2. Number Theory

Divisibility

An integer a is *divisible* by the integer b, written $b \mid a$, if there exists an integer c, such that $a = bc$. Divisibility is a binary relation.

Transitivity of divisibility relation

If a divides b, and b divides c then there are integers d, e such that $b = ad$ and $c = be$.

$$c = be = (ad)e = a(de)$$

which means that a divides c. In other words,

$$a \mid b \text{ and } b \mid c \implies a \mid c.$$

This is the transitivity property of binary relations, described in Chapter 4.

Euclidean Division

Common Divisors and the GCD function

Basis Representation Theorem

Congruence and Modular Arithmetic

Euler's Totient Function

Euler's totient function, usually written as $\varphi(n)$, counts the number of positive integers up to n that are coprime (relatively prime) to n.

$$\varphi(n) = |\{k \in \mathbb{N} : \gcd(k, n) = 1\}|$$

n	$\{k : \gcd(k, n1) = 1\}$	$\varphi(n)$
1	{1}	1
2	{1}	1
3	{1,2}	2
4	{1,3}	2
5	{1,2,3,4}	4
6	{1,5}	2
7	{1,2,3,4,5,6}	6
8	{1,3,5,7}	4
9	{1,2,4,5,7,8}	6
10	{1,3,7,9}	4
11	{1,2,3,4,5,6,7,8,9,10}	10
12	{1,5,7,11}	4

Fermat's Little Theorem

$$a^p \equiv a(\mod p)$$

for every prime number p, and integer a.

Chinese Remainder Theorem