Math 312 Final Study Guide

Alisa Liu

April 2018

1. The Integers

- **The Well-Ordering Principle**: Every non-empty subset $S \in \mathbb{Z}$ of the positive integers contains a least element.

2. Mathematical Induction

- Weak induction
  - Base case: Let $n = m$. Show that the theorem is true in this case.
  - Inductive hypothesis: Suppose the theorem is true for some $n \geq m$.
  - Inductive step: Show that the theorem is true for $n + 1$.
  - Therefore by mathematical induction, the theorem is true for all $\mathbb{Z}_{\geq m}$.
- Strong induction
  - Base case: Let $n = m_1, ..., m_k$. Show that the theorem is true in this case.
  - Inductive hypothesis: Let $n \geq m_k$ and suppose that the theorem is true for all integers $m_1, ..., n$.
  - Inductive step: Show that the theorem is true for $n + 1$.
  - Therefore by mathematical induction, the theorem is true for all $\mathbb{Z}_{\geq m}$.

3. Divisibility

- Let $a, b \in \mathbb{Z}$. Then a **divides** b, denoted $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = a \cdot c$.
- **Division Algorithm**: Let $n, a \in \mathbb{Z}$ with $a > 0$. Then there exists unique $q, r \in \mathbb{Z}$ such that

$$n = q \cdot a + r \quad 0 \leq r < a$$

- Theorems
  - Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.
  - Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid ma + nb$.

4. Representation of Integers

- Theorems
  - Let $b \geq 2$ be an integer. Then every positive integer n can be uniquely written in base b. More precisely,

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 + a_0 \quad \text{with} \quad a_k \neq 0, \quad 0 \leq a_i < b \text{ for } i = 0, ...k$$

    We denote n in base b by $a_k a_{k-1} ... a_1 a_0$.

5. The Greatest Common Divisor

- Let $a, b \in \mathbb{Z}$ not both 0. The **greatest common divisor** of a and b is the largest positive integer d such that $d \mid a$ and $d \mid b$. When $\gcd(a,b) = 1$, a and b are coprime.
- Theorems
  - Let $a, b \in \mathbb{Z}$ not both zero. Then $\gcd(a,b)$ is the smallest positive integral linear combination of a and b. That is, the smallest positive integer of the form
  $$ma + nb \quad \text{where} \quad m, n \in \mathbb{Z}$$
  - If $\gcd(a,b) = 1$, then $ma + nb = 1$ for some $m, n \in \mathbb{Z}$.
  - Every common divisor of a and b divides $\gcd(a,b)$.
  - Let $d = \gcd(a,b)$. Then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
- Let $a_1, ...a_n \in \mathbb{Z}$ not all 0. The greatest common divisor is the largest positive integer dividing all the a_i. When $\gcd(a_1, ..., a_n) = 1$, the a_i are coprime, and if $\gcd(a_i, a_j) = 1$ for all $i \neq j$, then they are pairwise coprime.
  - Generalization from theorem above: Every common divisor of all the a_i divides $\gcd(a_1, ..., a_k)$.

6. The Euclidean Algorithm

- **The Euclidean Algorithm**: Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the Division Algorithm, there exist $q_1, r_1 \in \mathbb{Z}$ such that
  $$a = bq_1 + r_1 \quad 0 \leq r_1 < b$$
  While $r_i > 0$, continue
  $$b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$$
  $$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$$
  $$\vdots$$
  Continue until $r_n = 0$ for some n. If $n = 1$, then $\gcd(a,b) = b$. If $n > 1$, then $\gcd(a,b) = r_{n-1}$. This follows from
  $$\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) = ... = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, 0) = r_{n-1}$$
- Back substitution allows us to find $m, n \in \mathbb{Z}$ such that $\gcd(a,b) = ma + nb$.

7. Prime Numbers

- **Euclid's Theorem**: There are infinitely many prime numbers.

  Proof. Let $p_1, ..., p_k$ be any finite list of primes. Then consider
  $$Q = p_1 \cdots p_k + 1$$
  Since $Q > 1$, it has a prime divisor. However, Q is not divisible by any of the p_i, since $Q \equiv 1 \pmod{p_i}$ for any i. Thus our list of primes is incomplete.
- Theorems
  - Every integer $n > 1$ has a prime divisor.
  - **Dirichlet Density Theorem**: Let $a, b \in \mathbb{Z}$ satisfy $\gcd(a,b) = 1$. Then there are infinitely many primes of the form $a + bk$ with $k \in \mathbb{Z}$.
  - Let n be composite. Then n has a prime divisor $p \leq \sqrt{n}$. In particular, we only need to test the divisibility of n by all primes up to $\sqrt{n}$ to tell whether n is prime.

8. The Fundamental Theorem of Arithmetic

- **The Fundamental Theorem of Arithmetic**: Let $n \in \mathbb{Z}_{\geq 2}$. Then n has a prime factorization of the form
$$n = \pm p_1^{a_1} \cdots p_r^{a_r} \quad a_i \geq 1$$
where p_i are distinct primes. Up to the order of the p_i, this factorization is unique.

- Theorems
  - Let $a, b \in \mathbb{Z}_{>0}$ satisfy $\gcd(a, b) = 1$. If $a \mid bc$, then $a \mid c$.
  - Let $a_1, ...a_n, p$ be integers with p prime. If $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.
  - Let $n \in \mathbb{Z}_{\geq 2}$ have a prime factorization $n = p_1^{a_1} \cdots p_n^{a_n}$. Suppose that $d \mid n$. Then the prime factorization of d is of the form
$$d = p_1^{b_1} \cdots p_n^{b_n} \quad \text{with} \quad 0 \leq b_i \leq a_i$$

9. The Least Common Multiple

- Let $a_1, ...a_n \in \mathbb{Z}_{>0}$. The **least common multiple** of $a_1, ..., a_n$ is the smallest positive integer that is divisible by all of the a_i.

- Theorems
  - Let $a, ..., a_n \in \mathbb{Z}_{>0}$ have prime decompositions
$$a_1 = p_1^{s_{1,1}} \cdots p_k^{s_{1,k}} \quad \text{with} \quad s_{1,1}, ..., s_{1,n} \geq 0$$
$$\vdots$$
$$a_n = p_1^{s_{n,1}} \cdots p_k^{s_{n,k}} \quad \text{with} \quad s_{n,1}, ...s_{n,k} \geq 0$$
Then
$$\gcd(a_1, ..., a_n) = p_1^{\min\{s_{1,1}, ..., s_{n,1}\}} \cdots p_n^{\min\{s_{1,k}, ..., s_{n,k}\}}$$
$$\gcd(a_1, ..., a_n) = p_1^{\max\{s_{1,1}, ..., s_{n,1}\}} \cdots p_n^{\max\{s_{1,k}, ..., s_{n,k}\}}$$
For $n = 2$,
$$a_1 \cdot a_2 = \gcd(a_1, a_2) \cdot \operatorname{lcm}(a_1, a_2)$$
  - Let $a_1, ..., a_n \in \mathbb{Z}$. Then $\operatorname{lcm}(a_1, ..., a_n) = \operatorname{lcm}(a_1, \operatorname{lcm}(a_2, ..., a_n))$.
  - Every common multiple of $a_1, ..., a_n$ is a multiple of $\operatorname{lcm}(a_1, ..., a_n)$. That is, if $k \in \mathbb{Z}$ such that $a_i \mid k$ for all i, then $\operatorname{lcm}(a_1, ..., a_n) \mid k$.
  - Let $a_1, ..., a_n \in \mathbb{Z}$ be pairwise coprime. Then $\operatorname{lcm}(a_1, ...a_n) = a_1 \cdots a_n$.
  - Let a, b be pairwise coprime integers. If $d \mid ab$, then there are unique integers $d_1 \mid a$ and $d_2 \mid b$ such that $d = d_1 d_2$. Conversely, any such product is a divisor of ab.

10. Primes of the Form $4k + 3$

- **Proposition**: There are infinitely many primes of the form $4k + 3$.

Proof. Suppose any finite list of primes of the form $4k + 3$, and denote them $p_0 = 3, p_1, p_2, ..., p_n$ and consider the number
$$Q = 4p_1 \cdots p_n + 3$$
Since Q is odd, the prime factorization of Q contains only odd primes. Further, it must be of the form $4k + 1$ or $4k + 3$. However, if all the primes in its factorization is of the form $4k + 1$, then Q is also of the form $4k + 1$. Here, Q is of the form $4k + 3$, so there is at least one prime factor of Q which is of the form $4k + 3$.

Let $p \mid Q$ be of the form $4k + 3$. Notice that $p \neq p_0 = 3$, since $3 \nmid Q - 3 = 4p_1 \cdots p_n$. Also, $p \neq p_i$ for any $1 \leq i \leq n$, since $p_i \nmid Q - 4p_1 \cdots p_n = 3$. Thus p is not one of $p_0, p_1, ...p_n$, and our list of primes of the form $4k + 3$ is incomplete.

- Lemmas
  - Let n be an integer. Then n is of the form $4k, 4k+1, 4k+2$ or $4k+3$ for $k \in \mathbb{Z}$.
  - Let $a, b \in \mathbb{Z}$ of the form $4k+1$. Then ab is also of the form $4k+1$.

11. Linear Diophantine Equations

- Any equation with one or more variable to be solved in the integers is called a **Diophantine equation**. Let $a_1, ..., a_n \in \mathbb{Z}$. A linear Diophantine equation in n variables has the form

$$a_1x_1 + ... + a_nx_n = b \quad \text{with} \quad b \in \mathbb{Z}$$

- **Theorem**: Let $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$. Write $d = \gcd(a, b)$. Consider the equation

$$ax + by = c$$

  (i) If $d \nmid c$ then there are no solutions.

  (ii) Suppose $d \mid c$. Then all solutions are given by the formulas

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t \quad \text{with} \quad t \in \mathbb{Z}$$

  where (x_0, y_0) is a particular solution.

  Note. We can find the particular solution in part (ii) by applying the Euclidean Algorithm and back substitution.

12. Irrational Numbers

- A real number $x \in \mathbb{R}$ is **irrational** if $x \notin \mathbb{Q}$.
- Theorems
  - The number $\sqrt{2}$ is irrational.

    Proof. Suppose for contradiction that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ with a, b coprime positive integers.

$$\sqrt{2} = \frac{a}{b} \quad \Rightarrow \quad 2b^2 = a^2 \quad \Rightarrow \quad 2 \mid a$$

    because 2 is a prime dividing $a^2 = a \cdot a$, it divides one of the factors. Therefore, $a = 2k$ for some $k \in \mathbb{Z}$. Then

$$2b^2 = a^2 = (2k)^2 \quad \Rightarrow \quad b^2 = 2k^2 \quad \Rightarrow \quad 2 \mid b$$

    So both a, b are divisible by 2, contradicting the fact that $\gcd(a, b) = 1$.
  - Let $f(x) = x^n + c_{n-1}x^{n-1} + ... + c_1x + c_0$ be a polynomial with coefficients $c_i \in \mathbb{Z}$. Suppose that the real number α satisfies $f(\alpha) = 0$. Then α is either an integer or irrational.
  - Let $a, m \in \mathbb{Z}_{>0}$ satisfy $a \neq k^m$ for $k \in \mathbb{Z}$ so that the real number $\sqrt[m]{a}$ is not an integer. Then $\sqrt[m]{a}$ is irrational.

13. Congruences

- Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Then a is **congruent** to b modulo m iff $m \mid a - b$. We write $a \equiv b \pmod{m}$.
- The **congruence class** of a mod m is

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$$

- A set $S \subset \mathbb{Z}$ such that every integer is congruent mod m to exactly one integer in S is a **complete residue system** mod m.

- We define $\mathbb{Z}/m\mathbb{Z}$, the integers mod m, to be the set of congruence classes mod m

$$\frac{\mathbb{Z}}{m\mathbb{Z}} = \{[0], [1], ..., [m-1]\}$$

- We define the arithmetic operations in $\mathbb{Z}/m\mathbb{Z}$ as follows. Let $[r], [s] \in \mathbb{Z}$ and $\lambda \in \mathbb{Z}$.
  - Addition: $[r] + [s] = [r+s]$
  - Multiplication: $[r] \cdot [s] = [r \cdot s]$
  - Multiplication by scalar: $\lambda \cdot [r] = [\lambda \cdot r]$
- Theorems
  - Let $m \in \mathbb{Z}_{>0}$. Then the relation of congruence modulo m is an equivalence relation in $\mathbb{Z}$. More precisely, for all $a, b, c, \in \mathbb{Z}$, we have
    (i) $a \equiv a \pmod{m}$ (reflexivity)
    (ii) $a \equiv b \pmod{m} \quad \Rightarrow \quad b \equiv a \pmod{m}$ (symmetry)
    (iii) $a \equiv b, b \equiv c \pmod{m} \quad \Rightarrow \quad a \equiv c \pmod{m}$ (transitivity)
  - Let $a, m \in \mathbb{Z}$ with $m > 0$. Then $a \equiv r \pmod{m}$, where r is the remainder of the division of a by m. In particular, a is congruent to exactly one integer in $\{0, 1, 2, ..., m-1\}$.
  - Let $a, b, m \in \mathbb{Z}$ with $m > 0$. If $a \equiv b \pmod{m}$ and $0 \leq a, b \leq m-1$, then $a = b$.
  - Let $m \in \mathbb{Z}_{>0}$. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then
    (i) $a + c \equiv b + d \pmod{m}$
    (ii) $a - c \equiv b - d \pmod{m}$
    (iii) $ac \equiv bd \pmod{m}$
  - Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$ and $c \neq 0$. Write $d = \gcd(c, m)$. Then

$$c \cdot a \equiv c \cdot b \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$$

    In particular, only if $d = \gcd(c, m) = 1$, then

$$c \cdot a \equiv c \cdot b \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$$

14. Fast Modular Exponentiation

- Steps to compute $a^k \pmod{m}$
  - Step 1: Write the exponent in base 2.

$$k = 2^{s_1} + \cdots + 2^{s_n} \quad r_1 > \cdots > r_n$$

  - Step 2: Compute

$$a \pmod{m}, \quad a^2 \pmod{m}, \quad ... \quad , \quad a^{2^{s_1}} \pmod{m}$$

    by successfully squaring and reducing the result modulo m.
  - Step 3: Compute

$$a^k = a^{2^{s_1} + \cdots + 2^{s_n}} \equiv a^{2^{s_1}} \cdots a^{2^{a_n}} \pmod{m}$$

    using the values in step 2 for the right hand side.

15. The Congruence Method

- The congruence method is used to conclude that certain Diophantine equations have no solutions in $\mathbb{Z}$. If an equation is satisfied in $\mathbb{Z}$, then it must be satisfied mod m for all $m > 0$. If we can find a value of m for which it is not satisfied, then we can conclude that there are no slutions in $\mathbb{Z}$.
- Outline
  - Suppose for contradiction that there are x, y satisfying the Diophantine equation
$$ax^k + by^r = c$$
  - Since every integer is congruent to itself, for all integers $m > 0$, we have
$$ax^k + by^r \equiv c \pmod{m}$$
  - In particular, taking $m = a$, we have
$$by^r \equiv c \pmod{a}$$
  - Now, $y \equiv 0, ...,$ or $a - 1 \pmod{a}$. Then we obtain
$$b[0]^r \equiv c_0 \pmod{a}$$
$$\vdots$$
$$b[a-1]^r \equiv c_{a-1} \pmod{a}$$
    where none of $c_0, ..., c_{a-1}$ are congruent to c mod a. Thus
$$by^r \not\equiv c \pmod{a}$$
    and the integer solution x, y cannot exist, otherwise y satisfies an impossible congruence.

16. Linear Congruences in One Variable

- **Theorem**: Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Write $d = \gcd(a, m)$. Consider the equation
$$ax \equiv b \pmod{m}$$
  (i) If $d \nmid b$ then there are no solutions.
  (ii) Suppose $d \mid b$. Then there are exactly d non-congruent solutions mod m, which are given by
$$x \equiv x_0 - \frac{m}{d}t \quad \text{where} \quad 0 \le t \le d - 1$$
  and x_0 is a particular solution.

  Proof. This comes fairly directly from reading $ax \equiv b \pmod{m}$ as $ax - my = b$, which was treated in chapter 11.

- Let $a, m \in \mathbb{Z}$ with $m > 0$ and $\gcd(a, m) = 1$. Any integer solution of the congruence $ax \equiv 1 \pmod{m}$ is an **inverse** of a modulo m. The congruence class $[x_0]$ in $\mathbb{Z}/m\mathbb{Z}$ which satisfies $[a] \cdot [x_0] = [1]$ is called the inverse of $[a]$ in $\mathbb{Z}/m\mathbb{Z}$. We write $a^{-1} \pmod{m}$ to denote the smallest positive representative of the congruence class $[a]^{-1}$.
- To compute $a^{-1} \pmod{m}$, we can try the numbers $1, ..., m - 1$ or solve the linear Diophantine equation $ax + my = 1$ using the Euclidean Algorithm and back substitution.
- Propositions
  - The congruence equation $ax \equiv 1 \pmod{m}$ has exactly one solution mod m iff $\gcd(a, m) = 1$.
  - Let $k \in \mathbb{Z}_{>0}$. Then $(a^k)^{-1} \equiv (a^{-1})^k \pmod{m}$.

17. The Chinese Remainder Theorem

- **Chinese Remainder Theorem**: Let $n_1, ..., n_k \in \mathbb{Z}_{>0}$ be pairwise coprime and $b_1, ..., b_k \in \mathbb{Z}$. Consider the system of congruences
$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ \vdots \\ x \equiv b_k \pmod{n_k} \end{cases}$$
Write $m = n_1 \cdots n_k$. Then there is a unique solution mod m. Define $m_i = \frac{m}{n_i}$. Then the solution is given by
$$x = b_1 m_1 y_1 + ... + b_k m_k y_k \pmod{m}$$
where y_i is chosen so that $m_i y_1 \equiv 1 \pmod{n_i}$. This y_i exists because $\gcd(m_i, n_i) = 1$.

- Propositions
  - Let $a, b, m, n \in \mathbb{Z}$ with $m, n > 0$ and $n \mid m$. If $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.
  - If $b_1 = ... = b_k = 1$, then $x \equiv 1 \pmod{m}$. If $b_1 = ... = b_k = -1$, then $x \equiv -1 \pmod{m}$.

- Problem (computing inverses): Say we want to find $a^{-1} \pmod{m}$, which means solving $ax \equiv 1 \pmod{m}$. If m is composite such that $m = n_1 \cdots n_k$ with $\gcd(n_1, ..., n_k) = 1$, then any solution to this congruence will also satisfy
$$\begin{cases} ax \equiv 1 \pmod{n_1} \\ \vdots \\ ax \equiv 1 \pmod{n_k} \end{cases}$$
We compute $a^{-1} \pmod{n_i}$ more easily by reducing each equation mod n_i.
$$\begin{cases} x \equiv a^{-1} \pmod{n_1} \\ \vdots \\ x \equiv a^{-1} \pmod{n_k} \end{cases}$$
Now solve using CRT.

- Problem (fast modular exponentiation): Apply the same method to find $a^k \pmod{m}$, with $m = n_1 \cdots n_k$ and $\gcd(n_1, ..., n_k) = 1$.

18. Applications of Congruences

- Divisibility test theorems
  - Let $n \in \mathbb{Z}_{>0}$. Then n is divisible by 3 or 9 iff the sum of its digits is divisible by 3 or 9, respectively.

    Proof. Let $q = 3$ or $q = 9$. We have
$$10 \equiv 1 \pmod{q} \quad \Rightarrow \quad 10^k \equiv 1 \pmod{q} \quad \text{for all } k > 0$$
$$\begin{aligned} n &= a_k 10^k + \cdots + a_1 10 + a_0 \quad a_k \neq 0 \\ &\equiv a_k + \cdots + a_1 + a_0 \pmod{q} \end{aligned}$$
$$q \mid n \quad \Leftrightarrow \quad n \equiv 0 \pmod{q} \quad \Leftrightarrow \quad a_k + \cdots + a_1 + a_0 \equiv 0 \pmod{q} \quad \Leftrightarrow \quad q \mid a_k + \cdots + a_1 + a_0$$
  - n is divisible by 11 iff the alternating sum of its digits is divisible by 11.

    Proof.
$$10 \equiv -1 \pmod{11} \quad \Rightarrow \quad 10^k \equiv (-1)^k \pmod{11} \quad \text{for all } k > 0$$
$$\begin{aligned} n &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \quad a_k \neq 0 \\ &\equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_2 - a_1 + a_0 \pmod{11} \end{aligned}$$
$$\begin{aligned} 11 \mid n \quad \Leftrightarrow \quad n \equiv 0 \pmod{11} \quad &\Leftrightarrow \quad a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_2 - a_1 + a_0 \equiv 0 \pmod{11} \\ &\Leftrightarrow \quad 11 \mid a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_2 - a_1 + a_0 \end{aligned}$$

- n is divisible by 2^m iff the integer obtained from the last m digits of n is divisible by 2^m.

  Proof.
  $$10 \equiv 0 \pmod 2 \quad \Rightarrow \quad 10^m \equiv 0 \pmod{2^m}$$
  $$n = a_k 10^k + \cdots + a_1 10 + a_0 \equiv a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 \pmod{2^m}$$
  The number on the right hand side is just the integer obtained from the last m digits of n.

- The ISBN10 Code
  - An ISBN10 code has 10 digits $a_1, ..., a_{10}$ such that $0 \leq a_i \leq 9$ for $i = 1, ..., 9$, and a_{10} is an integer mod 11, where X denotes 10
  - An ISBN10 code is valid if
  $$S = \sum_{i=1}^{10} i \cdot a_i \equiv 0 \pmod{11}$$
  - Let $a_1, ..., a_9$ be integers such that $0 \leq a_i \leq 9$ for $i = 1, ..., 9$. Take
  $$a_{10} = \sum_{i=1}^{9} i \cdot a_i \equiv 0 \pmod{11}$$
  Then $a_1 \cdots a_{10}$ is a valid ISBN10 code. That is, we can form an ISBN10 code by choosing 9 digits arbitrarily and calculating the last digit.
  - The ISBN10 code detects both single errors and transposition errors.

19. Wilson's Theorem

- **Wilson's Theorem**: Let p be a prime. Then $(p-1)! \equiv -1 \pmod p$.
- Propositions
  - Let $a, p \in \mathbb{Z}$ with p a prime and a invertable mod p. That is, $p \nmid a$. Then $a^2 \equiv 1 \pmod p$ iff $a \equiv \pm 1 \pmod p$.

20. Fermat's Little Theorem

- **Fermat's Little Theorem**: Let p be a prime. If $a \in \mathbb{Z}$ satisfies $\gcd(a, p) = 1$, then
$$a^{p-1} \equiv 1 \pmod p$$

Proof. Let $a \in \mathbb{Z}$ be coprime to p and consider the sequence of integers
$$a, 2a, 3a, ..., (p-1)a$$
These are all distinct mod p and not congruent to zero mod p (proof omitted), so they form $p-1$ distinct integers in the interval $[1, p-1]$. On one hand,
$$a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv (p-1)! \pmod p$$
On the other hand,
$$a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv a^{p-1}(p-1)! \pmod p$$
Together,
$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p$$
By Wilson's theorem, we conclude that
$$a^{p-1}(-1) \equiv (-1) \pmod p \quad \Leftrightarrow \quad a^{p-1} \equiv 1 \pmod p$$

- Propositions
  - Let p be prime, $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$.
  - Let p be prime and $a \in \mathbb{Z}$ coprime to p. Suppose $d \equiv e \pmod{p-1}$ Then $a^d \equiv a^e \pmod{p}$.
- Problem (fast modular exponentiation): Solve $a^k \pmod{p}$.

  Method 1: $k \equiv k_0 \pmod{p-1} \quad \Rightarrow \quad a^k \equiv a^{k_0} \pmod{p}$

  Method 2: $k = (p-1)q + r \quad \Rightarrow \quad a^k \equiv \left(a^{p-1}\right)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{p}$

21. Primality Testing, Pseudoprimes, and Charmichael Numbers

- Primality testing
  - Converse of Wilson's Theorem: n is prime iff $(n-1)! \equiv -1 \pmod{n}$.
  - Fermat's Test (contrapositive of FLT): Let $n, b \in \mathbb{Z}_{>1}$ with $1 < b < n$. If $b^{n-1} \not\equiv 1 \pmod{n}$, then n is composite. (If $b^{n-1} \equiv 1 \pmod{n}$, then n is prime OR n is a pseudoprime to the base b.)
- If $n \in \mathbb{Z}_{>1}$ is composite and satisfies $b^{n-1} \equiv 1 \pmod{n}$ for some $1 < b < n$, then n is a **pseudoprime** to the base b. If this is true for every $b \geq 2$ where $\gcd(n, b) = 1$, then n is a Charmichael number.
- **Korset's Theorem**: A composite positive integer n is a Charmichael number iff
  (i) n is square free
  (ii) If $p \mid n$, then $p - 1 \mid n - 1$

22. Euler's φ-function and Euler's Theorem

- The Euler φ-function is the function $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ defined by

  $$\varphi(n) = \#\{x \in \mathbb{Z} : 1 \leq x \leq n \text{ and } \gcd(x, n) = 1\}$$

  It counts the number of positive integers up to n that are coprime to n.
- **Euler's Theorem**: Let $a, m \in \mathbb{Z}$ with $m > 0$ and $\gcd(a, m) = 1$. Then

  $$a^{\varphi(m)} \equiv 1 \pmod{m}$$

  Since $\varphi(p) = p - 1$ for any prime p, we can recover FLT directly.
- A set of integers with $\varphi(m)$ elements, no two of which are congruent mod m, and all of which are coprime to m, is a **reduced residue system** mod m.
- Problem (fast modular exponentiation): Solve $a^k \pmod{m}$

  $$k = \varphi(m) \cdot q + r$$

  $$a^k \equiv a^{\varphi(m) \cdot q + r} \equiv \left(a^{\varphi(m)}\right)^q \cdot a^r \equiv 1 \cdot a^r \equiv a^r \pmod{m}$$

23. Arithmetic Functions

- A function whose domain is $\mathbb{Z}_{>0}$ is an **arithmetic function**.
- Let f be an arithmetic function. Then f is **multiplicative** if, for all $n_1, n_2 \in \mathbb{Z}_{>0}$ satisfying $\gcd(n_1, n_2) = 1$, we have

  $$f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2)$$

  And f is **completely multiplicative** if this is true for all n_1, n_2.

- Define

$$\varphi(n) = \#\text{ of coprime numbers } \leq n$$
$$\tau(n) = \sum_{\substack{d|n \\ d>0}} 1 = \#\text{ positive divisors of } n$$
$$\sigma(n) = \sum_{\substack{d|n \\ d>0}} d = \text{sum of positive divisors of } n$$

- **Theorem**: Let f be an arithmetic function and define the arithmetic function F by

$$F(n) = \sum_{\substack{d|n \\ d>0}} f(d) \quad \forall n \in \mathbb{Z}_{>0}$$

  If f is multiplicative, then F is multiplicative.

- Theorems
  - The function $\varphi(n)$ is multiplicative.
  - The functions $\tau(n)$ and $\sigma(n)$ are multiplicative.

    Proof. $\tau(n)$ and $\sigma(n)$ are in the form of F where we choose $f(n) = 1$ and $f(n) = n$, respectively. These two functions f are multiplicative.

24. Formulas for the Functions φ, τ, σ

- For a multiplicative function f and $n = p_1^{a_1} \cdots p_k^{a_k}$

$$f(n) = f(p_1^{a_1}) \cdots f(p_k^{a_k})$$

  So f is completely determined by its values at prime powers. Similarly, a completely multiplicative function f is completely determined by its values at primes.

- Theorems
  - Let $n \in \mathbb{Z}_{>1}$ have factorization $n = p_1^{a_1} \cdots p_k^{a_k}$. Then

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$$
$$\varphi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1)$$
$$\tau(p^a) = a + 1$$
$$\tau(n) = \prod_{i=1}^{k} (a_i + 1)$$
$$\sigma(p^a) = 1 + p + \cdots + p^a = \frac{1 - p^{a+1}}{1 - p}$$
$$\sigma(n) = \prod_{i=1}^{k} \frac{1 - p_i^{a_i+1}}{1 - p_i}$$

  - n prime $\quad \Leftrightarrow \quad \varphi(n) = p - 1 \quad \Leftrightarrow \quad \tau(n) = 2 \quad \Leftrightarrow \quad \sigma(n) = n + 1$
  - Let $n \in \mathbb{Z}_{>0}$. Then

$$\sum_{\substack{d|n \\ d>0}} \varphi(d) = n$$

    That is, the sum of the number of divisors of each divisor of n is n.

- Problem: Find all integers $n > 0$ satisfying $\varphi(n) = m$.

  Write
  $$n = p_1^{a_1} \cdots p_k^{a_k}$$
  $$\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1) = m$$
  From the formula, we get $p_i - 1 \mid m$ for all i. Thus $p_i - 1 \in \{d : d \mid m\}$, and $p_i \in \{d + 1 : d \mid m, d + 1 \text{ prime}\}$. Now, for each p_i, we devise an upper bound on a_i satisfying $p_i^{a_i - 1} \mid m$. Finally, we try all combinations of the valid a_i to see which give $\varphi(n) = m$.

25. Perfect Numbers and Mersenne Primes

- An integer $n > 0$ is perfect if $\sigma(n) = 2n$.
- Let $n > 1$ be an integer. Then $M_n = 2^n - 1$ is the n-th **Mersenne number**. If M_n is prime, we call it a **Mersenne prime**.
- Theorems
  - Let $n \in \mathbb{Z}_{>0}$. Then n is an even perfect number iff
    $$n = 2^{m-1}(2^m - 1) \quad \text{with } 2^m - 1 \text{ a Mersenne prime}$$
  - If M_n is prime, then n is prime.

26. Primitive Roots

- From Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod m$ for any a such that $\gcd(a, m) = 1$. Given m, we are interested in whether there exists an $x < \varphi(m)$ that satisfies $a^x \equiv 1 \pmod m$.
- Let $a, m \in \mathbb{Z}$ with $m > 0$ and $\gcd(a, m) = 1$. The **order** of a mod m, denoted $\text{ord}_m(a)$, is the least positive integer x such that $a^x \equiv 1 \pmod m$. That is, $a^{\text{ord}_m(a)} \equiv 1 \pmod m$ and $\text{ord}_m(a) \le \varphi(m)$.
- We say a is a **primitive root** mod m if $\text{ord}_m(a)$ is maximal. That is, $\text{ord}_m(a) = \varphi(m)$.
- Theorems
  - Let $a, m \in \mathbb{Z}$ with $m > 0$ and $\gcd(a, m) = 1$. An integer $x \in \mathbb{Z}_{>0}$ satisfies $a^x \equiv 1 \pmod m$ iff $\text{ord}_m(a) \mid x$. In particular, $\text{ord}_m(a) \mid \varphi(m)$.
  - For $i, j \in \mathbb{Z}$, we have
    $$a^i \equiv a^j \pmod m \quad \Leftrightarrow \quad i \equiv j \pmod{\text{ord}_m(a)}$$
    For $i > 0$, we have
    $$\text{ord}_m(a^i) = \frac{\text{ord}_m(a)}{\gcd(\text{ord}_m(a), i)}$$
  - Let r be a primitive root mod m and $S = \{r, r^2, ..., r^{\varphi(m)}\}$. Then S is a reduced residue system mod m.
  - Let m be an integer admitting a primitive root. Then there are $\varphi(\varphi(m))$ non-congruent primitive roots mod m.
  - Let $m \in \mathbb{Z}_{>0}$. Suppose $m = kn$ where $\gcd(k, n) = 1$ and $\varphi(k), \varphi(n)$ are even. Then for all $a \in \mathbb{Z}$ coprime to m, we have
    $$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod m$$
    In particular, m admits no primitive roots.
    * If $m > 0$ is divisible by two different odd primes, then m admits no primitive roots.
    * If $m = 2^a p^b$ with p and odd prime, $a \ge 2, b \ge 1$, then m admits no primitive roots.

– Suppose $m = 2^d$, $d \geq 3$. Then for all $a \in \mathbb{Z}$ coprime to m, we have

$$a^{2^{d-2}} \equiv 1 \pmod{m}$$

In particular, m admits no primitive roots.

– **Primitive Root Theorem**: Let $m \in \mathbb{Z}_{>0}$. Then a primitive root mod m exists iff $m = 1, 2, 4, p^a, 2p^a$, where $a \geq 1$ and p is an odd prime.

- Problem: Determine $\text{ord}_m(a)$. That is, find the smallest x such that $a^x \equiv 1 \pmod{m}$.
  - Find $\varphi(m)$. We know $\text{ord}_m(a) \mid \varphi(m)$ for any a. That is, $\text{ord}_m(a) \in \{\text{factors of } \varphi(m)\}$.
  - For every element $x \in \{\text{factors of } \varphi(m)\}$, compute $a^x \pmod{m}$. If $a^x \equiv 1 \pmod{m}$, then $x = \text{ord}_m(a)$.
- Problem: Find a primitive root mod m. That is, find a number r such that $\text{ord}_m(r) = \varphi(m)$.
  - For every a coprime to m (excluding 1), find $\text{ord}_m a$ using the method above. If $\text{ord}_m a = \phi(a)$, then a is a primitive root.
- Problem: Find all primitive roots mod m.
  - Check if m admits any primitive roots using the primitive root theorem.
  - Use the method above to find one primitive root mod m. Call it r.
  - We know $\{r, r^2, ..., r^{\varphi(m)}\}$ is a reduced residue system mod m, so all primitive roots mod m are congruent to r^i for some $1 \leq i \leq \varphi(m)$. Any such i must fulfill $\gcd(\varphi(m), i) = 1$. Calculate such i. The primitive roots are all the r^i.

27. Primitive Roots for Primes

- Let p be a prime. Then there exists a primitive root mod p.
- Consider a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with integer coeffients. We call n the **degree** of f and we say that f is **monic** if $a_n - 1$. An integer c satisfying $f(c) \equiv 0 \pmod{m}$ is a root of f mod m.
- Theorems
  - **Lagrange's Theorem**: Let f be a monic polynomial of degree n with integer coefficients. Then f has at most n roots mod p.
  - Let p be a prime. From before, $\text{ord}_p(a) \in \{\text{factors of } p-1\}$ for any integer a, $1 \leq a \leq p-1$. For each element d in the set, there are $\varphi(d)$ integers a such that $\text{ord}_p(a) = d$. (Every element d is chosen $\varphi(d)$ times.) In particular, there are $\varphi(p-1)$ primitive roots mod p.

28. Index Arithmetic and Discrete Logarithms

- Let r be a primitive root mod m. Recall that the set $\{r, r^2, ..., r^{\varphi(m)}\}$ is a reduced residue system mod m. In particular, for all $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$, we have $r^i \equiv a \pmod{m}$ for some i in the range $1 \leq i \leq \varphi(m)$. The smallest such i is the **index** of a relative to r and is denoted $\text{ind}_r(a)$.
- We know that $r = 3$ is a primitive root mod $n = 7$. Computing the first two rows of the table allow us to determine all indices relative to 3 mod 7.

h	1	2	3	4	5	6
$3^i \pmod 7$	3	2	6	4	5	1
a	1	2	3	4	5	6
$\text{ind}_3(a)$	6	2	1	4	5	3

- Theorems
  - Let r be a primitive root mod m. Let $a, b \in \mathbb{Z}$ be coprime to m and $d \geq 1$.

(i) $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$
(ii) $\text{ind}_r(r) \equiv 1 \pmod{\varphi(m)}$
(iii) $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)}$
(iv) $\text{ind}_r(a^d) \equiv d \cdot \text{ind}_r(a) \pmod{\varphi(m)}$

It is common to refer to indices as discrete logs since they share similar properties.

– Let m be an integer admitting a primitive root. Let $a, k \in \mathbb{Z}$ with $\gcd(a, m) = 1$ and $k \geq 1$. Consider the congruence equation
$$x^k \equiv a \pmod{m}$$
Write $d = \gcd(k, \varphi(m))$. Then

(i) If $a^{\frac{\varphi(m)}{d}} \not\equiv 1 \pmod{m}$, then the equation has no solutions.
(ii) If $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$, then the equation has exactly d non-congruent solutions mod m.

- Problem: Let $a, b, d \in \mathbb{Z}$ with $d \geq 1$, and let r be a primitive root mod m. Then consider the congruence equation
$$ax^d \equiv b \pmod{m}$$
It follows
$$r^{\text{ind}_r(ax^d)} \equiv r^{\text{ind}_r(b)} \pmod{m}$$
$$\text{ind}_r(a) + d \cdot \text{ind}_r(x) \equiv \text{ind}_r(b) \pmod{\varphi(m)}$$
$$d \cdot \text{ind}_r(x) \equiv \text{ind}_r(b) - \text{ind}_r(a) \pmod{\varphi(m)}$$
This is a linear congruence in one variable which we know how to solve from Chapter 16. After finding $\text{ind}_r(x) \pmod{\varphi(m)}$, we can easily determine $x \pmod{m}$.

- Problem: Consider the congruence equation
$$a^x \equiv b \pmod{m}$$
It follows that
$$x \cdot \text{ind}_r(a) \equiv \text{ind}_r(b) \pmod{\varphi(m)}$$
In this case, the original congruence is mod m but the final description of integer solutions is mod $\varphi(m)$.

34. Cryprography

- **Cryptography** is the design and implementation of secure systems. **Symmetric cryptosystems** have a key that must be kept secret for decryption. **Asymmetric cryptosystems** have one key that is publicly available and used for encryption, and another that is private and used for decryption.

- A cryptosystem is made up of

$\mathscr{P}$: the set of all plaintext messages
$\mathscr{C}$: the set of all ciphertext messages
K: the set of all keys

The correspondence $k \mapsto (E_k, D_k)$ for some $k \in K$ where
$$E_k : \mathscr{P} \mapsto \mathscr{C} \quad \text{the encryption function}$$
$$D_k : \mathscr{C} \mapsto \mathscr{P} \quad \text{the decryption function}$$
These functions satisfy $D_k(E_k(x)) = x$ for all $x \in \mathscr{P}$.

- **The Shift Cipher**.
  - Here, $\mathscr{P} = \mathscr{C} = K = \mathbb{Z}/26\mathbb{Z}$. Let $b \in K$ so that $b \in \{0, 1, ..., 25\}$. The shift cipher is described via the correspondence
  $$b \mapsto E_b(x) = x + b \pmod{26}, \quad D_b(x) = x - b \pmod{26}$$
  where the key b is fixed and secret.
  - To break the cipher, we compute the frequencies of the letters in the ciphertext and compare them with the frequencies obtained from English. We would choose b such that E is mapped to the most common letter in the message.
- **The Affine Cipher.**
  - Let a and m be coprime. The encryption key is (a, b).
  $$E_{a,b}(x) = ax + b \pmod{m}$$
  $$D_{a,b}(x) = cy + d$$
  where $c \equiv a^{-1} \pmod{m}$ and $d \equiv -a^{-1}b \pmod{m}$. Note a^{-1} exists because $\gcd(a, m) = 1$. When $a = 1$, we recover the shift cipher.
  - These ciphers can also be broken by frequency analysis, but we now need 2 bits of information. Let k_1 and k_2 be the most common letters in the ciphertext. Then $D_{a,b} = cx + b$ should satisfy
  $$\begin{cases} D_{a,b}(k_1) \equiv 4 \\ D_{a,b}(k_2) \equiv 19 \end{cases} \quad \Leftrightarrow \quad \begin{cases} k_1 c + d \equiv 4 \pmod{26} \\ k_2 c + d \equiv 19 \pmod{26} \end{cases}$$
  And we can solve for c and d.
- **The Exponential Cipher.**
  - Let p be a prime. The encryption key is (p, e) with $e \in \mathbb{Z}$ such that $\gcd(e, p - 1) = 1$.
  $$E_{p,e}(x) = x^e \pmod{p}$$
  $$D_{p,e}(x) = x^d \pmod{p}$$
  where $d \equiv e^{-1} \pmod{p - 1}$.
  - We group the resulting numbers into blocks of $2m$ digits, where $2m$ is the largest positive integer such that all blocks $< p$. This way, the numerical value of each block does not get reduced mod p. So if $25 < p \leq 2525$, choose blocks of $2m = 2$ digits. If $2525 < p \leq 252525$, choose blocks of $2m = 4$ digits. Use 25 to fill the last block so that every block has $2m$ digits.
  - Even if we know p and that the plaintext x corresponds to ciphertext y, we must solve for d in the equation
  $$y^d \equiv x \pmod{p}$$
  to obtain the decryption key d. There is no efficient algorithm to do this. The simplest approach is to raise y to larger and larger powers k until $y^k \equiv x \pmod{p}$.
- **The RSA Cryptosystem.**
  - Let p and q be two large primes, and let $m = pq$ so that $\varphi(m) = (p - 1)(q - 1)$. Choose an exponent e such that
  $$1 < e < \varphi(m) \quad \text{and} \quad \gcd(e, \varphi(m)) = 1$$
  The public encryption key is (m, e) and the private decryption key is (m, d)
  $$E_{m,e}(x) = x^e \pmod{m}$$
  $$D_{m,e}(x) = x^d \pmod{m}$$
  where $d \equiv e^{-1} \pmod{\varphi(m)}$.

- **Theorem:** $D_{m,e}(E_{m,e}(x)) \equiv x \pmod m$

  Proof. We need to show that $D_{m,e}(E_{m,e}(x)) = x^{ed} \equiv x \pmod m$. By the CRT, it is enough to show that

  $$x^{ed} \equiv x \pmod p, \quad \text{and} \quad x^{ed} \equiv x \pmod q$$

  If $x \equiv 0 \pmod p$, then $x^{ed} \equiv 0 \equiv x \pmod p$. Suppose $x \not\equiv 0 \pmod p$. By construction $d \equiv e^{-1} \pmod{\varphi(n)}$ so

  $$ed \equiv 1 \pmod{\varphi(n)} \quad \Leftrightarrow \quad ed = 1 + \varphi(n)k = 1 + (p-1)(q-1)k$$

  Hence

  $$x^{ed} \equiv x^{1+(p-1)(q-1)k} \equiv x(x^{p-1})^{(q-1)k} \equiv x \pmod p$$

  where the last equivalence follows by FLT since $\gcd(x, p) = 1$. The same argument holds for modulus q, completing the proof.

- To break the RSA we only need to value of d, which can be computed from $d \equiv e^{-1} \pmod{\varphi(m)}$. However, even though (m, e) is public, it is very hard to factor m so that we can find $\varphi(m) = (p-1)(q-1)$.