1. Long Division

   Definition 0.1. *Given two integers a and b with $b \neq 0$, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.*

2. Greatest Common Divisor

   Definition 0.2. *Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b.*

3. Euclidean Algorithm

   Theorem 0.1. *Let a and b be integers, not both zero. Then the greatest common divisor of a and b is the same as the greatest common divisor of b and $a \mod b$.*

4. Bézout Identity

   Theorem 0.2. *Given integers a and b, not both zero,*

   $$a\mathbb{Z} + b\mathbb{Z} = \{ax + by : x, y \in \mathbb{Z}\} = \gcd(a, b)\mathbb{Z} \tag{1}$$

5. Coprime Integers

   Definition 0.3. *Two integers a and b are said to be coprime if $\gcd(a, b) = 1$.*

6. Prime and Composite Numbers

   Definition 0.4. *An integer $p > 1$ is said to be prime if its only positive divisors are 1 and p. Otherwise, it is said to be composite.*

7. The fundamental theorem of arithmetic

   Theorem 0.3. *Every integer greater than 1 can be written as a product of prime numbers, and this factorization is unique up to the order of the factors.*

8. Diophantine Equations

   Definition 0.5. *A Diophantine equation is an equation where the unknowns are required to be integers or rational numbers.*

9. Rational Root Test

   Theorem 0.4. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If $r = p/q$ is a rational root of $f(x)$, then p divides a_0 and q divides a_n.*

10. Eisenstein's Criterion

    Theorem 0.5. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If there exists a prime p such that p divides a_i for $i = 0, 1, \ldots, n-1$, p does not divide a_n, and p^2 does not divide a_0, then $f(x)$ is irreducible over $\mathbb{Q}$.*

11. Linear Diophantine Equations

Theorem 0.6. *Consider the linear Diophantine equation* $ax+by=c$*, where* $gcd(a,b,c)=1$*.*
If $gcd(a,b) \neq 1$ *then, the equation has no solution.*
If $gcd(a,b)=1$*, then the equation has the following general solution:*

$$x = x_0 + bt, \quad y = y_0 - at \tag{2}$$

where x_0 *and* y_0 *are particular solutions and* t *is an integer.*

12. Chinese Remainder Theorem

Theorem 0.7. *Let* $m_1, m_2, \ldots, m_k$ *be pairwise coprime integers, and let* $a_1, a_2, \ldots, a_k$ *be any integers. Then the system of congruences*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_k \pmod{m_k} \tag{3}$$

has a unique solution modulo $m_1 m_2 \cdots m_k$*.*
The solution is given by

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k \tag{4}$$

where $M_i = m_1 m_2 \cdots m_k / m_i$ *and* y_i *is the modular inverse of* M_i *modulo* m_i*.*