A Bird's-eye View

Number Theory

Dane Jeon

Chapter 1 *The Integers*

This chapter deals with (1.3) mathematical induction, the (1.4) Fibonacci numbers, and (1.5) divisibility.

Def. *The Well-ordering Principle*

Thm 1.2. *The Pigeon Hole Principle*

Thm 1.5. *The Principle of Mathematical Induction*

Def. *The Fibonacci Sequence*

Thm 1.7. There exists a formula that calculates the nth term of the Fibonacci sequence.

Thm 1.8. The divisibility relation is transistive.

Thm 1.9. A linear combination of divisible integers (by a certain dividend) is also also divisible (by the same dividend).

Thm 1.10. *The Division Algorithm*

Chapter 3 *Primes and Greatest Common Divisors*

This chapter deals with (3.1) prime numbers, the (3.2) distribution of primes, (3.3) greatest common divisors and their properties, the (3.4) Euclidean algorithm, the (3.4) fundamental theorem of arithmetic, (3.6) factorisation methods and the Fermat numbers, and (3.7) linear Diophantine equations.

Lem 3.1. Every integer greater than 1 has a prime divisor.

Thm 3.1. There are infinitely many primes.

Thm 3.2. If n is a composite integer, than n has a prime factor not exceeding $\sqrt{n}$.

Thm 3.3. *Dirichlet's Theorem on Primes in Arithmetic Progressions*

Thm 3.4. *The Prime Number Theorem*

Cor 3.4.1. The nth prime number is approximately $n \ln n$.

Thm 3.5. For any positive integer n, there exists a sequence of at least n integers that are all composite.

Thm 3.7. Let a, b, and c be integers. Then,

$$(a + bc, b) = (a, b).$$

Thm 3.8. The greatest common divisors of the integers a and b, not both 0, is the least positive integer that is a linear combination of a and b.

Thm 3.11. *The Euclidean Algorithm*

Thm 3.15. *The Fundamental Theorem of Arithmetic*

Thm 3.16. $[a, b] = ab \;/\; (a, b)$

Thm 3.17 There are infinitely many primes of the form $4n + 3$.

Thm 3.18. Quotient solutions of a polynomial ring over $\mathbb{Z}$ are all integers.

Def. *Fermat Numbers*

Lem 3.10. $F_0\ F_1 \cdots F_{n-1} = F_n - 2$

Thm 3.21. Two distinct Fermat numbers are relatively prime.

Thm 3.23. A two variable linear Diophantine equation has integer solutions if and only if the constant term is divisible by the greatest common divisor of the two coefficients.

Chapter 4 *Congruences*

This chapter contains an (4.1) introduction to congruences, (4.2) linear congruences, and the (4.3) Chinese remainder theorem.

Thm 4.1. If a and b are integers, then a is congruent to b modulo m if and only if there exists an integer k such that

$$a = km + b.$$

Thm 4.2. The relation formed by congruent integers form an equivalent relation on the set of integers.

Thm 4.3. Two integers being congruent modulo a modulus means that the result of reducing the two integers modulo the modulus are identical (the least positive residues of the integers are identical).

Def. *A Complete System of Residues Modulo m*

Thm 4.4. You can add, subtract, and multiply integers to congruences.

Thm 4.5. Consider two integers that are divisible by a common integer c. Given that they are congruent modulo m, the congruence modulo $m \;/\; (c, m)$ is guaranteed.

Cor 4.5.1. If (c, m) is 1, the two quotients aforementioned are congruent modulo m.

Thm 4.6. You can add subtract and multiply congruences from one another.

Lem 4.1. A set of m incongruent integers modulo m forms a complete set of residues modulo m.

Thm 4.7. Consider a vector $\vec{\mathbf{v}}_1$ whose entries are a complete system of residues modulo m. Some $\vec{\mathbf{v}}_2$ defined as $a\vec{\mathbf{v}}_1 + b$ also have entries that consist a complete systems of residues, given that $(a, m) = 1$.

Thm 4.8. You can exponentiate congruences.

Thm 4.9. Two integers are congruent modulo a series of moduli if and only if they are congruent modulo their least common multiple.

Cor 4.9.1. Two integers are congruent modulo a series of moduli that are pairwise relatively prime if and only if they are congruent modulo the product of the moduli.

Thm 4.11. A single variable linear congruence has solutions if and only if the greatest common divisor d of the modulus and the coefficient divides the constant term. When it does, there are exactly d numbers of incongruent solutions.

Cor 4.11.1. When the coefficient and the modulus are relatively prime, there exists a unique solution modulo the modulus.

Def. *Modular Inverse*

Thm 4.12. An positive integer is an inverse of itself if and only if it is congruent to 1 or -1.

Thm 4.13. *Chinese Remainder Theorem*

Def. *Formal Derivative*

Thm 4.15. *Hensel's Lemma*

Cor 4.15.1. In the case that $f(c)$ is congruent to 0 modulo p and $f'(c)$ is not congruent to 0 modulo p, there exists a formula for lifting a solution to modulo p^2 and etcetera.

Chapter 6 *Some Special Congruences*

This chapter deals with (6.1) Wilson's theorem and Fermat's little theorem, and (6.3) Euler's Theorem.

Thm 6.1. *Wilson's Theorem*

Thm 6.2. A positive integer $n > 1$ that satisfies $(n-1)! \equiv -1 \pmod{n}$ is a prime number.

Thm 6.3. *Fermat's Little Theorem*

Thm 6.4. Given that (a, p) is equal to 1 or not, for a positive integer a and prime p, a^p is congruent to a modulo p.

Thm 6.5. For an integer a that is relatively prime to prime p, a^{p-2} is its modular inverse modulo p.

Cor 6.5.1. For an integer a that is relatively prime to prime p, the solution for the linear congruence $ax \equiv b \pmod{p}$ is $x \equiv a^{p-2}b \pmod{p}$

Def. *Euler Phi-function*

Def. *Reduced Residue System Modulo n*

Thm 6.13. Consider a vector $\vec{\mathbf{v}}_1$ whose entries are a reduced residues system modulo m. Some $\vec{\mathbf{v}}_2$ defined as $a\vec{\mathbf{v}}_1$ also have entries that consist a complete systems of residues, given that $(a, m) = 1$.

Thm 6.14. *Euler's Theorem*

Chapter 7 *Multiplicative Function*

This chapter deals with the (7.1) Euler phi-function, the (7.2) sum and number of divisors, (7.3) perfect numbers and Mersenne primes.

Def. *Arithmetic Function*

Def. *Multiplicative Function*

Def. *Divisor Summatory Function*

Thm 7.7

$$\sum_{d|n} \phi(d) = n$$

Def. *Sum of Divisors Function*

Def. *Number of Divisors Function*

Thm 7.8. The summatory function of a multiplicative function is also multiplicative.

Cor 7.8.1. The sum of divisors function and the number of divisors function are multiplicative functions.

Lem 7.1. There exists formulas for $\sigma(p^n)$ and $\tau(p^n)$ in terms of positive integer n and prime p.

Thm 7.9.

$$\sigma(n) = \prod_{j=1}^{s} \frac{p_j^{a_j+1} - 1}{p - 1} \qquad \text{and} \qquad \tau(n) = \prod_{j=1}^{s} (a_j + 1)$$

Def. *Perfect Number*

Thm 7.10. A positive number n is a perfect number if and only if $n = 2^{m-1}(2^m - 1)$ where m is a positive integer greater than 1 and $2^m - 1$ is prime.

Thm 7.11. If m is a positive integer and $2^m - 1$ is prime, then m must be prime.

Def. *Mersenne Numbers*

Thm 7.12. For an odd prime p, the pth Mersenne number only has positive divisors in the form of $2kp + 1$ where k is a positive integer.

Chapter 9 *Primitive Roots*

This chapter deals with the (9.1) order of an integer and primitive roots, (9.2) primitive roots for primes, the (9.3) existence of primitive roots, and (9.4) discrete logarithms and index arithmetic.

Def. *Order of a Modulo n* (necessary that $(a, n) = 1$)

Thm 9.1. For a nonzero integer a and a positive integer n with $(a, n) = 1$, x is a solution of $a^x \equiv 1 \pmod{n}$ if and only if the order of a modulo n divides x.

Cor 9.1.1. For a nonzero integer a and a positive integer n with $(a, n) = 1$, $\phi(n)$ is always a solution of the congruence above, and the order of a modulo n divides $\phi(n)$.

Thm 9.2. Given $(a, n) = 1$, two different exponentials of a in modulo n are congruent if and only if the powers are congruent modulo $\text{ord}_n a$.

Def. *Primitive Root Modulo n*

Thm 9.3. The first $\phi(n)$ powers of a primitive root modulo m form a reduced residue system modulo m.

Thm 9.4. $\text{ord}_n(a^u) = t/(t, u)$

Cor 9.4.1. A power of a primitive root is a primitive root if and only if the power and $\phi(n)$ is relatively prime.

Thm 9.5. For modulus n, there are $\phi(\phi(n))$ incongruent primitive roots.

Thm 9.6. *Lagrange's Theorem* A n-degree polynomial ring over the field $\mathbb{Z}/p\mathbb{Z}$ (expressible as $\mathbb{Z}_p[x]$) where p is prime has at most n incongruent solutions.

Thm 9.7. Let d be a divisor of $p - 1$ where p is prime. $x^d - 1$ has exactly d incongruent solutions modulo p.

Thm 9.8. We can find the number of positive integers less than p that has a certain integer (albeit there's a condition that this integer has to divide $p - 1$) as its order. The number of integers less than p that have d as its order is exactly $\phi(d)$.

Lem 9.1. The number of integers less than p that have $d \mid p - 1$ as its order does not exceed $\phi(d)$.

Cor 9.8.1. Every prime has a primitive root.

Def. *Index, Discrete Logarithm of a base r modulo m*

Thm 9.16. (a) $\text{ind}_r 1 \equiv 0 \pmod{\phi(m)}$

(b) $\text{ind}_r ab \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$

(c) $\text{ind}_r a^k \equiv k \,\text{ind}_r a \pmod{\phi(m)}$

Chapter 11 *Quadratic Residues*

This chapter deals with (11.1) quadratic residues and nonresidues, the (11.2) law of quadratic reciprocity, and the (11.3) Jacobi symbol.

Def. *Quadratic Residue*

Thm 11.1. There are $(p-1)/2$ quadratic residues of p bigger than 0 and smaller than p.

Lem 11.1. Let p be an odd prime and a be an integer such that $(a,p)=1$. $x^2 \equiv a \pmod{m}$ has either no and 2 solutions.

Thm 11.2. Let a be an integer such that $(a,p)=1$. If a is a quadratic residue, $\text{ind}_r a$ is even and if not, $\text{ind}_r a$ is odd.

Def. *Legendre Symbol*

Thm 11.3. *Euler's Criterion*

Thm 11.4. (a) If $a \equiv b \pmod{p}$ then $(a/p) = (b/p)$

(b) $(a/p)(b/p) = (ab/p)$

(c) $\left(a^2/p\right) = 1$

Lem 11.2. *Gauss's Lemma*

Thm 11.6. Given odd prime p,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

Thm 11.7. *The Law of Quadratic Reciprocity*

Lem 11.3.

Thm 11.8. Let p and q be distinct odd primes with $(a,p)=1$ and $p \equiv \pm q \pmod{4a}$. Then,

$$\left(\frac{a}{p}\right) = \left(\frac{b}{q}\right)$$

References

[1] K.H. Rosen. *Elementary Number Theory and Its Applications.* Alternative eText Formats Series. Pearson/Addison Wesley, 2005.