Number Theory

Jatinder Singh

June, 2022

Contents

1 Divisibility and Primes **2**

1.1 Divisibility 2

1.2 Greatest Common Divisor 3

1.3 Least Common Multiple 4

1.4 Prime Numbers 5

2 Modular Arithmetic **6**

2.1 Congruence 6

2.2 Residue Systems 8

2.3 Modular Arithmetic with Prime Moduli 9

2.4 Primitive Roots and Indices 10

Chapter 1

Divisibility and Primes

1.1 Divisibility

Definition 1.1. *Let $a, b \in \mathbb{Z}$. Then we say **a divides b**, written as $a \mid b$, if there exists another integer q such that $b = aq$.*

Theorem 1.2. $\forall a \in \mathbb{Z}, a \mid 0$ *and* $1 \mid a$

Theorem 1.3. *Let $a, b, c, d \in \mathbb{Z}$. Then*

(a) *if $a \mid b$ then $a \mid bc$;*

(b) *if $a \mid b$ and $b \mid c$ then $a \mid c$;*

(c) *if $a \mid b$ and $a \mid c$ then $a \mid bx + cy$, for all $x, y \in \mathbb{Z}$;*

(d) *if $a \mid b$ and $c \mid d$ then $ac \mid bd$;*

(e) *if $d \mid a$ and $d \mid (a + b)$ then $d \mid b$.*

Theorem 1.4. *Let $a, b \in \mathbb{Z}$. Then $a \mid b \iff a \mid |b| \iff |a| \mid |b|$.*

Theorem 1.5. $\forall a, b \in \mathbb{Z}, (a \mid b) \wedge (b \neq 0) \implies |a| \leq |b|$.

Corollary 1.5.1. $\forall a, b \in \mathbb{Z}, (a \mid b) \wedge (|b| < |a|) \implies b = 0$.

Corollary 1.5.2. $\forall a, b \in \mathbb{N}, a \mid b \implies a \leq b$.

Corollary 1.5.3. $\forall a, b \in \mathbb{Z}, (a \mid b) \wedge (b > 0) \implies a \leq b$.

Theorem 1.6. $\forall a, b \in \mathbb{Z}, (a \mid b) \wedge (b \mid a) \implies |a| = |b|$.

Corollary 1.6.1. $\forall a, b \in \mathbb{N}, (a \mid b) \wedge (b \mid a) \implies a = b$.

Theorem 1.7. *For integers a and b with $a \neq 0$, there exist unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$.*

1.2 Greatest Common Divisor

Definition 1.8. *Let $a \in \mathbb{Z}$. Then $D_a^+ = \{n \in \mathbb{N} : x \mid a\}$.*
So $D_8^+ = \{1, 2, 4, 8\}, D_{12}^+ = \{1, 2, 3, 4, 6, 12\}$ and $D_{-36}^+ = \{1, 2, 3, 6, 12, 18, 36\}$.

Remark. $D_0^+ = \mathbb{N}$ *since* $\forall n \in \mathbb{N}, n \mid 0$.

Theorem 1.9. *Let $a \in \mathbb{Z}$. Then $D_a^+ = D_{|a|}^+$.*

Theorem 1.10. $\forall a \in \mathbb{Z} - \{0\}, \max(D_a^+) = |a|$.

Theorem 1.11. *Let $a \in \mathbb{Z} - \{0\}$. The $D_a^+ \subseteq \{1, 2, \ldots, |a|\}$ is a nonempty finite set.*

Theorem 1.12. *Let $a, b \in \mathbb{Z}$ not both zero. Then $D_a^+ \cap D_b^+$ has a largest element.*

Definition 1.13. *Let $a, b \in \mathbb{Z}$ not both zero. Then* $\gcd(a, b) = \max(D_a^+ \cap D_b^+)$

Remark. *If $a = b = 0$ then* $\gcd(0, 0) = \max(D_0^+ \cap D_0^+) = \max(\mathbb{N} \cap \mathbb{N}) = \max(\mathbb{N})$ *is not defined.*

Theorem 1.14. *Let a and b be integers not both zero. Then* $\gcd(a, b) = \gcd(b, a)$.

Theorem 1.15. $\forall a \in \mathbb{Z} - \{0\}, (\gcd(a, 0) = |a|) \wedge (\gcd(a, a) = |a|)$.

Theorem 1.16. *Let a and b be integers not both zero. Then* $\gcd(a, b) = \gcd(|a|, |b|)$.

Theorem 1.17. *Let a and b be nonzero integers. Then* $1 \leq \gcd(a, b) \leq \min(|a|, |b|)$.

Theorem 1.18. *Let a and b be integers not both zero. Then*
$d = \gcd(a, b) \iff (d \in \mathbb{N}) \wedge (d \mid a) \wedge (d \mid b) \wedge (\forall k \in \mathbb{N}, k \mid a \wedge k \mid b \implies k \leq d)$.

Theorem 1.19. *Let a and b be integers not both zero and suppose $b = aq + r$ for some integers q and r. Then* $\gcd(a, b) = \gcd(a, r)$.

Theorem 1.20. *Let a and b be integers and suppose $a \neq 0$. If $a \mid b$ then* $\gcd(a, b) = |a|$.

Theorem 1.21 (Bezout's Identity)**.** *Let a and b be integers not both zero. Then* $\gcd(a, b)$ *can be written as a linear combination of a and b i.e., there exist integers x and y such that* $\gcd(a, b) = ax + by$. *Moreover* $\gcd(a, b)$ *is the smallest positive linear combination of a and b.*

Theorem 1.22. *If* $\gcd(a,b) = 1$ *and* $a \mid bc$ *then* $a \mid c$.

Theorem 1.23. *Let* a *and* b *be integers not both zero. Then* $\gcd(a,b) = d \iff [(d \in \mathbb{N}) \wedge (d \mid a) \wedge (d \mid b) \wedge (\forall k \in \mathbb{N}, k \mid a \wedge k \mid b \implies k \mid d]$.

Theorem 1.24. *Let* a *and* b *be integers not both zero. Then* $\gcd(a,b) = 1 \iff \exists s,t \in Z \ni as + bt = 1$.

Theorem 1.25. *Let* a *and* b *be integers not both zero and let* $d = \gcd(a,b)$ *then* $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

1.3 Least Common Multiple

Definition 1.26. *Let* $a \in \mathbb{Z} - \{0\}$. *Define* $M_a^+ = \{x \in \mathbb{N} : a \mid x\}$.

Definition 1.27. *Let* a *and* b *be nonzero integers. The* ***least common multiple*** *of* a *and* b *is the smallest* $m \in \mathbb{N}$ *which* $a \mid m$ *and* $b \mid m$. *So* $\operatorname{lcm}(a,b) = min(M_a^+ \cap M_b^+)$.

Theorem 1.28. *Let* a *and* b *be nonzero integers. Then*
$\operatorname{lcm}(a,b) = m \iff (m \in \mathbb{N}) \wedge (a \mid m) \wedge (b \mid m) \wedge (\forall k \in \mathbb{N}, a \mid k \wedge b \mid k \implies m \leq k)$

Theorem 1.29. *Let* a *and* b *be nonzero integers. Then* $\max(|a|,|b|) \leq \operatorname{lcm}(a,b) \leq |ab|$.

Theorem 1.30. *Let* a *and* b *be nonzero integers. If* $a \mid b$ *then* $\operatorname{lcm}(a,b) = |b|$.

Theorem 1.31. *Let* a *and* b *be nonzero integers. Then*
$\operatorname{lcm}(a,b) = m \iff (m \in \mathbb{N}) \wedge (a \mid m) \wedge (b \mid m) \wedge (\forall k \in \mathbb{N}, a \mid k \wedge b \mid k \implies m \mid k)$

Theorem 1.32. *Let* a *and* b *be nonzero integers. Let* $a = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$ *and* $b = p_1^{f_1} \times p_2^{f_2} \times \cdots \times p_k^{f_k}$ *be the decomposition of* a *and* b *with* $e_i \geq 0$ *and* $f_i \geq 0$ *for each* $1 \leq i \leq k$. *Then*

$$\operatorname{lcm}(a,b) = p_1^{max\{e_1,f_1\}} \times p_2^{max\{e_2,f_2\}} \times \cdots \times p_k^{max\{e_k,f_k\}}$$

Theorem 1.33. *Let* a *and* b *be nonzero integers. Then* $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$

Corollary 1.33.1. *If* $\gcd(a,b) = 1$ *then* $\operatorname{lcm} = ab$.

1.4 Prime Numbers

Definition 1.34. *A* ***prime number*** *is an integer $p > 1$ whose only positive divisors are 1 and p. So, let $p \in \mathbb{Z}$ with $p > 1$. Then*

$$\begin{aligned} p \textit{ is prime } &\iff \forall x \in \mathbb{N}, x \mid p \implies (x = 1) \vee (x = p) \\ &\iff \forall x \in \mathbb{N}, (x \neq 1) \wedge (x \neq p) \implies x \nmid p \end{aligned}$$

Definition 1.35. *An integer $n > 1$ that is not prime is said to be* ***composite****. So, let $n \in \mathbb{Z}$ with $n > 1$. Then*
n is composite $\iff \exists x \in \mathbb{N}, (x \neq 1) \wedge (x \neq n) \wedge (x \mid n)$.

Theorem 1.36. *Let $p \in \mathbb{Z}$ with $p > 1$. Then p is prime $\iff \forall a, b \in \mathbb{N}, p = ab \implies (a = 1) \vee (b = 1)$.*

Theorem 1.37. *An integer $n > 1$ is composite $\iff \exists a, b \in \mathbb{N} \ni n = ab$ and $1 < a < n$ and $1 < b < n$.*

Theorem 1.38. *Let p and q be prime numbers. If $p \mid q$, then $p = q$.*

Theorem 1.39. *Every integer larger than 1 is divisible by a prime number.*

Theorem 1.40. *There are an infinite number of primes.*

Theorem 1.41. *Let $n > 1$ be an integer. If n is a composite number then there exists a prime number p such that $p \leq \sqrt{n}$ and $p \mid n$.*

Theorem 1.42. *Let p be a prime. Then $\forall a \in \mathbb{Z}, \gcd(a, p) = 1$ or $\gcd(a, p) = p$.*

Theorem 1.43. *If p is prime then*

(a) $\gcd(a, p) = 1 \iff p \nmid a$;

(b) $\gcd(a, p) = p \iff p \mid a$.

Theorem 1.44. *If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Theorem 1.45. *If p is prime and p divides a product $a_1 a_2 \cdots a_n$ of integers, then p must divide at least one of the factors of the product.*

Theorem 1.46 (Fundamental theorem of arithmetic)**.** *Let $n > 1$ be a natural number. Then n can be written as a product of one or more primes.*

Chapter 2

Modular Arithmetic

2.1 Congruence

Definition 2.1. *Let n be a fixed positive integer and a, b be integers. Then we say 'a is congruent to b modulo n' written as* $a \equiv b \pmod{n} \iff n \mid a{-}b$.

Theorem 2.2. *Let a be an integer. Then* $a \equiv 0 \pmod{n} \iff n \mid a$.

Theorem 2.3. *For arbitrary integers a and b we have*

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n$$

.

Theorem 2.4 (Properties of Congruences)**.**

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

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

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

Theorem 2.5. *Suppose* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$ *then*

(a) $a + c \equiv b + d \pmod{n}$.

(b) $a \cdot c \equiv b \cdot d \pmod{n}$.

(c) $\forall k \in \mathbb{N}$, $a^k \equiv b^k \pmod{n}$.

(d) $P(a) \equiv P(b) \pmod{n}$ *where* $P(x) = c_0 + c_1x + c_2x^2 + \cdots + c_mx^m$ *be an mth degree polynomial with integer coefficients.*

Corollary 2.5.1. *If* $a \equiv b \pmod{n}$ *then for any integer* c *we have* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$.

Theorem 2.6 (Cancellation)**.** *If* $ac \equiv bc \pmod{n}$ *then* $a \equiv b \pmod{\frac{n}{g}}$ *where* $g = \gcd(c, n)$.

Corollary 2.6.1. *If* $ac \equiv bc \pmod{n}$ *and* $\gcd(c, n) = 1$ *then* $a \equiv b \pmod{n}$.

Corollary 2.6.2. *If* $ac \equiv bc \pmod{n}$ *where* p *is prime and* $p \nmid c$ *then*

$$a \equiv b \pmod{p}.$$

Theorem 2.7. *Let* p *be a prime. We have*

(a) *If* $a \times b \equiv 0 \pmod{p}$ *then* $a \equiv 0 \pmod{n}$ *or* $b \equiv 0 \pmod{p}$.

(b) $a^2 \equiv b^2 \pmod{p} \iff a \equiv \pm b \pmod{p}$.

Theorem 2.8. *The linear congruence*

$$ax \equiv b \pmod{n}$$

has a solution $\iff \gcd(a, n) \mid b$.

Theorem 2.9. *The linear congruence*

$$ax \equiv b \pmod{n}$$

has exactly $\gcd(a, n)$ *incongruent modulo* n *provided* $\gcd(a, n) \mid b$. *These residues can be written in compact form as:*

$$x \equiv x_0 + t(\frac{n}{\gcd(a, n)})(modn) \text{ for } t = 0, 1, 2, \cdots, g - 1.$$

Corollary 2.9.1. *If* $\gcd(a, n) = 1$ *then the linear congruence* $ax \equiv b \pmod{n}$ *has a unique solution modulo* n.

Theorem 2.10 (Chinese Remainder Theorem)**.** *Let* $n_1, n_2, n_3, \cdots, n_r$ *be positive integers which are pairwise prime. Then the simultaneous 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 solution satisfying all these equations. Moreover, the solution is unique modulo $n_1 \times n_2 \times \cdots \times n_r$.

2.2 Residue Systems

Definition 2.11. *A set of integers $\{r_1, r_2, \cdots, r_s\}$ is called a complete residue system modulo n if for each integer a there is one and only one r_i such that $a \equiv r_i \pmod{n}$.*

Theorem 2.12. *The set $\{0, 1, 2, \cdots, n-1\}$ forms a complete residue system modulo n.*

Theorem 2.13. *A set of integers $\{r_1, r_2, \cdots, r_s\}$ is called a complete residue system modulo n if*

(a) $r_i \equiv r_j \pmod{n} \implies r_i = r_j$*; meaning they are pairwise incongruent.*

(b) *for each integer a there is one r_i such that $a \equiv r_i \pmod{n}$.*

Theorem 2.14. *Any complete residue system modulo n has n elements.*

Theorem 2.15. *A set of integers $\{r_1, r_2, \cdots, r_n\}$ is a complete residue system modulo n if $r_i \equiv r_j \pmod{n} \implies r_i = r_j$; meaning they are pairwise incongruent.*

Theorem 2.16. *A set of integers $\{r_1, r_2, \cdots, r_n\}$ is a complete residue system modulo n if for each integer a there is one r_i such that $a \equiv r_i \pmod{n}$.*

Theorem 2.17. *If $\{r_1, r_2, \cdots, r_n\}$ is a complete residue system modulo n then $\{r_1 + k, r_2 + k, \cdots, r_n + k\}$ is also a complete residue system modulo n for any integer k.*

Definition 2.18. *A set of integers $\{r_1, r_2, \cdots, r_s\}$ is called a reduced residue system modulo n if*

(a) $\gcd(r_i, n) = 1$ *for each i;*

(b) *for each integer a relatively prime to n there is one and only one r_i such that $a \equiv r_i \pmod{n}$.*

Theorem 2.19. *Let $n > 1$ be a positive integer. Then the set $U_n = \{a \in \mathbb{N} : 1 \leq a \leq n$ and $\gcd(a, n) = 1\}$ forms a reduced residue system modulo n.*

Theorem 2.20. *A set of integers $\{r_1, r_2, \cdots, r_s\}$ is a reduced residue system modulo n if*

(a) $\gcd(r_i, n) = 1$ *for each i;*

(b) $r_i \equiv r_j \pmod{n} \implies r_i = r_j$*; meaning they are pairwise incongruent.*

(c) *for each integer a relatively prime to n there is one r_i such that $a \equiv r_i \pmod{n}$.*

Theorem 2.21. *Any two reduced residue systems modulo n have the same number of elements.*

Definition 2.22. *The number of elements in a reduced residue system modulo n is denoted by $\phi(n)$, called Euler's phi function or the totient function. So $\phi(n)$ is the number of elements between 1 and n that are relatively prime to n. Hence $\phi(n) = |U_n|$.*

Theorem 2.23. *A set of integers $\{r_1, r_2, \cdots, r_{\phi(n)}\}$ is a reduced residue system modulo n if*

(a) $\gcd(r_i, n) = 1$ *for each i;*

(b) $r_i \equiv r_j \pmod{n} \implies r_i = r_j$*; meaning they are pairwise incongruent.*

Theorem 2.24. *A set of integers $\{r_1, r_2, \cdots, r_{\phi(n)}\}$ is a reduced residue system modulo n if*

(a) $\gcd(r_i, n) = 1$ *for each i;*

(b) *for each integer a relatively prime to n there is one r_i such that $a \equiv r_i \pmod{n}$.*

Theorem 2.25. *If $\{r_1, r_2, \cdots, r_{\phi(n)}\}$ is a reduced residue system modulo n and $\gcd(a, n) = 1$ then $\{ar_1, ar_2, \cdots, ar_{\phi(n)}\}$ is also a reduced residue system modulo n.*

2.3 Modular Arithmetic with Prime Moduli

Theorem 2.26 (Fermat's Little Theorem)**.** *Let a be an integer and p be a prime number which does not divide a. Then*

$$a^{p-1} \equiv 1 \pmod{n}$$

Theorem 2.27. *Let a be an integer and p be a prime number which does not divide a. Show that $a^{-1} \equiv a^{p-2} \pmod{n}$.*

Corollary 2.27.1. *Let $a, n \in \mathbb{Z}$ and $\gcd(a, n) = 1$. Then $a^{n-1} \not\equiv 1 \pmod{n} \implies n$ is composite.*

Remark. *Converse of the Fermat's Little Theorem is not true.* $2^{340} \equiv 1 \pmod{341}$ *but* 341 *is composite.*

Corollary 2.27.2. *Let a be any integer and p be a prime number. Then*

$$a^p \equiv a \pmod{n}$$

Theorem 2.28. *Let p be prime. Then*

$$x^2 \equiv 1 \pmod{p} \iff x \equiv 1 \vee x \equiv -1 \pmod{n}$$

Theorem 2.29 (Wilson's Theorem)**.**

$$p \textit{ is prime} \iff (p-1)! \equiv -1 \pmod{p}$$

2.4 Primitive Roots and Indices

Definition 2.30. *Let $n > 1$ and $\gcd(a, n) = 1$. The order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.*

Theorem 2.31. *If $a \equiv b \pmod{n}$ then a and b have the same order.*

Theorem 2.32. *If $\gcd(a, n) > 1$ then $a^k \not\equiv 1 \pmod{n}$ for any positive integer k.*

Theorem 2.33. *Let a modulo n have order k. Then $a^h \equiv 1 \pmod{n} \iff k \mid h$.*

Corollary 2.33.1. *Let a modulo n have order k. Then $k \mid \phi(n)$*

Theorem 2.34. *Let a modulo n have order k. Then $a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{k}$.*

Theorem 2.35. *Let a modulo n have order k. Then the integers $a, a^2, \cdots, a^k$ are incongruent modulo n.*

Theorem 2.36 (Order Formula)**.** *Let a modulo n have order k. Then a^s has order $\dfrac{k}{\gcd(s,k)}$ where s is a positive integer.*