = dg.c.d(r, s) \implies g.c.d(r, s) = 1 \implies rd(x' - x_0) = sd(y_0 - y') \implies r|s(y_0 - y')$ but $g.c.d(r, s) = 1 \implies r|(y_0 - y') \implies \exists t \in Z, \exists y_0 - y' = tr.$

By substituting we have,

$$r(x' - x_0) = str \implies x' - x_0 = st \implies x' = x_0 + st = x_0 + \left(\frac{b}{d}\right)t$$

and

$$y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right)t.$$

It is only to show that these values satisfy the diophantine equation $ax + by = c.$

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

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

**Example 1.4.1.** Determine all solutions in integers of the following Diophantine equation

$$56x + 72y = 40.$$

**Solution:** we apply Euclidian algorithm to find $g.c.d(56, 72).$

$$72 = 56 \cdot 1 + 16$$

$$56 = 16 \cdot 3 + 8$$

$$16 = 8 \cdot 2 + 0.$$

Then $g.c.d(56, 72) = 8,$ since $8|40,$ then the Diophantine equation has solution.

$$8 = 56 - 16 \cdot 3$$

$$= 56 - (72 - 56)3$$

$$= 56(1 + 3) - 3(72)$$

$$= 4(56) - 3(72).$$

Then $40 = 20(56) - 15(72).$ Then $x_0 = 20,$ $y_0 = -15$ are the particular solutions and all solutions are $x = 20 + 9t,$ $y = -15 - 7t,$ where $t \in Z.$

**Corollary 1.4.2.** If $g.c.d(a, b) = 1$ and if $x_0, y_0$ is a particular solution of the linear diophantine equation $ax + by = c,$ then all solutions are given by

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

for integral values of $t.$
Example 1.4.2. Find all solutions of the diophantine equation,

\[ 30x + 17y = 300. \]

Solution

\[ 30 = 17 \cdot 1 + 13 \]
\[ 17 = 13 \cdot 1 + 4 \]
\[ 13 = 4 \cdot 3 + 1 \]
\[ 4 = 4 \cdot 1 + 0. \]

Then the \( g.c.d(30, 17) = 1 \). Then

\[ 1 = 13 - 4(3) = 13 - (17 - 13)(3) = 13(4) - 3(17) = (30 - 17)4 - 3(17) \]

\[ 1 = 4(30) - 7(17). \]

Then \( 300 = 1200(30) - 2100(17) \).

Then the particular solutions are \( x_0 = 1200, \ y_0 = -2100 \) and all solutions are \( x = 1200 + 17t, \ y = -2100 - 30t. \)
Chapter 2

Primes and their distributions

2.1 Fundamental theorem of arithmetics

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

Example 2.1.1. \( 2, 3, 5, 7 \) are primes but \( 4, 6, 8, 9, 10 \) are composite. \( 2 \) is the only even prime, and all other primes are odd.

Theorem 2.1.1. If \( p \) is a prime and \( p|ab \), then \( p|a \) or \( p|b \).

Proof. Assume that \( p \nmid a \implies \gcd(a, p) = 1 \implies \text{if } p|ab \implies p|b \). if \( g.c.d(a, p) = p \implies p|a \). \( \Box \)

Corollary 2.1.2. If \( p \) is a prime and \( p|a_1a_2\cdots a_n \), then \( p|a_k \) for some \( k \), where \( 1 \leq k \leq n \).

Proof. Assume that \( p \nmid a_k \) for \( 1 \leq k \leq n \implies g.c.d(p, a_k) = 1 \) for \( 1 \leq k \leq n \implies g.c.d(p, a_1a_2\cdots a_n) = 1 \implies p \nmid a_1a_2\cdots a_n \) contradiction. So there exists some \( k \), \( 1 \leq k \leq n \) such that \( p|a_k \). \( \Box \)

Corollary 2.1.3. If \( p, q_1, q_2, \ldots, q_n \) are all primes and \( p|q_1q_2\cdots q_n \) then \( p = q_k \) for some \( k \), where \( 1 \leq k \leq n \).

Proof. By previous corollary (2.1.2) \( \exists k, 1 \leq k \leq n \; \exists p|q_k \), being a prime, \( q_k \) is not divisible by any positive integer other than 1 or \( q \) itself, since \( p > 1 \) then \( p = q_k \). \( \Box \)
Theorem 2.1.4. (Fundamental theorem of arithmetic) Every positive integer \( n > 1 \) can expressed as a product of primes, this representation is unique, a part from the order in which the factors occur.

Proof. If \( n \) is prime then done.
If \( n \) is composite then there exists a prime \( p_1 \) such that,
\[ n = p_1 n_1, \quad 1 < n_1 < n. \]
If \( n_1 \) is prime done, if not there exists \( p_2 \) and \( n_2 \) such that
\[ n_1 = p_2 n_2, \quad 1 < n_2 < n_1 < n \implies n = p_1 p_2 n_2. \]
After \( k - 1 \) times we have,
\[ n = p_1 p_2 \cdots p_{k-1} n_{k-1} \text{ and } 1 < n_k < \cdots < n_2 < n_1 < n, \]
the sequence cannot be infinite, so after \( n_{k-1} \) steps, \( n_{k-1} \) must be prime say \( n_{k-1} = p_k \implies n = p_1 p_2 \cdots p_k. \)
To establish the uniqueness, suppose that \( n \) has two representations as a product of primes, say
\[ n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_s, \]
where \( k \leq s \) and \( p_i, q_j \) are primes and \( p_1 \leq p_2 \leq \cdots p_k, \)
\[ q_1 \leq q_2 \cdots \leq q_s. \]
Since \( p_1 | q_1 q_2 \cdots q_s \), there exists \( i, 1 \leq i \leq s \) such that \( p_1 = q_i \geq q_1, \)
similarly \( q_1 \geq p_1 \) then \( q_1 = p_1. \)
If \( s = k \) after repeated the same process \( k \) times we have unique representation of \( n. \) If \( k < s \) then after \( k \) times we have \( p_1 p_2 \cdots p_k = p_1 p_2 \cdots p_k q_{k+1} q_{k+2} \cdots q_s \)
and by cancelling the common factors we obtain
\[ 1 = q_{k+1} q_{k+2} \cdots q_s \text{ which is a contradiction. Since } q_i > 1 \text{ then } k = s \text{ and } p_1 = q_1, \cdots p_k = q_k. \text{ So } n \text{ has unique representation.} \]

Corollary 2.1.5. Any positive integer \( n > 1 \) can be written uniquely in a canonical form
\[ n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \]
where, for \( i = 1, 2, \cdots, r, \) each \( k_i \) is positive integer and each \( p_i \) is a prime, with \( p_1 < p_2 < \cdots < p_r. \)

Example 2.1.2.
\[ 360 = 2^3 \cdot 3^2 \cdot 5, \quad 4725 = 3^3 \cdot 5^2 \cdot 7, \text{ and } 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2. \]

Theorem 2.1.6. The number \( \sqrt{2} \) is irrational number.

Proof. Suppose that \( \sqrt{2} \) is rational number say \( \sqrt{2} = \frac{a}{b}, \) where \( a \) and \( b \) are both integers with \( \text{g.c.d}(a, b) = 1. \)
Then $a^2 = 2b^2 \implies b|a^2$. If $b > 1$, then by the fundamental theorem of arithmetic, there exists a prime $p \nmid b \implies p|b \implies p|a^2 \implies p|a \implies g.c.d(a,p) \geq p$, contradiction unless $b = 1$. If $b = 1 \implies a^2 = 2$ which is impossible because no integer can be multiplied by itself to give 2. \hfill \Box

**Theorem 2.1.7.** Suppose $a$ and $b$ are positive integers. Let the distinct primes dividing $a$ or $b$ (or both) be $p_1, p_2, \ldots, p_n$. Suppose $a = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n}$ and $b = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ (some of the $j$’s and the $k$’s may be zero). Let $m_i$ be the smaller and $M_i$ be the larger of $j_i$ and $k_i$ for $i = 1, 2, \ldots, n$.

(a) $a | b$ if and only if $j_i \leq k_i$ for $i = 1, 2, \ldots, n$.

(b) $\text{g.c.d}(a, b) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$.

(c) $\text{l.c.m}(a, b) = p_1^{M_1} p_2^{M_2} \cdots p_n^{M_n}$.

### 2.2 The sieve of Eratosthenes

**Theorem 2.2.1.** If $n$ is composite it must have a prime factor $p \leq \sqrt{n}$.

*Proof.* Let $n$ be composite, then $n = d_1 d_2$ where $d_1$ and $d_2 > 1$. If $d_1$ and $d_2 > \sqrt{n}$ then $n = d_1 d_2 > (\sqrt{n})^2 = n$ which impossible. Suppose $d \leq \sqrt{n}$, then $d_1$ is either prime or else has a prime divisor $p \leq \sqrt{n}$. \hfill \Box

**Corollary 2.2.2.** If the integer $n > 1$ has no prime divisor $\leq \sqrt{n}$, then $n$ is prime.

**Example 2.2.1.** Determine whether $n = 1999$ is prime number or composite number.

*Solution:* $\sqrt{n} = \sqrt{1999} < 45$, then all of the primes $2, 3, 5, \ldots, 43 < 45$ are not divisors of 1999 so $n = 1999$ is prime.

**Theorem 2.2.3.** (Euclid) There are an infinite number of primes.

*Proof.* Suppose that $p_1, p_2, \ldots, p_r$ are a finite number of primes. Let $n = 1 + p_1 p_2 \cdots p_r$. Since $n > 1$, then if $p$ is a prime number and $p \nmid n$, then $p$ is one of the primes $p_1, p_2, \ldots, p_r$ because $p \nmid p_1 p_2 \cdots p_r \implies p \nmid n - p_1 p_2 \cdots p_r \implies p | 1 \implies p = 1$, a contradiction because $p > 1$. So $p$ does not belong to set of primes $p_1, p_2, \ldots, p_r$, so the number of primes is infinite. \hfill \Box
Remark 2.2.1. If \( p_n \) is the \( n \)th prime number in the natural order then
\[
p_{n+1} \leq p_1p_2 \cdots p_n + 1 \quad \text{for} \quad n \geq 1.
\]
For example if \( n = 3 \) then \( p_4 = 7 \leq p_1p_2p_3 + 1 = (2) \cdot (3) \cdot (5) + 1 = 31 \).

The above estimation is wide; a sharper limitation to this size of \( p_n \) is given in the following theorem.

**Theorem 2.2.4.** If \( p_n \) is the \( n \)th prime number, then \( p_n \leq 2^{2^{n-1}} \).

**Proof.** By induction on \( n \). If \( n = 1 \), then \( p_1 = 2^{2^0} = 2^1 = 2 \implies p_1 \leq 2 \).
Assume that the result is true for \( n > 1 \), then \( p_n \leq 2^{2^{n-1}} \). We will show the result is true for \( n + 1 \).
Since
\[
p_{n+1} \leq p_1p_2 \cdots p_n + 1
\leq 2 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+ \cdots + 2^{n-1}} + 1.
\]
And since \( 1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1 \), then
\[
p_{n+1} \leq 2^{2^n - 1} + 1.
\]
But \( 1 \leq 2^{2^{n-1}} \) for all \( n > 1 \), then,
\[
p_{n+1} \leq 2^{2^n - 1} + 2^{2^n - 1} = 2 \cdot 2^{2^n - 1} = 2^{2^n}.
\]
So the result is true for \( n + 1 \).

**Corollary 2.2.5.** For \( n \geq 1 \), there are at least \( n + 1 \) primes less than \( 2^{2^n} \).

**Proof.** \( p_1, p_2, \cdots, p_{n+1} \) are all less than \( 2^{2^n} \).

### 2.3 The Goldbach conjecture

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

**Proof.** Let \( k = 4n + 1 \) and \( k' = 4m + 1 \) then \( k \cdot k' = (4n + 1)(4m + 1) = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1 \) which is of the desired form.

**Theorem 2.3.2.** There is infinite number of primes of the form \( 4n + 3 \)
Proof. Assume that there exist only finitely many primes of the form $4n+3$, call them $q_1$, $q_2$, \ldots $q_s$. Consider the positive integer

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

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

\[
\text{Theorem 2.3.3. If } a \text{ and } b \text{ are relatively prime positive integers then the arithmetic progression}
\]

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

contains infinitely many primes.

Proof. Suppose that $p = a+nb$, where $p$ is prime. If $n_k = n + kp$, for $k = 1, \; 2, \; 3, \cdots$ then the $n_k$th term in the progression is

$$a + n_kb = a + (n + kp)b = (a + nb) + kpb = p + kpb \Rightarrow p|a + n_kb.$$ 

So the arithmetic progression must contain infinitely many composite numbers which are divisible by infinitely prime numbers. 

\[
18
\]
Chapter 3

The theory of congruences

3.1 Basic properties of congruence

**Definition 3.1.1.** Let \( n \) be a fixed positive integer. Two integers \( a \) and \( b \) are said to be congruent modulo \( n \), symbolized by \( a \equiv b \pmod{n} \) if \( n \) divides the difference \( a - b \); that is provided that \( a - b = kn \) for some integer \( k \).

**Example 3.1.1.** If \( n = 7 \) then \( 3 \equiv 24 \pmod{7} \), and \( -31 \equiv 11 \pmod{7} \).

If \( n \nmid (a - b) \), then we say that \( a \) is not incongruent to \( b \) modulo \( n \) and in this case we write \( a \not\equiv b \pmod{n} \). For example \( 25 \not\equiv 12 \pmod{7} \) since \( 7 \nmid (25 - 12) = 13 \).

**Remark 3.1.1.**

1. Any two integers are congruent modulo 1.
2. Two integers are congruent modulo 2 when they are both even or both odd.
3. Given integer \( a \), let \( q \) and \( r \) be its quotient and remainder upon division by \( n \), so that

\[
a = nq + r, \quad 0 \leq r < n \implies a - r = nq \implies n|a - r \implies a \equiv r \pmod{n}.
\]

There are \( n \) choices of \( r \), \( r = 0, 1, \ldots, n - 1 \). So every integer \( a \) is congruent modulo \( n \) to exactly one of the numbers \( 0, 1, 2, \ldots, n - 1 \). and \( a \equiv 0 \pmod{n} \iff n|a \).

The set of \( n \) integers \( 0, 1, 2, \ldots n - 1 \) is called the set of least positive residues modulo \( n \).
Definition 3.1.2. The set of \( n \) integers \( a_1, a_2, a_3, \ldots a_n \) is said to form a complete residues set (or a complete residue system) modulo \( n \) if every integer \( y \) is congruent modulo \( n \) to one and only one of the \( a_i \) for \( 1 \leq i \leq n \); i.e. the set \( \{a_1, a_2, a_3, \ldots a_n\} \) is called complete residue set modulo \( n \) if \( \forall y \in \mathbb{Z}, \exists \) one and only one \( a_i, 1 \leq i \leq n \) \( \ni y \equiv a_i \pmod{n} \).

Example 3.1.2. Any integers \( a_1, a_2, \ldots a_n \) are congruent modulo to \( 0, 1, 2, \ldots n-1 \), taken in some order.

Example 3.1.3. \(-12, -4, 11, 13, 22, 82, 91\) constitute a complete set of residues modulo 7, because \(-12 \equiv 2, -4 \equiv 3, 11 \equiv 4, 13 \equiv 6, 22 \equiv 1, 82 \equiv 5 \) and \( 91 \equiv 0 \) all modulo 7.

Remark 3.1.2. Any \( n \) integers from a complete residue set modulo \( n \) if and only if no two of the integers are congruent modulo \( n \).

Theorem 3.1.1. For arbitrary integers \( a \) and \( b \), \( a \equiv b \pmod{n} \) if and only if \( a \) and \( b \) leave the same nonnegative remainder when divided by \( n \).

Proof. Let \( a \equiv b \pmod{n} \implies n|a-b \), so \( \exists k \in \mathbb{Z} \ni a-b = nk \implies a = b + nk \) by division algorithm

\[
b = qn + r, \quad 0 \leq r < n \text{ so } n \text{ leaves the remainder } r,
\]

then

\[
a = b + kn = (qn + r) + kn = (q + k)n + r \implies a \text{ has the same remainder as } b.
\]

Conversely, suppose that

\[
a = q_1n + r, \quad b = q_2n + r \ni 0 \leq r < n.
\]

Then

\[
a - b = (q_1n + r) - (q_2n + r) = (q_1 - q_2)n \implies n|a - b \implies a \equiv b \pmod{n}.
\]

Example 3.1.4.

\[-56 \equiv (-7)9 + 7 \]
\[-11 \equiv (-2)9 + 7,\]

then by the above theorem (3.1.1)

\[-56 \equiv -11 \pmod{9}.\]
Theorem 3.1.2. Let $n > 0$ be fixed and $a, b, c, d$ be arbitrary integers. Then the following properties hold:

(1) $a \equiv a \pmod{n}$.

(2) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

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

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

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

(6) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer $k$.

Proof. (1) $a - a = 0 \implies n|a - a \implies a \equiv a \pmod{n}$.

(2) $n|a - b \implies \exists k \in Z \ni a - b = nk \implies b - a = -kn \implies n|b - a \implies b \equiv a \pmod{n}$.

(3) Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then there exist integers $h$ and $k$ satisfying $a - b = nk$ and $b - c = kn$. It follows that $a - c = (a - b) + (b - c) = hn + kn = (h + k)n$, so $n|a - c \implies a \equiv c \pmod{n}$.

(4) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $\exists k_1, k_2 \in Z \ni a - b = k_1n$, $c - d = k_2n \implies (a + c) - (b + d) = k_1n + k_2n = (k_1 + k_2)n \implies a + b \equiv (b + d) \pmod{n}$.

For the second assertion of (4)

$ac = (b + k_1n)(d + k_2n) = bd + (bk_2 + dk_1 + k_1k_2)n \implies ac \equiv bd \pmod{n}$.

(5) $a \equiv b \pmod{n}$, then $n|a - b \implies n|(a + c) - (b + c)$ also $n|ca - cb \forall c \in Z \implies a + c \equiv b + c \pmod{n}$ and $ca \equiv cb \pmod{n}$.

(6) For $k = 1$ the result holds.

Assume it is true for $n = k \implies a^k \equiv b^k \pmod{n}$, then by (4) since $a \equiv b \pmod{n} \implies a \cdot a^k \equiv b \cdot b^k \pmod{n} \implies a^{k+1} \equiv b^{k+1} \pmod{n}$. So it is true for $n = k + 1$. So the induction step is complete.

\[\square\]
Example 3.1.5. Show that $2^{20} \equiv 1 \pmod{41}$.

Solution: $2^{5} \equiv 32 \equiv -9 \pmod{41} \implies 2^{20} = (2^{5})^{4} \equiv (-9)^{4} \pmod{41} \equiv (81)(81) \equiv (-1)(-1) \equiv 1 \pmod{41}$.

Example 3.1.6. Find the remainder obtained upon dividing the sum $1! + 2! + 3! + 4! + \cdots 99! + 100!$ by 12.

Solution:

fork \geq 4, 
4! \equiv 0 \pmod{12} \implies k! \cdot 5 \cdot 6 \cdot \cdots k \equiv 0 \pmod{12}.

1! + 2! + 3! + 4! + \cdots 100! \equiv 1 + 2 + 6 + 0 + \cdots 0 \equiv 9 \pmod{12}.

So the sum leaves a remainder of 9 when divided by 12.

Remark 3.1.3.
If $a \equiv b \pmod{n} \implies ac \equiv bc \pmod{n}$ but the converse need not true. for example $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$ but $4 \not\equiv 1 \pmod{6}$.

Theorem 3.1.3. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{\frac{n}{d}}$ where $d = \gcd(c, n)$.

Proof. If $ca \equiv cb \pmod{n}$, then $n|ca - cb \implies \exists k \in \mathbb{Z} \ni c(a - b) = kn$ but $\gcd(c, n) = d \implies \gcd\left(\frac{c}{d}, \frac{n}{d}\right) = 1 \implies \frac{c}{d}(a - b) = k\frac{n}{d} \implies \frac{n}{d}|\frac{c}{d}(a - b)$.

But $\gcd\left(\frac{c}{d}, \frac{n}{d}\right) = 1$, so by previous theorem $\frac{n}{d}|(a - b) \implies a \equiv b \pmod{\frac{n}{d}}$. □

Corollary 3.1.4. If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$ then $a \equiv b \pmod{n}$.

Proof. If $ca \equiv cb \pmod{n}$ then $n|ca - cb = c(a - b)$ but $\gcd\left(n, c\right) = 1 \implies n|a - b \implies a \equiv b \pmod{n}$. □

Corollary 3.1.5. If $ca \equiv cb \pmod{p}$, where $p$ is prime number and $p \nmid c$ then $a \equiv b \pmod{p}$.

Proof. $p \nmid c \implies \gcd(p, c) = 1$ and $p|ca - cb = c(a - b) \implies p|a - b \implies a \equiv b \pmod{p}$. □

Example 3.1.7. $33 \equiv 15 \pmod{9} \implies 3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$ and $\gcd(3, 9) = 3 \implies 11 \equiv 5 \pmod{3}$.

Example 3.1.8. $-35 \equiv 45 \pmod{8}$ then $5(-7) \equiv 5(9) \pmod{8}$, since $\gcd(5, 8) = 1$ then $-7 \equiv 9 \pmod{8}$.
Remark 3.1.4. (1) If \( a \cdot b \equiv 0 \pmod{n} \) then it is not necessarily true that \( a \equiv 0 \pmod{n} \) and \( b \equiv 0 \pmod{n} \). For example \( 4 \cdot 3 \equiv 0 \pmod{12} \) but \( 3 \not\equiv 0 \pmod{12} \) and \( 4 \not\equiv 0 \pmod{12} \).

(2) If \( a \cdot b \equiv 0 \pmod{n} \) and \( \gcd(a, n) = 1 \) then \( b \equiv 0 \pmod{n} \).

(3) If \( p \) is prime and \( a \cdot b \equiv 0 \pmod{p} \) then either \( a \equiv 0 \pmod{p} \) or \( b \equiv 0 \pmod{p} \).

3.2 Special divisibility tests

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

\[
N = a_mb^m + a_{m-1}b^{m-1} + \cdots + a_2b^2 + a_1b + a_0.
\]

Where the coefficient \( a_k \) can take on the \( b \) different values \( 0, 1, 2, \cdots, b - 1 \).

By division algorithm

\[
N = q_1b + a_0, \quad 0 \leq a_0 < b.
\]

If \( q_1 \geq b \), we can divide once more, obtaining

\[
q_1 = q_2b + a_1, \quad 0 \leq a_1 < b_1.
\]

Now substitute for \( q_1 \) in the earlier equation to get

\[
N = (q_2b + a_1)b + a_0 = q_2b^2 + a_1b + a_0.
\]

As long as \( q_2 \geq b \), we can continue in the same fashion, going one more step: \( q_2 = q_3b + a_2 \), where \( 0 \leq a_2 < b \), we hence

\[
N = q_3b^3 + a_2b^2 + a_1b + a_0.
\]

Since \( N > q_1 > q_2 > \cdots \geq 0 \) is a strictly decreasing sequence of integers, this process must eventually terminate say, at the \( (m-1) \)th stage, where \( q_{m-1} = q_mb + a_{m-1}, \quad 0 \leq a_{m-1} < b \) and \( 0 \leq q_m < b \). Setting \( a_m = q_m \), we reach the representation

\[
N = a_mb^m + a_{m-1}b^{m-1} + \cdots + a_1b + a_0.
\]
Which was our aim.
The number
\[
N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0
\]
may be replaced by the simpler symbol
\[
N = (a_m \ldots a_2 a_1 a_0)_{b}.
\]
We call this the base \(b\) place value notation for \(N\).
If \(b = 2\) the resulting system of enumeration is called the binary number system.

Example 3.2.1. \(a = 105\) can be written in binary system as
\[
105 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1 = 2^6 + 2^5 + 2^3 + 1.
\]
Or in abbreviated form
\[
105 = (1101001)_{2}.
\]
And \((1001111)_{2}\) translates into
\[
1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 = 2^6 + 2^3 + 2^2 + 2 + 1 = 79.
\]

**decimal system:** If the base \(b = 10\) then we can represent any integer with this base.

Example 3.2.2. \(a = 1492 = 1 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10 + 2\).
The integers 1, 4, 9, 2 are called the digits of the given number.
1 is called the thousands digit, 4 the hundreds digits, 9 the tens digit, and 2 the unit digit.

Theorem 3.2.1. Let \(P(x) = \sum_{k=0}^{m} c_k x^k\) be a polynomial function of \(x\) with integral coefficients \(c_k\). If \(a \equiv b \pmod{n}\), then \(P(a) \equiv P(b) \pmod{n}\).

Proof. Since \(a \equiv b \pmod{n}\) then \(a^k \equiv b^k \pmod{n}\) for \(k = 0, 1, 2, \ldots, m\) therefore \(c_k a^k \equiv c_k b^k \pmod{n}\) for all such \(k\). Adding these congruences, we conclude that
\[
\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}.
\]
or \(P(a) \equiv P(b) \pmod{n}\) \(\Box\)

Definition 3.2.1. If \(P(x)\) is a polynomial with integral coefficients, one says that \(a\) is a solution of the congruence \(P(x) \equiv 0 \pmod{n}\) if \(P(a) \equiv 0 \pmod{n}\).
Corollary 3.2.2. If \( a \) is a solution of \( P(x) \equiv 0 \pmod{n} \) and \( a \equiv b \pmod{n} \), then \( b \) is also a solution.

Proof. From previous theorem \( P(a) \equiv P(b) \pmod{n} \). Hence if \( a \) is a solution of \( P(x) \equiv 0 \pmod{n} \), then \( P(b) \equiv P(a) \equiv (mod n) \), making \( b \) a solution.

Theorem 3.2.3. Let \( N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0 \), be the decimal expansion of the positive integer \( N \), \( 0 \leq a_k < 10 \), and let \( S = a_0 + a_1 + \cdots + a_m \). Then \( 9 | N \) if and only if \( 9 | S \).

Proof. Consider \( P(x) = \sum_{k=0}^{m} a_k x^k \), a polynomial with integral coefficients. \( 10 \equiv 1 \pmod{9} \Rightarrow P(10) \equiv P(1) \pmod{9} \), but \( P(10) = N \) and \( P(1) = a_0 + a_1 + \cdots + a_m = S \Rightarrow N \equiv S \pmod{9} \). It follows that \( N \equiv 0 \pmod{9} \) if and only if \( S \equiv 0 \pmod{9} \).

Which is the wanted prove.

Theorem 3.2.4. Let \( N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0 \), be the decimal expansion of the positive integer \( N \), \( 0 \leq a_k < 10 \), and let \( T = a_0 - a_1 + a_2 - \cdots + (\pm 1)^m a_m \). Then \( 11 | N \) if and only if \( 11 | T \).

Proof. Put \( P(x) = \sum_{k=0}^{m} a_k x^k \). Since \( 10 \equiv -1 \pmod{11} \), we get \( P(10) \equiv P(-1) \pmod{11} \).

But \( N = P(10) \), \( T = P(-1) = a_0 - a_1 + a_2 - \cdots + (\pm 1)^m a_m \). So \( N \equiv T \pmod{11} \), it follows that \( N \equiv 0 \pmod{11} \) if and only if \( T \equiv 0 \pmod{11} \).

Example 3.2.3. Let \( N = 1571724 \) then \( 1 + 5 + 7 + 1 + 7 + 2 + 4 = 27 \) is divisible by \( 9 \Rightarrow 9 | N \).

And it divisible by \( 11 \) because \( 4 - 2 + 7 - 1 + 7 - 5 + 1 = 11 \) is divisible by \( 11 \Rightarrow 11 | N \).

3.3 Linear congruences

Definition 3.3.1. An equation \( ax \equiv b \pmod{n} \) is called a linear congruence and \( x_0 \) is a solution of this congruence if \( ax_0 \equiv b \pmod{n} \).

Theorem 3.3.1. 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 it has \( d \) mutually incongruent solutions modulo \( n \).
Proof. Let \( ax \equiv b \pmod{n} \) has a solution the there exists \( x_0 \in \mathbb{Z} \ni ax_0 \equiv b \pmod{n} \) \( \Rightarrow n|ax_0 - b \Rightarrow y \in \mathbb{Z} \ni ax_0 - b = ny \Rightarrow ax_0 - ny = b, \) but this equation has a solution, then \( \gcd(a, n) = d|b. \)

Conversely, let \( d|b \) and let \( ax \equiv b \pmod{n} \) \( \Rightarrow n|ax - b \Rightarrow \exists y \in \mathbb{Z} \ni ax - b = ny \Rightarrow \frac{ax}{n} - \frac{ny}{n} = b, \) since \( \gcd(a, n) = d|b. \)

Let now \( x = x_0 + \frac{n}{d}t \) be all solutions for the congruence, where \( 0 \leq t \leq d - 1. \) We will show that the solutions \( x_0, x_0 + \frac{n}{d}, \ldots, x_0 + \frac{(d-1)n}{d} \) are not congruent modulo \( n. \)

Suppose that \( x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}, \) where \( 0 \leq t_1 < t_2 \leq d - 1. \) We have \( \frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}, \) but \( \gcd(\frac{n}{d}, n) = \frac{n}{d} \Rightarrow t_1 \equiv t_2 \pmod{\frac{n}{d}} \Rightarrow t_1 \equiv t_2 \pmod{d} \Rightarrow d|t_2 - t_1 \Rightarrow d < t_2 - t_1, \) but \( 0 \leq t_2 - t_1 < d, \) contradiction.

Then \( x_0 + \frac{n}{d}t_1 \not\equiv x_0 + \frac{n}{d}t_2 \pmod{n}. \)

It remains to show that any other solution \( x_0 + \frac{n}{d}t \) is congruent modulo \( n \) to one of the \( d \) integers listed above.

By division algorithm \( t = qd + r \) where \( 0 \leq r \leq d - 1. \) Hence

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

whith \( x_0 + \frac{n}{d}r \) being one of our \( d \) selected solutions. \( \square \)

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

**Example 3.3.1.** Solve the congruence \( 18x \equiv 30 \pmod{42}. \)

**Solution** \( \gcd(18, 42) = 6 \) and \( 6|30 \implies \)

the congruence has exactly six solutions which are incongruent modulo \( 42. \)

Then

\[
18x \equiv 30 \pmod{42} \\
3x \equiv 5 \pmod{7} \\
6x \equiv 10 \pmod{7}
\]

26
\[ -x \equiv 3 \pmod{7} \implies x \equiv -3 \pmod{7} \]
\[ x \equiv 4 \pmod{7} \implies x_0 = 4. \]

All solutions of the original congruence are
\[ x = x_0 + \frac{42}{6} t = 4 + 7t, \ 0 \leq t < 6, \]
which are \( x = 4, 11, 18, 25, 32, 39 \pmod{42} \).

**Example 3.3.2.** Solve the congruence
\[ 9x \equiv 21 \pmod{30}. \]

**Solution** \( \gcd(9, 30) = 3 \), \( 3 \mid 21 \), so the congruence is solvable, then
\[ 3x \equiv 7 \pmod{10} \]
\[ 21x \equiv 49 \pmod{10} \]
\[ x \equiv 9 \pmod{0} \implies x_0 = 9. \]

All solutions are \( x = x_0 + t \frac{30}{3} = 9 + 10t \) for \( 0 \leq t < 3 \).

**Theorem 3.3.3.** (*The Chinese Remainder theorem*)

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
\[ x \equiv a_1 \pmod{n_1} \]
\[ x \equiv a_2 \pmod{n_2} \]
\[ \vdots \]
\[ x \equiv a_r \pmod{n_r} \]

has a common solution which is unique modulo \( n_1 n_2 \cdots n_r \).

**Proof.** Let \( n = \prod_{i=1}^{r} n_i = n_1 n_2 \cdots n_r \) and \( N_k = \frac{n}{n_k} \) for \( 1 \leq k \leq r \).

Since \( \gcd(n_i, n_j) = 1 \) for \( i \neq j \), then \( \gcd(N_k, n_k) = 1 \implies \exists \) a unique solution \( x_k \) for the congruence \( N_k x \equiv 1 \pmod{n_k} \) \( \forall k, \ 1 \leq k \leq r \).

\( \implies a_k N_k x_k \equiv a_k \pmod{n_k} \) \( \forall k, 1 \leq k \leq r, \) and \( a_k N_k x_k \equiv 0 \pmod{n_j} \) for \( j \neq k \).

Let
\[ \bar{x} = \sum_{k=1}^{r} a_k N_k x_k \equiv a_k N_k x_k \pmod{n_k}. \]
the $\bar{x}$ is a common solution for the original system of congruences.

But $x_k$ was chosen to satisfy the congruence $N_kx \equiv 1 \pmod{n_k}$, which forces 
\[ \bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}. \]

This implies that the solution of the given system of congruences exists.

To show uniqueness,

Suppose that $x'$ is another common solution of the congruences 
\[ x \equiv a_k \pmod{n_k}, \text{ for } 1 \leq k \leq r. \]

Then $x' \equiv \bar{x} \pmod{n_k}$ for $1 \leq k \leq r$.

Then $\text{lcm}(n_1, n_2, \cdots, n_r)|x' - \bar{x}$, but $\gcd(n_i, n_j) = 1$ for $i \neq j$, then $n|x' - \bar{x}$ then $x' \equiv \bar{x} \pmod{n}$.

\[ \square \]

**Example 3.3.3.** Find the common solution of the system of congruences 
\[ x \equiv 2 \pmod{3}, \ x \equiv 3 \pmod{5}, \ x \equiv 2 \pmod{7}. \]

**Solution**

\[ a_1 = 2, \ a_2 = 3, \ a_3 = 2 \text{ and } n_1 = 3, \ n_2 = 5, \ n_3 = 7 \]

\[ n = 3 \cdot 5 \cdot 7 = 105. \]

\[ N_1 = \frac{n}{n_1} = 35, \ N_2 = \frac{n}{n_2} = 21, \ N_3 = \frac{n}{n_3} = 15. \]

The linear congruences

\[ 35x \equiv 1 \pmod{3}, \ 21x \equiv 1 \pmod{5}, \ 15x \equiv 1 \pmod{7}, \]

has solutions

\[ x \equiv 2 \pmod{3}, \ x \equiv 1 \pmod{5}, \ x \equiv 1 \pmod{7}. \]

So $x_1 = 2, \ x_2 = 1, \ x_3 = 1$ respectively.

Thus the common solution of the original system is given by

\[ \bar{x} = \sum_{k=1}^{3} a_k N_k x_k = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}. \]

The solution of the congruence $ax + by \equiv c \pmod{n}$

The congruence $ax + by \equiv c \pmod{n}$ has a solution if and only $\gcd(a, b, n)|c$. If $\gcd(a, b, n) = 1$, then either $\gcd(a, n) = 1$ or $\gcd(b, n) = 1$.

Let $\gcd(a, b) = 1$. The congruence can be written in the form

\[ ax \equiv c - by \pmod{n}. \]
then the congruence has a unique solution $x$ for each of the $n$ incongruent values of $y$.

**Example 3.3.4.** Solve the congruence

$$7x + 4y \equiv 5 \pmod{12},$$

then $7x \equiv 5 - 4y \pmod{12}$. Substitution of $y \equiv 5 \pmod{12}$ then $7x \equiv -15 \pmod{12}$. Then

$$-5x \equiv -15 \pmod{12} \implies x \equiv 3 \pmod{12}$$

It follows that $x \equiv 3 \pmod{12}$ and $x \equiv 5 \pmod{12}$ is one of the 12 incongruent solutions of $7x + 4y \equiv 5 \pmod{12}$.

**Theorem 3.3.4.** The system of linear congruences

$$ax + by \equiv r \pmod{n} \quad \text{(1)}$$

$$cx + dy \equiv s \pmod{n} \quad \text{(2)}$$

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

**Proof.** multiply the congruence (1) by $d$ and the congruence (2) by $b$ we get

$$adx + bdy \equiv rd \pmod{n}$$

$$cby + dby \equiv sb \pmod{n}.$$  

Now subtract the last equations we get

$$(ad - cb)x \equiv rd - bs \pmod{n} \quad \text{(3)}.$$  

Since $\gcd(ad - bc, n) = 1$ then the congruence

$$(ad - bc)z \equiv 1 \pmod{n}$$

has a unique solution; denote the solution by $t$.

Now multiply the congruence (3) by $t$ we obtain

$$(ad - bc)tx \equiv (dr - bs)t \pmod{n}.$$  

Then

$$x \equiv (dr - bs)t \pmod{n}. 29$$
now if we multiply the congruence (1) by $c$ and the congruence (2) by $a$ and subtract we obtain
\[(ad - bc)y \equiv (as - cr)(mod \ n).\]

now multiply the congruence by $t$ we get
\[y \equiv t(as - cr)(mod \ n).\]

So we have get the solution of the congruence. \qed

**Example 3.3.5.** Solve the system of congruences

\[
\begin{align*}
7x + 3y &\equiv 10 \pmod{16}, \\
2x + 5y &\equiv 9 \pmod{16}
\end{align*}
\]

**Solution:** Since $gcd(7 \cdot 5 - 2 \cdot 3, 16) = 1$ so there is a solution of the congruences. Multiply the first congruence by 5, the second by 3 and subtract we get
\[29x \equiv 23 (mod \ 16)\]
then
\[13x \equiv 7 (mod \ 16),\]
now multiply by 5 we get
\[65x \equiv 35 \pmod{16} \implies x \equiv 3 (mod \ 16).\]

Now multiply the first congruence by 2 and the second by 7 we get
\[14x + 6y \equiv 20 (mod \ 16)\]
\[14x + 35y \equiv 63 (mod \ 16).\]
now by subtraction we get
\[29y \equiv 43 (mod \ 16) \implies 13y \equiv 11 (mod \ 16),\]
multiply by 5 we get $65y \equiv 55 (mod \ 16) \implies y \equiv 7 (mod \ 16)$. 

30
Chapter 4

Fermat’s theorem

4.1 Fermat’s little theorem

Theorem 4.1.1. (Fermat’s theorem)

If \( p \) is a prime and \( p \nmid a \) then \( a^{p-1} \equiv 1 \pmod{p} \).

Proof. Consider the first \( p - 1 \) positive multiples of \( a \); that is the integers

\[ a, 2a, 3a, \ldots, (p-1)a. \]

None of these numbers is congruent modulo \( p \) to any other, nor is any congruent to zero, because if \( ra \equiv sa \pmod{p} \), for \( 1 \leq r \leq s \leq p - 1 \) and \( \gcd(a, p) = 1 \implies r \equiv s \pmod{p} \). A contradiction.

Therefore, the above set of integers must be congruent modulo \( p \) to 1, 2, 3, \ldots, \( p-1 \), taken in some order. multiplying all these congruences together, we find that

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

Then

\[ a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \]

but \( p \nmid (p-1)! \) then \( \gcd((p-1)!, p) = 1 \implies a^{p-1} \equiv 1 \pmod{p} \). \( \square \)

Corollary 4.1.2. If \( p \) is a prime, then \( a^p \equiv a \pmod{p} \) for any integer \( a \).

Proof. when \( p | a \) then \( p | a^p \implies p | a^p - a \implies a^p \equiv a \pmod{p} \).

If \( p \nmid a \), then \( a^{p-1} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p} \). \( \square \)

Theorem 4.1.3. \((a + 1)^p \equiv a^p + 1 \equiv (mod \ p) \equiv a + 1 \pmod{p} \).
Proof.

\[(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1 \equiv a^p + 0 + \cdots + 0 + 1 \pmod{p} \equiv a+1 \pmod{p}.
\]

\[\square\]

Example 4.1.1. Verify that \(5^{38} \equiv 4 \pmod{11}\).

Solution: \(5^{38} = 5^{10\cdot3+8} = (5^{10})^3 \cdot (5^2)^4\) since \(\gcd(5, 11) = 1\) then \(5^{11-1} \equiv 1 \pmod{11}\) \(\implies 5^{10} \equiv 1 \pmod{11}\) \(\implies 5^{38} \equiv 1^3 \cdot (5^2)^4 \equiv 1 \cdot 3^4 \equiv 81 \pmod{11}\) \(\equiv 4 \pmod{11}\).

Note: (1) If \(n\) is composite then it is not necessarily true \(a^n \equiv a \pmod{n}\).

For Example 2 \(117 = 2^{7\cdot16+5} = (2^7)^{16} \cdot 2^5 \pmod{117}\) and \(2^7 = 128 \equiv 11 \pmod{117}\), we have

\[2^{117} \equiv 11^{16} \cdot 2^5 \pmod{117} \equiv (121)^8 \cdot 2^5 \pmod{117} \equiv 4^8 \cdot 2^5 \pmod{117}
\]

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

The number 117 = 13 \cdot 9 is a composite number.

(2) If \(a^{n-1} \equiv 1 \pmod{n}\) \(\implies n\) is not necessarily prime.

For example \(2^{341-1} \equiv 1 \pmod{341}\) but 341 = 11 \cdot 31 is not prime.

Lemma 4.1.4. If \(p\) and \(q\) are distinct primes such that \(a^p \equiv a \pmod{q}\) and \(a^q \equiv a \pmod{p}\), then \(a^{pq} \equiv a \pmod{pq}\).

Proof. \((a^q)^p \equiv a^q \pmod{pq}\) \(\forall a \in \mathbb{Z}\). While \(a^q \equiv a \pmod{p}\) \(\implies a^{pq} \equiv a \pmod{p}\) or \(p|a^{pq} - a\), also \(q|a^{pq} - a\). Since \(\text{lcm}(p, q) = pq|a^{pq} - a \implies a^{pq} \equiv a \pmod{pq}\). \(\square\)

Example 4.1.2. Show that \(2^{340} \equiv 1 \pmod{341}\), where 341 = 11(31).

Solution: \(2^{10} = 1024 = 31 \cdot 33 + 1\)

\[2^{11} = 2 \cdot 2^{10} \equiv 2 \pmod{31} \quad \text{and} \quad 2^{31} = 2(2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11} \implies (2^{11})^{31} \equiv 2 \pmod{11} \cdot 31 \implies 2^{341} \equiv 2 \pmod{341}\]

Since \(\gcd(2, 341) = 1 \implies 2^{340} \equiv 1 \pmod{341}\).

4.2 Wilson’s theorem

Theorem 4.2.1. If \(p\) is a prime then \((p - 1)! \equiv -1 \pmod{p}\).
Proof. If $p = 2$ or $p = 3$ then the proof is trivial.

Let $p > 3$, suppose that $a$ is any one of the $p−1$ positive integers $1$, $2$, $3$, \cdots, $p−1$ and consider the linear congruence $ax \equiv 1 \pmod{p}$, then $\gcd(a, p) = 1$. So the congruence $ax \equiv 1 \pmod{p}$ has a unique solution modulo $p$, $\exists a' \in \mathbb{Z}$ with $1 \leq a' \leq p−1$, satisfying $aa' \equiv 1 \pmod{p}$.

Since $p$ is prime $a = a'$ if and only if $a = 1$ or $p−1$, because $1 \cdot 1 \equiv 1 \pmod{p}$ and $(p−1)^2 \equiv 1 \pmod{p}$. Or the congruence $a^2 \equiv 1 \pmod{p}$ is equivalent to $(a−1)(a+1) \equiv 0 \pmod{p}$, then either

$$a−1 \equiv 0 \pmod{p} \text{ or } a+1 \equiv 0 \pmod{p} \text{ then } a \equiv 1 \pmod{p} \implies a = 1 \text{ or } a+1 = p \implies a = p−1.$$  

If we omit the numbers 1 and $p−1$, the effect is to group the remaining integers $2$, $3$, \cdots, $p−2$ into pairs $a, a'$, where $a \neq a'$; Such that $aa' \equiv 1 \pmod{p}$. When these $\frac{p−3}{2}$ congruences are multiplied together and the factors rearranged we get

$$2 \cdot 3 \cdots (p−2) \equiv 1 \pmod{p}$$

or

$$(p−2)! \equiv 1 \pmod{p}$$

then

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

which implies that $(p−1)! \equiv −1 \pmod{p}$. \hfill \square


Solution: We divide the integers $2$, $3$, \cdots, $11$ into $\frac{p−3}{2} = 5$ pairs each of whose products is congruent to 1 modulo 13. Now write out these congruences explicitly we get

$$2 \cdot 7 \equiv 1 \pmod{13}$$

$$3 \cdot 9 \equiv 1 \pmod{13}$$

$$4 \cdot 10 \equiv 1 \pmod{13}$$

$$5 \cdot 8 \equiv 1 \pmod{13}$$

$$6 \cdot 11 \equiv 1 \pmod{13}$$

Multiply the above congruence gives the result

$$11! = (2\cdot7)(3\cdot9)(4\cdot10)(5\cdot8)(6\cdot11) \equiv 1 \pmod{13}.$$  

$\implies 12! \equiv 12 \equiv −1 \pmod{13} \implies (p−1)! \equiv −1 \pmod{p}$ with $p = 13$. 

Note: The converse of Wilson’s theorem is also true If $(n−1)! \equiv −1 \pmod{n}$, then $n$ must be prime.
To prove this: let \( n \) be not 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 \((n - 1)!\), whence \( d|\(n - 1)! \), Now we are assuming that \( n|\(n - 1)! + 1 \) and so \( d|\(n - 1)! + 1 \) too, then \( d|1 \) which is a contradiction. So \( n \) is prime.

**Theorem 4.2.2.** The quadratic congruence \( x^2 + 1 \equiv 0 \pmod{p} \), where \( p \) is an odd prime, has a solution if and only if \( p \equiv 1 \pmod{4} \).

**Proof.** Let \( a \) be any solution of \( x^2 + 1 \equiv 0 \pmod{p} \), so that \( a^2 \equiv -1 \pmod{p} \). Since \( p \nmid a \), the outcome of applying Fermat’s Theorem is

\[
1 = a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (\pmod{p}).
\]

The possibility that \( p = 4k + 3 \) for \( k \in \mathbb{Z} \) is not arise because

\[
(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1 \implies 1 \equiv -1 (\pmod{p}) \implies p|2 \quad \text{which false. Therefore}
\]

\( p = 4k + 1 \) because \( (-1)^{\frac{p+k}{2}} = (-1)^{2k} = 1 \implies 1 \equiv 1 (\pmod{p}) \), so \( p \equiv 1 (\pmod{4}) \). Conversely, Let \( p \equiv 1 (\pmod{4}) \). By Wilson’s theorem, we have \( (p - 1)! = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdots (p - 2)(p - 1) \), also

\[
p - 1 \equiv -1 (\pmod{p}),
\]

\[
p - 2 \equiv -2 (\pmod{p})
\]

\[
\vdots
\]

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

Rearranging the factor produces,

\[
(p - 1)! \equiv 1 \cdot (-1) \cdot (2) \cdot (-2) \cdots \left(\frac{p-1}{2}\right) \cdot \left(-\frac{p-1}{2}\right) (\pmod{p}),
\]

then

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

If \( p \equiv 1 (\pmod{4}) \implies p = 4k + 1 \), then \(-1 \equiv ((\frac{p-1}{2})!)^2 (\pmod{p}) \). The conclusion \( (\frac{p-1}{2})! \) satisfies the quadratic congruence \( x^2 + 1 \equiv 0 (\pmod{p}) \).

**Example 4.2.2.** Solve the congruence \( x^2 + 1 \equiv 0 (\pmod{13}) \).

**Solution:** Since \( p = 13 \) and \( 13 \equiv 1 (\pmod{4}) \) then the congruence has a solution, so \( x = (\frac{p-1}{2})! = 6! = 720 \equiv 5 (\pmod{13}) \) is a solution.

34