Summary of Math 312

Tom Wang

Spring, 2024

1 Induction

Some basic properties of the natural numbers:

- Mathematical induction

  Suppose $S \subseteq \mathbb{N}$ such that:

  - $1 \in S$
  - $\forall n \in \mathbb{N}, n \in S \implies n+1 \in S$

- Strong Induction

  Suppose $S \subseteq \mathbb{N}$ such that:

  - $1 \in S$
  - $\forall n \in \mathbb{N}, \forall k \in \mathbb{N}, 1 \leq k \leq n \implies k \in S \implies n+1 \in S$

- Well-Ordering Principle: Every non-empty subset of $\mathbb{N}$ has a least element.

Note that the above three are equivalent.

1.1 Examples

Let $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$, Prove that the n-th Fibonacci number $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{5}}$.

Proof. Note that α, β are the roots of $x^2 - x - 1 = 0$. Then we have $\alpha^2 = \alpha + 1, \beta^2 = \beta + 1$. We will prove the statement by **Strong** induction on n.

Base Case: $n = 1, F_1 = 1 = \frac{\alpha-\beta}{\sqrt{5}} = \frac{\alpha^1-\beta^1}{\sqrt{5}}$.

$n = 2, F_2 = 1 = \frac{\alpha^2-\beta^2}{\sqrt{5}}$.

Inductive Step: Suppose $F_k = \frac{\alpha^k-\beta^k}{\sqrt{5}}$ for all $k \leq n$. Then we have $F_{n+1} = F_n + F_{n-1} = \frac{\alpha^n-\beta^n}{\sqrt{5}} + \frac{\alpha^{n-1}-\beta^{n-1}}{\sqrt{5}} = \frac{\alpha^{n-1}(\alpha+1)-\beta^{n-1}(\beta+1)}{\sqrt{5}} = \frac{\alpha^{n+1}-\beta^{n+1}}{\sqrt{5}}$.

Used the properties of α, β in the last step. □

Another example:

Prove that all positive integers are a product of primes. Here we treat the empty product as 1 and the product of one prime as itself.

Proof. We use proof by contradiction to show the use of the well-ordering principle.

Let S be the set of positive integers which cannot be written as products of primes. **Assume** that S is not empty:

Then by the well-ordering principle, S has a least element n. Since n is the least element, it cannot be prime.

Then $n = ab$ for some $a, b \in \mathbb{N}$. Then $a, b < n$. Since n is the least element, $a, b \notin S$. Then a, b can be written as products of primes. Then $n = ab$ can be written as a product of primes. This is a contradiction.

Therefore, S is empty and all positive integers can be written as products of primes. □

1.2 The division algorithm

Let $a \in \mathbb{Z}, a \geq 1$. $\forall n \in \mathbb{Z}, \exists q, r \in \mathbb{Z}$ such that $n = aq + r$ and $0 \leq r < a$. Moreover, q, r are unique.

Proof. Prove using the well-ordering principle.

Let $S = \{s \in \mathbb{Z} | s \geq 0 \wedge s = n - aq \wedge a, q, n \in \mathbb{Z}\}$. We claim that S is not empty.

Indeed $n - aq \geq 0 \iff n \geq aq \iff q \leq \frac{n}{a}$, given $a > 0$. So there are infinitely many q that satisfy the condition, which proves that S is not empty.

By the well-ordering principle, S has a least element r. Then $r = n - aq$ for some q. Then $n = aq + r$. It remains to show that $0 \leq r < a$. We argue by contradiction.

If $r \geq a$, then $r - a \geq 0$. Then $r - a = n - aq - a = n - a(q+1) \in S$. But $r - a < r$, which contradicts the fact that r is the least element of S. Therefore, $r < a$.

To show uniqueness, suppose $n = aq + r = aq' + r'$, where $0 \leq r, r' < a$. Our goal is to show that $q = q'$ and $r = r'$.

Subtracting the two equations, we have $a(q - q') = r' - r$. Notice that the LHS is divisible by a and the RHS is less than a but greater than 0. Therefore, $r' - r = 0$ and $q - q' = 0$. Therefore, $q = q'$ and $r = r'$.

This completes the proof. □

Remark: q stands for **quotient** and r stands for **remainder**.

Also, the Division algorithm is a **theorem**. The actual algorithm to find q and r is called **long division**.

2 Primes

Definition 1. *A positive integer p is called **prime** if $p \geq 2$ and the only positive divisors of p are 1 and p.*

2.1 Euclid's Theorem

Theorem 1. *There are infinitely many primes.*

Proof. Suppose there are only finitely many primes $p_1, p_2, \ldots, p_n$.

Let $N = p_1 p_2 \ldots p_n + 1$. (Products of primes plus 1)

Then N is not divisible by any of the primes $p_1, p_2, \ldots, p_n$. Therefore, N is either prime or divisible by a prime larger than p_n.

This is a contradiction. Therefore, there are infinitely many primes. □

The theorem can be used to generate infinitely many primes. For example, $2, 2 \cdot 3 + 1 = 7, 2 \cdot 3 \cdot 5 + 1 = 31, \ldots$ are all primes. However, this is not a good way to generate primes because the numbers get very large very quickly.

2.2 Sieve of Eratosthenes

Theorem 2. *Let $n \in \mathbb{N}, n \geq 2$. Then there exists a prime p such that $p \leq n$.*

The key idea is that if $n = ab$ and n is a composite, then at least one of a, b is less than or equal to $\sqrt{n}$. So we only need to check up to $\sqrt{n}$ to see if n is a prime.

For example, to check the primes within 25, we only need to check up to $\sqrt{25} = 5$. List out all the numbers from 2 to 25. Then cross out all the multiples of 2, 3, 5. The remaining numbers are all primes.

2.3 The prime number theorem

Theorem 3. *Let $\pi(x)$ be the number of primes less than or equal to x. Then $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$.*

In other words, the number of primes less than or equal to x is approximately $\frac{x}{\ln x}$.

3 Division

3.1 Greatest common divisor

Definition 2. *Let $a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$. The **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, is the largest positive integer that divides both a and b.*

Simple properties of gcd:

- $a \neq 0 \implies \gcd(a, 0) = |a|$.
- $\gcd(a, b) \geq 1$.
- $\gcd(a, b) = d \implies \gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof.

- Common divisors of a and 0 are all divisors of a. The largest one is $|a|$.
- We know 1 is a common divisor of a and b. Therefore, $\gcd(a, b) \geq 1$.
- Suppose $d = gcd(a, b), e = gcd(\frac{a}{d}, \frac{b}{d})$.

  We write $\frac{a}{d} = ek, \frac{b}{d} = em$ for some $k, m \in \mathbb{Z}$. Then $a = (de)k, b = (de)m$. Now we can know that de is a common divisor of a and b. Thus $de \leq d$. Since $d \geq 1$, we have $e \leq 1$. Therefore, $e = 1$. Proof concluded.

□

3.1.1 Some Crollaries

1. An integer e is a common divisor of a and b if and only if $e|gcd(a,b)$.

   Proof. If e is a common divisor of a and b, then $e|a$ and $e|b$. Therefore, $e|gcd(a,b) = ma + nb$ (Bezout's identity which will be proven below) for some $m, n \in \mathbb{Z}$. Therefore, $e|gcd(a,b)$.

   If $e|gcd(a,b)$, then $gcd(a,b) = ek$ for some $k \in \mathbb{Z}$. Then $gcd(a,b) = ek = ma + nb$. Therefore, $e|a$ and $e|b$. Therefore, e is a common divisor of a and b. □

2. Let c be an integer, then $ax + by = c$ has an integer solution if and only if $gcd(a,b)|c$.

   Proof.

   If $ax + by = c$ has an integer solution, then $gcd(a,b)|ax + by = c$.

   If $gcd(a,b)|c$, then $c = k(gcd(a,b)) = k(ax + by) = (ka)x + (kb)y$. Therefore, $ax + by = c$ has an integer solution. □

3.2 Bezout's identity

An integer linear combination of a and b is an integer of the form $ax + by$, where $x, y \in \mathbb{Z}$.

Theorem 4. *gcd(a, b) is the smallest positive integer that can be written as an integer linear combination of a and b.*

Proof. Let S be the set of positive integers that can be written as an integer linear combination of a and b. We want to show that $gcd(a,b)$ is the smallest element of S.

Note that since $(a,b) \neq (0,0)$, S is not empty. By the well-ordering principle, S has a least element d. We want to show that $d = gcd(a,b)$. To show it, we need to show that:

- $gcd(a,b)|d$. This tells us that $gcd(a,b) \leq d$.
- $d|a$ and $d|b$. This tells us that $d \leq gcd(a,b)$.

By definition, $d = x_0a+y_0b$ for some $x_0, y_0 \in \mathbb{Z}$ which is a linear combination of a and b. But we know that $gcd(a, b)|(ma+nb), \forall m, n \in \mathbb{Z}$. Also, $d = x_0a+y_0b$. Therefore, $gcd(a, b)|d$.

Now we want to show that $d|a$ and $d|b$. Let $a = dq + r$ where q is the quotient and r is the remainder. Just need to show that r = 0. Note that:

$$r = a - dq = a - (x_0a + y_0b)q = a(1 - x_0q) + b(-y_0q)$$

So r is a linear combination of a and b. Since r is a remainder, $0 \leq r < d$. Since d is the smallest positive integer in S, r must be 0. Therefore, $d|a$. Similarly, $d|b$. □

3.3 Euclidean Division Algorithm

The Euclidean algorithm is a highly **recursive** and fast algorithm to find the gcd of two numbers.

The complexity of the algorithm is $O(\log n)$, where n is the larger of the two numbers.

Before starting, we need to know the following lemma:

3.3.1 Lemma

Let $a, b, q, r \in \mathbb{Z}$ such that $a = bq + r$. Then $gcd(a, b) = gcd(b, r)$.

Proof. Let $d = gcd(a, b), d' = gcd(b, r)$. We want to show that $d = d'$.

We know that $d'|b$ and $d'|r$. Therefore, $d'|bq + r = a$. Therefore, $d'|a$. So $d' \leq d$, it is a common divisor of a and b.

At the same time, $d|a$ and $d|b$. Therefore, $d|bq + r = a$. Therefore, $d|a$ and $d|r$. So $d \leq d'$, it is a common divisor of b and r.

Combine two results: $d = d'$. □

3.3.2 Euclidean algorithm

The algorithm applies the lemma repeatedly until we get $r = 0$ if we have $a, b \geq 0$. Then the last non-zero remainder is the gcd of a and b.

Give a recursion code example:

```
int gcd(int a, int b) {
    if (b == 0) return a;
    if (a == 0) return b;
```

```
        if (a < b) return gcd(b % a, a);
        return gcd(b, a % b);
    }
```

So basically, we keep replacing $\gcd(a, b)$ with $\gcd(b, r)$ until $r = 0$ if we choose $a \geq b$ the whole time. Then the last non-zero remainder is the gcd of a and b.

3.3.3 Number of steps in Euclidean algorithm

Lemma:

Let $a, b \in \mathbb{Z}, a \geq b \geq 1$. We let $a = bq + r$ where $0 \leq r < b$. Then $r < \frac{a}{2}$.

Proof.

- Case 1: $b \leq \frac{a}{2}$. Then $r < b \leq \frac{a}{2}$.
- Case 2: $b > \frac{a}{2}$. Then $r = a - bq < a - \frac{a}{2}q = \frac{a}{2}(2 - q) \leq \frac{a}{2}$. Given $q \geq 1$ since $a \geq b \leq 0 \wedge r \geq 0$.

□

Corollary:

Assume $a \geq b \geq 1$. Then the number of steps in the Euclidean algorithm is at most $2 \log_2 a$.

Proof. By the lemma above, we know that for each iteration, $r < \frac{a}{2}$. Therefore, after k iterations, $r < \frac{a}{2^k}$.

But r is a positive integer otherwise it terminates (The last r before becoming zero is the gcd, we have r = 0 to be the termination point in the sample code since it is easier to program).

We want to find the smallest k such that $\frac{a}{2^k} < 1$ (termination point). This is equivalent to $2^k > a$. Therefore, $k > \log_2 a$. Therefore, the number of iterations is at most $\log_2 a$. □

3.3.4 Lame's theorem

Theorem 5. *Suppose $a, b \in \mathbb{Z}, a \geq b \geq 1$. Let d be the number of steps in the Euclidean algorithm. Then $d \leq 5 \log_{10} a$.*

The proof can be found on Wikipedia. The $\log_{10}$ is used because the proof involved Fibonacci numbers for some reason.

Now compare the bound by Lame's theorem and the bound by the corollary above. We can compare the two bounds:

$$2\log_2 a = \frac{2}{\log_{10} 2}\log_{10} a \approx 6.64\log_{10} a > 5\log_{10} a$$

So Lame's theorem is a better bound than the corollary above.

3.4 Linear equations

Solve linear equations in the form of $ax+by = c$ where $a, b, c \in \mathbb{Z}$, $(a, b) = (0, 0)$. And we are interested in the integer solutions of x, y. Note that real solutions are easy to find and there are infinitely many of them.

Bezout's identity proved that an integer solution exists if and only if $\gcd(a, b)|c$. $\gcd(a, b)$ is the smallest positive integer that can be written as an integer linear combination of a and b. So all linear combinations of a and b are multiples of $\gcd(a, b)$.

Now we want to find all the integer solutions.

- Describe the set of all integer solutions.
- Develop an algorithm to find all the integer solutions if exist

Let $d = \gcd(a, b)$.

1. if $c = d$, by Bezout's theorem, there exists $ax + by = d$ for some $x, y \in \mathbb{Z}$. To find them, use the Euclidean algorithm. Set $r_0 = a, r_1 = b$ assuming $a \geq b \geq 0$. Then $r_0 = r_1q_1 + r_2$. Then $r_1 = r_2q_2 + r_3$. Keep going until $r_{n-1} = r_nq_n + 0$. Then $r_n = d$. Then we can find x, y by back substitution.

   Back substitution:

   - start from $d = r_{n+1} = r_{n-1} - r_nq_n = r_{n-1} - q_n(r_{n-2} - r_{n-1}q_{n-1})$ So moving from a linear combination of r_{n-1} and r_n to a linear combination of r_{n-2} and r_{n-1}.
   - continues until we get a linear combination of $r_0 = a$ and $r_1 = b$.

   For example: find an integer solution for $154x + 35y = 7$.

$$\begin{aligned} 154 &= 35 \cdot 4 + 14 \\ 35 &= 14 \cdot 2 + 7 \\ 14 &= 7 \cdot 2 + 0 \end{aligned}$$

So $\gcd(154, 35) = 7$. Then we can find x, y by back substitution.

$$\begin{aligned} 7 &= 35 - 14 \cdot 2 \\ &= 35 - (154 - 35 \cdot 4) \cdot 2 \\ &= 35 \cdot 9 - 154 \cdot 2 \end{aligned}$$

So $x = -2, y = 9$ is a solution.

Another example: $553x + 327y = 1$.

$$\begin{aligned} 553 &= 327 \cdot 1 + 226 \\ 327 &= 226 \cdot 1 + 101 \\ 226 &= 101 \cdot 2 + 24 \\ 101 &= 24 \cdot 4 + 5 \\ 24 &= 5 \cdot 4 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

So $\gcd(553, 327) = 1$. Then we can find x, y by back substitution.

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (24 - 5 \cdot 4) = 5 \cdot 5 - 24 \cdot 1 \\ &= (101 - 24 \cdot 4) \cdot 5 - 24 \cdot 1 = 101 \cdot 5 - 24 \cdot 21 \\ &= 101 \cdot 5 - (226 - 101 \cdot 2) \cdot 21 = 101 \cdot 47 - 226 \cdot 21 \\ &= (327 - 226) \cdot 47 - 226 \cdot 21 = 327 \cdot 47 - 226 \cdot 68 \\ &= 327 \cdot 47 - (553 - 327 \cdot 1) \cdot 68 = 327 \cdot 115 - 553 \cdot 68 \end{aligned}$$

Now we can find $x = -68, y = 115$.

2. Back to $ax + by = c$. Now assume that $d = \gcd(a, b)|c$. So $c = td$, for some $t \in \mathbb{Z}$
   - In this case, find a solution (x_0, y_0) for $ax + by = d$.
   - Then $x = x_0 t, y = y_0 t$ is a solution for $ax + by = c$.
   - This is because $a(x_0 t) + b(y_0 t) = td = c$.

3. If $d \nmid c$, then there are no integer solutions.

   For example, $154x + 35y = 24$ has no integer solutions. This is because 24 is not a multiple of 7. t is not an integer.

4. Now we want to describe all solutions:

   Theorem 6. *Suppose* $a, b, c \in \mathbb{Z}, (a, b) \neq (0, 0)$.

   Let $d = \gcd(a, b)$. *Then the set of all integer solutions of* $ax + by = c$ *is given by*

   $$\{(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) | t \in \mathbb{Z}\}$$

   if $d|c \iff c = td$. *Otherwise, the set of all integer solutions is empty.*

   Note that (x_0, y_0) is a particular solution of $ax + by = c$. Here "general solution" means that (x, y) is a solution for every integer value of t, and every integer solution can be expressed in this form.

3.4.1 Key Lemma

Before proving the theorem, we need to prove the following lemma:

Key Lemma: Let $a, b, c \in \mathbb{Z}, (a, b) \neq (0, 0)$. Let $d = \gcd(a, b) = 1$. Then $a|bc \implies a|c$.

Note that the lemma is not true if $d \neq 1$.

Proof. By Bezout's theorem, $\gcd(a, b) = 1 \implies ax + by = 1$ for some $x, y \in \mathbb{Z}$. Then multiply both sides by c: $acx + bcy = c$. Then $a|bc \implies a|acx + bcy = c$ as defined in the Lemma. □

3.4.2 Proof of the general solution theorem

With the Lemma in hand, we can start proving the theorem:

Proof. • First need to show that $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ is a solution of $ax + by = c, \forall t \in \mathbb{Z}$.

We have $ax_0 + by_0 = ax + by = c$. Then

$$\begin{aligned} ax + by &= a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) \\ &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t \\ &= ax_0 + by_0 = c \end{aligned}$$

Therefore, we showed that $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ is a solution of $ax + by = c, \forall t \in \mathbb{Z}$.

- Now we need to show that every integer solution can be expressed in this form.

  Subtract $ax_0 + by_0 = ax + by = c$ togeather:

  $$a(x - x_0) + b(y - y_0) = 0 \implies \frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$$

  Note that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Therefore, $\frac{a}{d} | (y - y_0)$ by the Key Lemma.

  Then let $y - y_0 = -\frac{a}{d}t$ for some $t \in \mathbb{Z}$. Substitute it into the equation:

  $$\frac{a}{d}(x - x_0) = \frac{b}{d}\frac{a}{d}t$$

  Here we have two cases:

  - If $a = 0$, then $by = c$. x can be arbitrary and $y = \frac{c}{b}$. Then $a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = by_o = ax + by = c, \forall t \in \mathbb{R}$. Note that $b \neq 0$ in this case because $(a, b) \neq (0, 0)$. $a \neq 0 \wedge b = 0$ case is similar.
  - Now we talk about the general case. Divide both sides by $\frac{a}{d}$:

    $$x - x_0 = \frac{b}{d}t$$

    Then $x - x_0 = \frac{b}{d}t$ and we already have $y = y_0 - \frac{a}{d}t$. We have shown that every integer solution can be expressed in this form.

□

3.5 Fundedamental theorem of arithmetic

Theorem 7. *$\forall n \in \mathbb{N}, n \geq 1$, n can be written as a product of primes in a unique way.*

Note that one prime can appear multiple times in the product. For example, $12 = 2 \cdot 2 \cdot 3$. Also, we assume that $n = 1$ is an empty product which equals 1.

Usually, we collect the same primes together and write as

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

Now $p_1, p_2, \ldots, p_k$ are all distinct primes that appear in the product and $e_1, e_2, \ldots, e_k$ are the powers of the primes $\in \mathbb{N}$.

We have already proved the existence of the prime factorization in the previous section using the Well-Ordering Principle. Now we need to prove the uniqueness.

3.5.1 Corollary

Let p be a prime, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Then $p|a_1a_2 \ldots a_n \implies p|a_i$ for some i.

Proof. We prove by induction on n.

Base Case: $n = 1$. Then $p|a_1$. Obviously true.

Inductive Step: Suppose the statement is true for $n = k$. We want to show that the statement is true for $n = k + 1$.

Suppose $p|a_1a_2 \ldots a_{k+1}$. Then $p|a_1a_2 \ldots a_k$ or $p|a_{k+1}$. By the inductive hypothesis, $p|a_i$ for some i. □

3.5.2 Proof of the theorem

Proof. Let $n = p_1, p_2, \ldots, p_r = q_1, q_2, \ldots, q_s$ be two prime factorizations of n. We want to show that $r = s$ and $p_i = q_i$ for all i.

Cancel both primes on both sides if the same primes appear in both factorizations. Then we have new primes on both sides that do not equal each other

$$p_1p_2 \ldots p_a = q_1q_2 \ldots q_b$$

Our goal now is to show that there is nothing left on both sides.

Now by the corollary, $p_1|q_1q_2 \ldots q_b$. Then $p_1|q_i$ for some i. But q_i is a prime. Therefore, $p_1 = q_i$. Then we can cancel p_1 and q_i from both sides. So this is a contradiction. Therefore, $r = s$ and $p_i = q_i$ for all i. We have proved the uniqueness. □

Remark: Uniqueness of prime factorization fails in many number systems other than the integers. For example: "even integers": In this system, then 6, 10, 30 and 50 are primes in this system. Then 300 = 6 · 50 = 10 · 30. So the prime factorization is not unique in this system.

3.5.3 Applications

Proposition: Suppose $n = p_1^{d_1} \times \cdots \times p_k^{d_k}, m = p_1^{e_1} \times \cdots \times p_k^{e_k}$ where $p_1, \ldots, p_k$ are distinct primes and $d_1, \ldots, d_k, e_1, \ldots, e_k \in \mathbb{N} \cup 0$. Then $\gcd(n, m) = p_1^{\min(d_1, e_1)} \times \cdots \times p_k^{\min(d_k, e_k)}$ and the largest common multiple $lcm(n, m) = p_1^{\max(d_1, e_1)} \times \cdots \times p_k^{\max(d_k, e_k)}$.

For example:

$$\begin{aligned} 35 &= 5 \times 7 & &= 2^0 \times 5^1 \times 7^1 \times 11^0 \\ 154 &= 2 \times 7 \times 11 & &= 2^1 \times 5^0 \times 7^1 \times 11^1 \\ \gcd(35, 154) &= 2^0 \times 5^0 \times 7^1 \times 11^0 & &= 7 \end{aligned}$$

In general, prime factorization is difficult for large numbers. The Euclidean algorithm is a much faster way to find the gcd of two numbers.

To show the Proposition is true, we need the following corollary:

Let us write the highest power of p appearing in the prime factorization of n as $v_p(n)$. For example: $v_2(12) = 2, v_3(12) = 1, v_5(12) = 0$. Then we have the following corollary:

If m and n are positive integers, then $m|n \iff v_p(m) \leq v_p(n)$ for all primes p.

Proof. Prove both directions:

- $\implies$: Suppose $m|n$. Then $n = mk$ for some $k \in \mathbb{Z}$. Then $v_p(n) = v_p(mk) = v_p(m) + v_p(k) \geq v_p(m)$.
- $\impliedby$: Suppose $0 \leq v_p(m) \leq v_p(n)$ for all primes p. Then $n = p_1^{v_{p_1}(n)} \times \cdots \times p_k^{v_{p_k}(n)} = m(p_1^{v_{p_1}(n) - v_{p_1}(m)} \times \cdots \times p_k^{v_{p_k}(n) - v_{p_k}(m)})$. Since $0 \leq v_p(m) \leq v_p(n)$, we make sure that $\forall i, v_{p_i}(n) - v_{p_i}(m) \in \mathbb{N} \cup 0$. Therefore, $m|n$.

□

Now back to the Proposition:

Proof. By the Corollary above: $\forall$ common divisor m and n is of the form $p_1^{f_1} \ldots p_k^{f_k}$ where $f_i \leq \min(d_i, e_i)$.

Therefore, The greatest common divisor is exactly where $f_i = \min(d_i, e_i)$. Therefore, $\gcd(n, m) = p_1^{\min(d_1, e_1)} \ldots p_k^{\min(d_k, e_k)}$.

If we count for negatives, just add $\pm$ in front of the primes.

Proof of lcm is similar. $\forall$ lcm of m and n is of the form $p_1^{f_1} \ldots p_k^{f_k}$ where $f_i \geq \max(d_i, e_i)$. Therefore, $\text{lcm}(n, m) = p_1^{\max(d_1, e_1)} \ldots p_k^{\max(d_k, e_k)}$. □

Corollary: $\gcd(n, m) \times \text{lcm}(n, m) = nm$.

Proof. $\max(d_i, e_i) + \min(d_i, e_i) = d_i + e_i$. Therefore, $\gcd(n, m) \times \text{lcm}(n, m) = nm$. □

4 Congruences

Definition 3. *Let $a, b, n \in \mathbb{Z}, n \geq 2$. We say that a is **congruent** to b modulo n if $n|(a - b)$. We write $a \equiv b \pmod{n}$.*

Note that $\forall a, n \in \mathbb{Z}, n \geq 2, a \equiv b \pmod{n}$ for some $b \in \mathbb{Z}, 0 \leq b \leq n - 1$.

Congruences mod n may be thought of as a way of focusing on the remainder and casting out (ignoring) the quotient (multiples of n).

4.1 Congruence Class

Definition 4. *Let $n \in \mathbb{Z}, n \geq 2$. The **congruence class** of a modulo n is the set of all integers that are congruent to a modulo n. We write $[a]_n$.*

For example:

$$[0]_5 = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$
$$[1]_5 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$
$$[2]_5 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$
$$[3]_5 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$[4]_5 = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$$

Note that $[a]_n = [b]_n \iff a \equiv b \pmod{n}$.

4.2 Properties of congruences

$$
\begin{aligned}
&a \equiv a \pmod{n} \forall a, n \in \mathbb{Z} \\
&a \equiv b \pmod{n} \implies b \equiv a \pmod{n} \\
&a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \implies a \equiv c \pmod{n} \\
&a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n} \\
&a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n} \\
&a \equiv b \pmod{n} \implies ac \equiv bc \pmod{n} \\
&a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n} \forall k \in \mathbb{N}
\end{aligned}
$$

Note that it is reflective, symmetric and transitive. It is also closed under addition, multiplication and exponentiation.

4.2.1 Arithmetics on congruence classes

Arithmetics between congruence classes:

$$
\begin{aligned}
[a]_n + [b]_n &= [a + b]_n \\
[a]_n \times [b]_n &= [a \times b]_n \\
[a]_n^k &= [a^k]_n
\end{aligned}
$$

If $x_1 \equiv x_2 \pmod{n}, y_1 \equiv y_2 \pmod{n}$, then

- $x_1 + y_1 \equiv x_2 + y_2 \pmod{n}$
- $x_1 y_1 \equiv x_2 y_2 \pmod{n}$
- $x_1 - y_1 \equiv x_2 - y_2 \pmod{n}$

Proof. Suppose $x_1 - x_2 = an, y_1 - y_2 = bn$ for some $a, b \in \mathbb{Z}$. Then

- $(x_1 + y_1) - (x_2 + y_2) = an + bn = (a + b)n \equiv 0 \pmod{n}$ Thus $x_1 + y_1 \equiv x_2 + y_2 \pmod{n}$
- Subtraction is similar to addition proof
- $x_1 = x_2 + an, y_1 = y_2 + bn$ Then $x_1 y_1 = x_2 y_2 + n(a y_2 + b x_2 + ab) \equiv x_2 y_2 \pmod{n}$

□

Using the rules above, we can calculate some insanely big numbers:

$$\begin{aligned} 48^{100} + 15 \times 70002 \pmod 7 &\equiv (-1)^{100} + 1 \times 2 \pmod 7 \\ &\equiv 1 + 2 \pmod 7 \\ &\equiv 3 \pmod 7 \end{aligned}$$

Note that if $d \equiv e \pmod n$, does not imply $a^d \equiv a^e \pmod n$. For example, $2 \equiv 9 \pmod 7$, but $2^2 \not\equiv 2^9 \pmod 7$.

4.2.2 Modular exponentiation

Modular exponentiation like raising an integer to a high power modulo n, is used in cryptography.

For large $x, y \equiv a^x \pmod n$ is easy to compute. On the other hand, given y, recovering x is hard. Without additional information, it is a "Discrete Logarithm Problem".

A quick algorithm for computing $a^x \pmod n$ is called "the method of repeated squaring". For example, $a^{13} \pmod n$ can be computed as follows:

For example: find $7^5 1 \pmod 1 7$

$$\begin{aligned} 7^1 &\equiv 7 \pmod{17} \\ 7^2 &\equiv 7 \times 7 \equiv 49 \equiv 15 \equiv -2 \pmod{17} \\ 7^4 &\equiv (-2)^2 \equiv 4 \pmod{17} \\ 7^8 &\equiv 4^2 \equiv 16 \equiv -1 \pmod{17} \\ 7^{16} &\equiv (-1)^2 \equiv 1 \pmod{17} \\ 7^{32} &\equiv 1^2 \equiv 1 \pmod{17} \\ 7^{51} &\equiv 7^{32} \times 7^{16} \times 7^2 \times 7^1 \equiv 1 \times 1 \times (-2) \times 7 \equiv -14 \equiv 3 \pmod{17} \end{aligned}$$

4.2.3 Representations of integers

Theorem 8. *Let $b \in \mathbb{Z}, b \geq 2$. Then $\forall m \in \mathbb{N}$ can be written as*

$$m = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where $k \in \mathbb{N}, a_0, a_1, \ldots, a_k \in \mathbb{Z}, 0 \leq a_i \leq b - 1$ for all i.
Moreover, this representation is unique.

The theorem gives a representation of m in base b. a_k is the highest digit and a_0 is the lowest digit. If $b = 10$, then it is the normal decimal representation. We just simply leave out the subscript $b = 10$.

For example, $51 = 32 + 16 + 2 + 1 = 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 110011_2$.

Proof. Prove by strong induction on n.

Base Case: $b^0 \leq n < b^1$. Then $n = (n)_b$.

Inductive Step: Assume $n \geq b$ and the existence part of the theorem holds for any integer between 1 and $n - 1$. We want to show that the existence part of the theorem holds for n.

Divide n by b: $n = bq + r$ where $0 \leq r < b$. Then $0 \leq q < n$. By the inductive hypothesis, q can be written as

$$q = c_s b^s + c_{s-1} b^{s-1} + \cdots + c_1 b + c_0$$

Now $n = qb + r = c_s b^{s+1} + c_{s-1} b^s + \cdots + c_1 b^2 + c_0 b + r$. Therefore, n can be written as

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

This is the representation of n in base b.

For uniqueness, again by induction:

Base Case: $n = b^0 \leq n < b^1$. Then $n = (n)_b$. It only has 1 digit and it has to be n, thus unique.

Inductive Step: Assume $n \geq b$ and the uniqueness part of the theorem holds for any integer between 1 and $n - 1$. We want to show that the uniqueness part of the theorem holds for n.

assume n can be expressed in two ways:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$
$$n = c_s b^s + c_{s-1} b^{s-1} + \cdots + c_1 b + c_0$$

Then

$$a_0 = n \pmod b = c_0 \wedge 0 \leq a_0, c_0 \leq b - 1$$
$$\frac{1}{b}(n - a_0) = a_k b^{k-1} + \cdots + a_2 b + a_1 = \frac{1}{b}(n - c_0) = c_s b^{s-1} + \cdots + c_2 b + c_1$$

By induction assumption, $k - 1 = m - 1 \wedge a_i = c_i$ for all i. Therefore, $k = s \wedge a_i = c_i$ for all i. $\square$

4.2.4 Exponentiation arithmetic

Back to repeated squaring, the goal is to compute $a^x \pmod n$.

Pre-compute: $a, a^2, a^4, a^8, \ldots, a^{2^k} \pmod n$

Now write x in base 2: $x = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_m}$ where $k_1 > k_2 > \cdots > k_m \geq 0$.

Then $a^x = a^{2^{k_1}} \times a^{2^{k_2}} \times \cdots \times a^{2^{k_m}} \pmod n$.

For example: Compute the last two digits of 53^{29}. Equivalently, it is $53^{29} \pmod{100}$.

Start with 29 in base 2: $29 = 16+8+4+1$. Then $53^{29} = 53^{16} \times 53^8 \times 53^4 \times 53^1 \pmod{100}$.

$$
\begin{aligned}
53^1 &= 53 \pmod{100} \\
53^2 &= 2809 \equiv 9 \pmod{100} \\
53^4 &= (53^2)^2 \equiv 81 \pmod{100} \\
53^8 &\equiv 81^2 = 6561 \equiv 61 \pmod{100} \\
53^{16} &\equiv 61^2 = 3721 \equiv 21 \pmod{100} \\
53^{29} &= 21 \times 61 \times 81 \times 53 \equiv 13 \pmod{100}
\end{aligned}
$$

4.3 Linear congruences

$ax \equiv b \pmod n$ is a linear congruence. We want to find all solutions of x given a, b, n.

The case where $b = 1$ is of particular interest. Here x is called the inverse of a modulo n. We write $x = a^{-1} \pmod n$.

Note that $ax \equiv b \pmod n \iff ax = b + nk$ for some $k \in \mathbb{Z}$. For example, $ax - nk = b$ for some $k \in \mathbb{Z}$. We know that $ax - nk = \gcd(a, n)$ by Bezout's theorem. Therefore, $ax - nk = \gcd(a, n)$ for some $k \in \mathbb{Z}$.

If it exists, we are interested in how many there are.

4.3.1 Solving linear congruences

Two solutions x_1 and x_2 are considered the same $\iff \exists y \in \mathbb{Z}$ s.t $ax - b = ny$ or Equivalently $ax - ny = b$.

In particular, if $\gcd(a, n)$ does not divide b, then the congruence $ax \equiv b \pmod n$ has no integer solution.

Theorem 9. *If $d = \gcd(a, n)|b$, then the congurence $ax \equiv b \pmod{n}$ has exactly d solutions*

Proof. Assume that $d = \gcd(a, n)|b$. Then the linear Diophantine equation $ax - b = ny \iff ax - ny = b$ for some $x, y \in \mathbb{Z}$ has a particular solution (x_0, y_0) by Bezout's theorem.

General solution: $x = x_0 + \frac{n}{d}t, y = y_0 - \frac{a}{d}t$ for some $t \in \mathbb{Z}$.

We are only interested in x here and up to multiples of n. In other words, $x_0 + \frac{n}{d}t_1$ and $x_0 + \frac{n}{d}t_2$ are considered the same if and only if $\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}$ or equivalently, $\frac{n}{d}(t_1 - t_2) \equiv 0 \pmod{n}$. (So that the congruence is the same)

$\frac{n}{d}(t_1 - t_2) \equiv 0 \pmod{n} \implies \frac{n}{d}(t_1 - t_2) = ns \implies t_1 - t_2 = ds$ for some $s \in \mathbb{Z}$. Therefore, $t_1 - t_2 \equiv 0 \pmod{d}$. Thus we get exactly d solutions by letting t range from 0 to $d - 1$. □

Conclusion: Every solution is $ax \equiv b \pmod{n}$ is of the form $x = x_0 + \frac{n}{d}t$ for some $t \in \mathbb{Z}$ where $d = \gcd(a, n)$ and x_0 is a particular solution. Two solutions $x_1 = x_0 + \frac{n}{d}t_1$ and $x_2 = x_0 + \frac{n}{d}t_2$ are considered the same if and only if $\frac{n}{d}(t_1 - t_2) \equiv 0 \pmod{n} \iff t_1 - t_2 \equiv 0 \pmod{d}$. Thus we get exactly d solutions by letting t range from 0 to $d - 1$.

4.3.2 Examples

For example, solve $10x \equiv 3 \pmod{12}$. Here $d = \gcd(10, 12) = 2$. Since $2 \nmid 3$, there are no solutions. The gcd needs to divide the congruence value.

Another example, $10x \equiv 4 \pmod{12}$. Here we expect 2 solutions. To find them, we start by finding a particular solution for $10x - 12y = 4$. Since the number is small, we can just guess the solution:

$x_0 = 4, y_0 = 3$ is the particular solution. Then the general solution is $x = 4 + \frac{12}{2}t = 4 + 6t$ for some $t \in \mathbb{Z}$.

- t ranges from 0 to 1.
- When $t = 0$, $x = 4$.
- When $t = 1$, $x = 10$.

So the solutions are $x \equiv 4 \pmod{12}$ and $x \equiv 10 \pmod{12}$.

4.3.3 Multuplicative inverses

Particular interesting case when $b = 1$. Then $ax \equiv 1 \pmod{n}$ is called the inverse of a modulo n. We write $x = a^{-1} \pmod{n}$.

In this case, the congruence has a solution if and only if $\gcd(a, n) = 1$, which also means that the congruence has exactly one solution.

Not all congruence classes have an inverse. For example, $ax \equiv 1 \pmod{10}$:

$$\begin{aligned} 1 \times 1 &\equiv 1 \pmod{10} \\ 3 \times 7 &\equiv 1 \pmod{10} \\ 7 \times 3 &\equiv 1 \pmod{10} \\ 9 \times 9 &\equiv 1 \pmod{10} \end{aligned}$$

And the rest does not have one. It is because the rest have a gcd with 10 that is greater than 1.

Corollary: Let p be a prime, then every $a \not\equiv 0 \pmod{p}$ has an inverse modulo p.

Proof. It is because $\gcd(a, p) = 1$. By Bezout's theorem, $ax - py = 1$ for some $x, y \in \mathbb{Z}$. Therefore, $ax \equiv 1 \pmod{p}$. Therefore, x is the inverse of a modulo p. □

Corollary: Let p be a prime, then $a \equiv a^{-1} \pmod{p} \iff a \equiv \pm 1 \pmod{p}$.

Proof. Indeed multiplying both sides by a, we get $a \equiv a^{-1} \pmod{p} \implies a^2 \equiv 1 \pmod{p} \iff (a-1)(a+1) \equiv 0 \pmod{p} \iff a \equiv \pm 1 \pmod{p}$.

If $a \not\equiv 1$ then $a - 1$ has a multiplicative inverse modulo p. Denote this multiplicative inverse by b. Time both sides by b Then $b(a-1)(a+1) \equiv 0 \pmod{p} \implies a + 1 \equiv 0 \pmod{p} \implies a \equiv -1 \pmod{p}$. Therefore, $a \equiv b \pmod{p}$.

Similarly we can find that $a \not\equiv -1 \implies a \equiv 1 \pmod{p}$. So we proved the corollary. □

For example, solve $17x \equiv 1 \pmod{55}$. First, find the gcd of 17 and 55:

$$\begin{aligned} 55 &= 3 \times 17 + 4 \\ 17 &= 4 \times 4 + 1 \\ 4 &= 4 \times 1 \end{aligned}$$

Now use back substitution:

$$\begin{aligned} 1 &= 17 - 4 \times 4 \\ &= 17 - 4 \times (55 - 3 \times 17) \\ &= 13 \times 17 - 4 \times 55 \end{aligned}$$

Therefore, $13 \times 17 \equiv 1 \pmod{55}$. So the solution is $x \equiv 13 \pmod{55}$.

4.4 Chinese Remainder Theorem

Theorem 10. *Suppose $n_1, n_2 \in \mathbb{N}$ and $\gcd(n_1, n_2) = 1$ (Relatively prime). Then for any integers $a_1, a_2, \exists x \in \mathbb{Z}$ s.t*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}$$

Moreover, the solution is unique modulo $n_1 n_2$.

Here uniqueness means the following: Suppose

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned} \qquad\qquad \begin{aligned} y &\equiv a_1 \pmod{n_1} \\ y &\equiv a_2 \pmod{n_2} \end{aligned}$$

Then $x \equiv y \pmod{n_1 n_2}$.

4.4.1 Proof of uniqueness

Proof. Assume $x \equiv y \equiv a_1 \pmod{n_1}$ and $x \equiv y \equiv a_2 \pmod{n_2}$. Then $n_1 | (x - y)$ and $n_2 | (x - y)$.

Then $x - y = 0 \pmod{n_1}$ and $x - y = 0 \pmod{n_2}$. Then $n_1 | (x - y)$ and $n_2 | (x - y)$.

Note that any common multiple of n_1, n_2 is divisible by

$$\text{lcm}(n_1, n_2) = \frac{n_1 n_2}{\gcd(n_1, n_2)} = n_1 n_2.$$

Then $n_1 n_2 | (x - y)$. $(x - y)$ is a common divisor.
Therefore, $x \equiv y \pmod{n_1 n_2}$. □

Here we can also apply the Key Lemma to prove the existence of the solution.

4.4.2 Proof of existence

Proof. Let $n = n_1 n_2$. To each congruence class $[x] \pmod{n}$, associate a pair of integers (z_1, z_2) where $z_1 \equiv x \pmod{n_1}$ and $z_2 \equiv x \pmod{n_2}$. Pick $0 \leq z_1 < n_1$ and $0 \leq z_2 < n_2$.

Note that there are exactly $n_1 n_2 = n$ such pairs. And there are exactly n congruence classes $[x] \pmod{n}$.

Moreover, by uniqueness, we never associate the same pair z_1, z_2 to two different congruence classes $[x] \pmod{n}$.

By the Pigeonhole Principle, we conclude that every pair (a_1, a_2) is associated with some congruence class $[x] \pmod{n}$. Therefore, the solution exists. □

Example illustrating the theorem: $n_1 = 3, n_2 = 5$

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

Where $0 \leq x \leq 14$. Can list out all the combinations to find it, but we need a better algorithm for larger numbers.

4.4.3 Algorithm

Note that we only need to solve two systems of linear congruences:

$$\begin{aligned} y &\equiv 1 \pmod{n_1} \\ y &\equiv 0 \pmod{n_2} \end{aligned} \qquad \begin{aligned} z &\equiv 0 \pmod{n_1} \\ z &\equiv 1 \pmod{n_2} \end{aligned}$$

because we can do $x = a_1 y + a_2 z$ to get $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$. by solving:

$$\begin{aligned} x &\equiv a_1 y + a_2 z \equiv a_1 \times 1 + a_2 \times 0 \pmod{n_1} \\ x &\equiv a_1 y + a_2 z \equiv a_1 \times 0 + a_2 \times 1 \pmod{n_2} \end{aligned}$$

Now the problem comes to how do we solve

$$\begin{aligned} y &\equiv 1 \pmod{n_1} \\ y &\equiv 0 \pmod{n_2} \end{aligned}$$

Set $y = n_2 t$ into the first congruence. $n_2 t \equiv 1 \pmod{n_1}$. Since $\gcd(n_1, n_2) = 1$, we can find $t = t_1$ such that $n_2 t_1 \equiv 1 \pmod{n_1}$. Then t_1 is the multiplicative inverse of n_2 modulo n_1. Then $y = n_2 t_1$ is the solution to the first congruence.

Similarly, we can find $z = n_1 t_2$ is the solution to the second congruence.

In Summary, the solution to the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}$$

is

$$x = a_1 n_2 t_1 + a_2 n_1 t_2$$

where t_1 is the multiplicative inverse of n_2 modulo n_1 and t_2 is the multiplicative inverse of n_1 modulo n_2.

So basically: $t_1 \equiv n_2^{-1} \pmod{n_1}$ and $t_2 \equiv n_1^{-1} \pmod{n_2}$.

4.4.4 Example

For example, solve

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

Here: $n_1 = 7, n_2 = 3, a_1 = 3, a_2 = 2$.

First, find the multiplicative inverse of 3 modulo 7.

$$\begin{aligned} 7 &= 2 \times 3 + 1 \\ 1 &= 7 - 2 \times 3 \end{aligned}$$

Therefore, $3^{-1} \equiv -2 \equiv 5 \pmod{7}$.

Then find the multiplicative inverse of 7 modulo 3.

$$3 = 1 \times 3 + 0$$

Therefore, $7^{-1} \equiv 1 \pmod{3}$.

Then the solution is

$$x \equiv a_1 t_1 n_2 + a_2 t_2 n_1 \equiv 3 \times 5 \times 3 + 2 \times 1 \times 7 \equiv 45 + 14 \equiv 17 \pmod{21}$$

Another example, revisit: Find $17^{-1} \pmod{55}$.

Use the fact that $55 = 11 \times 5, \gcd(11, 5) = 1$. Then we can solve:

$$\begin{aligned} 17x &\equiv 1 \pmod{11} &&\implies 6x \equiv 1 \pmod{11} \\ 17x &\equiv 1 \pmod{5} &&\implies 2x \equiv 1 \pmod{5} \end{aligned}$$

Easily find that $x \equiv 2 \pmod{11}$ and $x \equiv 3 \pmod{5}$. Then we need to recover x. Know that:

$$x \equiv a_1 t_1 n_2 + a_2 t_2 n_1 \pmod{n_1 n_2}$$

And we know that $n_1 = 5, n_2 = 11, a_1 = 3, a_2 = 2$. Then we can find that

$$\begin{aligned} t_1 \equiv n_2^{-1} &\equiv 11^{-1} \equiv 1 \pmod{5} \\ t_2 \equiv n_1^{-1} &\equiv 5^{-1} \equiv -2 \pmod{11} \end{aligned}$$

Then $x \equiv 3 \times 1 \times 11 + 2 \times (-2) \times 5 \equiv 33 + 90 \equiv 123 \equiv 13 \pmod{55}$.

4.5 More general version of CRT

Theorem 11. *The system of r congruences:*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a unique solution modulo $N = n_1 n_2 \dots n_r$ if $n_1, n_2, \dots, n_r$ are pairwise relatively prime.

4.5.1 proof

Proof. Induction on r. The base case $r = 1$ is clear and $r = 2$ is the Chinese Remainder Theorem, discussed above.

Inductive step: Assume that the theorem holds for $r - 1$ numbers. We want to show that the theorem holds for r.

Let b be the unique solution to the system of

$$\begin{aligned} x &\equiv a_{r-1} \pmod{n_{r-1}} \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

Then we can reduce the system of r congruences to a system of $r-1$ congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_{r-2} \pmod{n_{r-2}} \\ x &\equiv b \pmod{n_{r-1}n_r} \end{aligned}$$

Note that there are only $r-1$ congruences now and all n_i are relatively prime to each other.

By induction assumption, the system has a unique solution modulo $N = n_1 n_2 \dots n_{r-2} n_{r-1} n_r$. Therefore, the system of r congruences has a unique solution modulo $N = n_1 n_2 \dots n_r$. □

4.5.2 Algorithm

In practice, to solve the system of linear congruences, we use the recursive step as shown in the proof.

Alternatively, there is a formula that allows us to find x in one step.

Let $N = n_1 n_2 \dots n_r$. $N_i = N/n_i$. Then the solution to the system of linear congruences is

$$x = \sum_{i=1}^{r} a_i N_i t_i$$

where t_i is the multiplicative inverse of N_i modulo n_i.

To see that $x \equiv a_i \pmod{n_i}$, note that $N_i t_i \equiv 1 \pmod{n_i}$ and $N_i t_i \equiv 0 \pmod{n_j}$ for all $j \neq i$.

For example, solve

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{7} \\ x &\equiv 5 \pmod{11} \end{aligned}$$

$$N = 2 \times 3 \times 5 \times 7 \times 11 = 2310$$
$$N_1 = 2310/2 = 1155$$
$$t_1 \equiv (3 \times 5 \times 7 \times 11)^{-1} \equiv (1^4)^{-1} \equiv 1 \pmod 2$$
$$N_2 = 2310/3 = 770$$
$$t_2 \equiv (2 \times 5 \times 7 \times 11)^{-1} \equiv ((-1) \times (-1) \times 1 \times (-1))^{-1} \equiv 2 \pmod 3$$
$$N_3 = 2310/5 = 462$$
$$t_3 \equiv (2 \times 3 \times 7 \times 11)^{-1} \equiv (2 \times 3 \times 2 \times 1)^{-1} \equiv 3 \pmod 5$$
$$N_4 = 2310/7 = 330$$
$$t_4 \equiv (2 \times 3 \times 5 \times 11)^{-1} \equiv (2 \times 3 \times (-2) \times 4)^{-1} \equiv 1 \pmod 7$$
$$N_5 = 2310/11 = 210$$
$$t_5 \equiv (2 \times 3 \times 5 \times 7)^{-1} \equiv (2 \times 3 \times 5 \times 7)^{-1} \equiv (10 \times 21)^{-1} \equiv 1 \pmod{11}$$

Thus $x = 1 \times 1155 \times 1 + 2 \times 770 \times 2 + 3 \times 462 \times 3 + 4 \times 330 \times 1 + 5 \times 210 \times 1 \equiv 1523 \pmod{2310}$.

Another example: Find $x = 8^{10003} \pmod{105}$.

Note that $105 = 3 \times 5 \times 7$. Then we can solve the system of linear congruences:

$$\begin{aligned} x &\equiv 8^{10003} \pmod 3 \\ x &\equiv 8^{10003} \pmod 5 \\ x &\equiv 8^{10003} \pmod 7 \end{aligned}$$

then put them all together using CRT.

$$x \equiv 8^{10003} \equiv (-1)^{10003} \equiv -1 \equiv 2 \pmod 3$$
$$x \equiv 8^{10003} \equiv (-2)^{10003} \equiv ((-2)^2)^{5001} \times (-2) \equiv (-1)^{5001} \times (-2) \equiv 2 \pmod 5$$
$$x \equiv 8^{10003} \equiv 1^{10003} \equiv 1 \pmod 7$$

3,5,7 are pairwise relatively prime. Then we can use the formula to find the solution:

$$\begin{aligned} a_1 = 2, N_1 = 35, t_1 &\equiv (N_1)^{-1} \pmod 3 \\ a_2 = 2, N_2 = 21, t_2 &\equiv (N_2)^{-1} \pmod 5 \\ a_3 = 1, N_3 = 15, t_3 &\equiv (N_3)^{-1} \pmod 7 \end{aligned}$$

$$
\begin{aligned}
t_1 &\equiv 35^{-1} \equiv (-1)^{-1} \equiv 2 \pmod 3 \\
t_2 &\equiv 21^{-1} \equiv 1^{-1} \equiv 1 \pmod 5 \\
t_3 &\equiv 15^{-1} \equiv 1^{-1} \equiv 1 \pmod 7
\end{aligned}
$$

$$
x = 2 \times 35 \times 2 + 2 \times 21 \times 1 + 1 \times 15 \times 1 \equiv 197 \equiv 92 \pmod{105}
$$

4.5.3 More generalized CRT

Now consider a system of $\gcd = d > 1$.

solve $x \equiv 2 \pmod 4, x \equiv 1 \pmod{12}$. There is no solution since the first congruence implies x is even and the second congruence implies x is odd.

solve $x \equiv 1 \pmod 8, x \equiv 1 \pmod{12}$. Obviously, $x = 1, 25$ are solutions to it. Here it has solutions, but it is not unique under modulo $8 \times 12 = 96$.

Theorem 12. *The system of linear congruences*

$$
\begin{aligned}
x &\equiv a_1 \pmod{n_1} \\
x &\equiv a_2 \pmod{n_2} \\
&\vdots \\
x &\equiv a_r \pmod{n_r}
\end{aligned}
$$

has a solution if and only if $a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$ *for all* i, j*. Moreover, the solution is unique modulo* $N = lcm(n_1, n_2, \ldots, n_r)$.

Here when $\gcd(n_i, n_j) = 1$, the congruence is the same as the original version of the Chinese Remainder Theorem. When $\gcd(n_i, n_j) > 1$, the congruence is the same as the more generalized version of CRT.

To prove it we need the following Lemma:

$$
x \equiv y \pmod n \iff ax \equiv ay \pmod{an}
$$

Proof. Let $z = x - y$. Then the lemma can be rewritten as

$$
z \equiv 0 \pmod n \iff az \equiv 0 \pmod{an}
$$

Forward direction: $\exists w \in \mathbb{Z}$ s.t $z = wn \implies \exists w \in \mathbb{Z}$ s.t $az = awn$.
Backward direction: $\exists w \in \mathbb{Z}$ s.t $az = awn \implies \exists w \in \mathbb{Z}$ s.t $z = wn$.
Therefore, the lemma is proved. □

Now back to the proof of the theorem.

Proof. If there is a solution x to the linear system, then reducing to modulo d, we obtain

$$\begin{aligned} x &\equiv a_1 \pmod{d} \\ x &\equiv a_2 \pmod{d} \\ &\vdots \\ x &\equiv a_r \pmod{d} \end{aligned}$$

Then $a_i \equiv a_j \pmod{d}$ for all i, j.

Conversely, if $a_i \equiv a_j \pmod{d}$ for all i, j, then we can find x_i such that $x_i \equiv a_i \pmod{n_i}$. Then $x_i \equiv a_i \pmod{d}$. Then $x_i \equiv a_j \pmod{d}$. Then $x_i \equiv x_j \pmod{d}$. Then $x_i = x_j + dn$ for some $n \in \mathbb{Z}$. Then $x_i \equiv x_j \pmod{dn_i}$. Then $x_i \equiv x_j \pmod{N}$. Therefore, the solution is unique modulo N. □

4.6 Divisibility criteria

$n = (a_m a_{m-1} \dots a_1 a_0)_b = a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b + a_0$.

4.6.1 Base 10 divisibility criteria

The idea is to find a pattern in the congruence of each power of 10 modulo n.

For example:

- $10^k \equiv 1 \pmod{9}, \forall k \geq 0$. Note that it is true for modulo 3 as well.
  - Consider $n = 114000$ Then $1 + 1 + 4 + 0 + 0 + 0 = 6$ and $6 \equiv 0 \pmod{3}$, but $6 \not\equiv 0 \pmod{9}$. Therefore, $n \not\equiv 0 \pmod{9}$.
- For divisibility by 11, $10^0 \equiv 1, 10^1 \equiv -1, 10^2 \equiv 1, 10^3 \equiv -1, \dots$. Then $10^k \equiv (-1)^k \pmod{11}$.
  - Consider $n = 123456$. Then $6 - 5 + 4 - 3 + 2 - 1 = 3$, not congruent to 0 mod 11. So n is not divisible by 11.

In particular, $(a_m a_{m-1} \dots a_1 a_0)$ is divisible by 2^k if and only if $(a_k a_{k-1} \dots a_1 a_0)$ is divisible by 2^k. Similarly, $(a_m a_{m-1} \dots a_1 a_0)$ is divisible by 5^k if and only if $(a_k a_{k-1} \dots a_1 a_0)$ is divisible by 5^k.

This is because $10^k \equiv 0 \pmod{2^k}$ if and only if $10^k \equiv 0 \pmod{5^k}$. For example, $n = 114000$ is divisible by $2^4, 5^3$ not $2^5, 5^4$.

- So for 2^4, $114000 \equiv 4 \times 10^3 \equiv 0 \pmod{2^4}$.
- For 2^5, $114000 \equiv 10^4 + 4 \times 10^3 \equiv 16 \pmod{2^5}$. Thus not divisible by 2^5.
- For 5^3, $114000 \equiv 0 \pmod{5^3}$.
- For 5^4, $114000 \equiv 10^3 + 4 \times 10^2 \equiv 400 \pmod{5^4}$. Thus not divisible by 5^4.

For mod 11, $10^k \equiv (-1)^k \pmod{11}$. For example, $n = 123456$ is not divisible by 11 because $10^6 \equiv 1 \pmod{11}$ and $1 - 2 + 3 - 4 + 5 - 6 \equiv 7 \pmod{11}$. This is because $10 \equiv -1 \pmod{1}1$

With the same idea, divisibility by 101: Use the congruence $10^2 \equiv -1 \pmod{101}$.

$$\begin{aligned} n &= (a_0 + 10a_1) + 10^2(a_2 + 10a_3) + \cdots + 10^{2k}(a_k + 10a_{k+1}) \\ &\equiv (a_0 + 10a_1) - 10^2(a_2 + 10a_3) + \cdots \pmod{101} \\ &= (a_0 + 10a_1) - (a_2 + 10a_3) + (a_4 + 10a_5) \cdots \pmod{101} \\ &= (a_1 a_0) - (a_3 a_2) + (a_5 a_4) \cdots \pmod{101} \end{aligned}$$

For example: n=123456789 is not divisible by 101 because $10^2 \equiv -1 \pmod{101}$ and $89 - 67 + 45 - 23 + 1 \equiv 22 + 22 + 1 \equiv 45 \pmod{101}$.

Similarly for 1001: $10^3 \equiv -1 \pmod{1001}$. Now break up into 3-digit bits. $n \equiv (a_2 a_1 a_0) - (a_5 a_4 a_3) + (a_8 a_7 a_6) \cdots \pmod{1001}$. For example, $n = 234934$ is not divisible by 1001 because $934 - 234 \equiv 700 \pmod{1001}$.

Note that $1001 = 7 \times 11 \times 13$. Therefore, n is divisible by 1001 if and only if n is divisible by 7, 11, and 13.

- Is $n = 234934$ divisible by 7? $234 - 934 \equiv 700 \equiv 0 \pmod{7}$.
- Is $n = 234934$ divisible by 11? $934 - 234 \equiv 700 \equiv 7 \pmod{11}$.
- Is $n = 234934$ divisible by 13? $934 - 234 \equiv 700 \equiv 7 \times 2^5 \times 5^2 \pmod{13}$.

Therefore, $n = 234934$ is not divisible by 1001.

5 Fermat's Theorems

5.1 Wilson's Theorem

Theorem 13. *Let p be a prime. Then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. When $p = 2$, this is obvious.

Assume now that $p > 3 \implies$ p is odd.

Consider the set $S = \{1, 2, \ldots, p-1\}$. Then S is a group under multiplication modulo p. Note that $\forall s \in S, \exists s^{-1} \in S$ such that $ss^{-1} \equiv 1 \pmod{p}$.

However, none of them is its own inverse except 1. It is because $x^2 \equiv 1 \pmod{p} \iff (x-1)(x+1) \equiv 0 \pmod{p}$. Then $x \equiv \pm 1 \pmod{p}$. A property of prime number modulo discussed in the previous section.

Then we can pair up the elements in S into pairs (s, s^{-1}). Then the product of each pair is congruent to 1 modulo p. Note that p is odd, then $p-1$ is even.

Claim: all numbers in S except 1 and the last term are paired up.

Note that the last term is $p-1$. Then $p-1 \equiv -1 \pmod{p}$. Then $p-1$ is its own inverse. Only the term ± 1 is its own inverse and left out.

Therefore, $(p-1)! \equiv 1 \times 2 \times \cdots \times (p-2) \times (p-1) \equiv 1 \times 2 \times \cdots \times (p-2) \times 1 \equiv -1 \pmod{p}$.

Therefore, the product of all the elements in S is congruent to -1 modulo p. □

For example: $10! = 1 \times (2 \times 6) \times (3 \times 4) \times (5 \times 9) \times (7 \times 8) \times 10 \equiv -1 \pmod{11}$.

5.2 Fermat's Little Theorem

Theorem 14. *Let p be a prime and a be an integer such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Claim: $a, 2a, 3a, \ldots, (p-1)a$ are all distinct modulo p.

if $ia \equiv ja \pmod{p}$, then $ia - ja \equiv 0 \pmod{p} \implies (i-j)a \equiv 0 \pmod{p}$. Since $p \nmid a$, then $p \mid (i-j)$. Since $0 < i, j < p$, then $i = j$.

Thus the $p-1$ distinct congruences $a, 2a, 3a, \ldots, (p-1)a$ are all distinct modulo p. Which is equivalent to the $p-1$ distinct congruences $1, 2, 3, \ldots, p-1$.

Then we can multiply all the congruences together to get

$$a \times 2a \times 3a \times \cdots \times (p-1)a \equiv a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

by Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Therefore, $a^{p-1} \equiv 1 \pmod{p}$. □

5.2.1 Corollaries

Corollary 1: Let p be a prime and a be an integer. Then $a^p \equiv a \pmod{p}$.

Proof. If $a \equiv 0 \pmod{p}$, then $a^p \equiv 0 \equiv a \pmod{p}$. If $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$. Then $a^p \equiv a \pmod{p}$. □

Corollary 2: Let p be a prime and a be an integer. If $d \equiv e \pmod{p-1}$, then $a^d \equiv a^e \pmod{p}$.

Note that Corollary 1 is a special case of Corollary 2 when $d = p, e = 1 \implies a^p \equiv a^1 \pmod{p}$.

Proof. May assume $d \geq e, d - e = k(p-1)$ for some $k \in \mathbb{Z}, k \geq 0$. Then $a^d \equiv a^{e+k(p-1)} \equiv a^e(a^{p-1})^k \equiv a^e \pmod{p}$.

We used Fermat's Little Theorem in the last step where $a^{p-1} \equiv 1 \pmod{p} \implies (a^{p-1})^k \equiv 1^k \equiv 1 \pmod{p}$. □

5.2.2 Example

Find $2^{180} \pmod{89}$.

Note that 89 is a prime. Then $2^{88} \equiv 1 \pmod{89}$ by Fermat's Little Theorem. Then $2^{180} \equiv 2^{88\times 2+4} \equiv (2^{88})^2 \times 2^4 \equiv 1^2 \times 16 \equiv 16 \pmod{89}$.

5.3 Euler's Theorem

5.3.1 Euler's phi-function

Definition 5. *Let $n \in \mathbb{N}$. The Euler's phi-function $\phi(n)$ is the number of positive integers less than n that are relatively prime to n.*

For example:

$$\begin{aligned}
\phi(1) &= 1 && \{1\} \\
\phi(2) &= 1 && \{1\} \\
\phi(3) &= 2 && \{1,2\} \\
\phi(4) &= 2 && \{1,3\} \\
\phi(5) &= 4 && \{1,2,3,4\} \\
\phi(6) &= 2 && \{1,5\} \\
\phi(7) &= 6 && \{1,2,3,4,5,6\} \\
\phi(8) &= 4 && \{1,3,5,7\} \\
\phi(9) &= 6 && \{1,2,4,5,7,8\} \\
\phi(10) &= 4 && \{1,3,7,9\} \\
\phi(11) &= 10 && \{1,2,3,4,5,6,7,8,9,10\}
\end{aligned}$$

Similarly, we can conclude that $\phi(p) = p - 1$ for any prime p.

5.3.2 Euler's Theorem

Theorem 15. *Let* $n \in \mathbb{N}$ *and* $a \in \mathbb{Z}$ *such that* $\gcd(a, n) = 1$. *Then* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Note that Fermat's Little Theorem is a special case of Euler's Theorem when n is a prime.

For example: $3^{\phi(10)} \equiv 3^4 \equiv 1 \pmod{10}$. It is due to the fact that $\gcd(3, 10) = 1$ and $\phi(10) = 4$.

Lemma. $\gcd(a, n) = 1 \wedge \gcd(b, n) = 1 \iff \gcd(ab, n) = 1$.

Proof. $\gcd(a, n) = 1 \wedge \gcd(b, n) = 1 \implies \exists x, y \in \mathbb{Z}$ such that $ax + ny = 1$ and $\exists u, v \in \mathbb{Z}$ such that $bu + nv = 1$. Then $ab(xu) + n(axv + nyu + bv) = 1$. Therefore, $\gcd(ab, n) = 1$.

$\gcd(ab, n) = 1 \implies \exists x, y \in \mathbb{Z}$ such that $abx + ny = 1$. Then $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$. □

5.3.3 Proof of Euler's Theorem

Proof. We use a similar proof to Fermat's Little Theorem.

Let $S = \{a_1, a_2, \ldots, a_{\phi(n)}\}$ be the set of all positive integers less than n that are relatively prime to n. Then S is a group under multiplication modulo n.

Claim: $aS = \{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$ is the same set as S if a is relatively prime to n.

If $aa_i \equiv aa_j \pmod{n}$, then $a_i \equiv a_j \pmod{n}$ because a is invertible modulo n. Then $a_i = a_j$ since S is a set of distinct elements. Therefore, $aS = S$. aS is another group under multiplication modulo n. The product of all elements in aS should be congruent to the product of all elements in S.

Then we can multiply all the elements in S together to get

$$a_1 a_2 \cdots a_{\phi(n)} \equiv a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv (a_1 a_2 \cdots a_{\phi(n)}) \pmod{n}$$

Thus $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Lemma. *Suppose $n = p^r$ for some prime p and $r \in \mathbb{N}$. Then*

$$\phi(n) = p^r - p^{r-1} = p^{r-1}(p-1) = n(1 - \frac{1}{p}) = n\frac{p-1}{p}.$$

Proof. We know that$\phi(n) = n$ minus the number of multiples of p less than n.

The number of multiples of p less than n is $\frac{n}{p}$ since $n = p^r$. Then $\phi(n) = n - \frac{n}{p} = n(1 - \frac{1}{p}) = n\frac{p-1}{p}$. □

Lemma. *If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. By the Chinese Remainder Theorem, there is a bijection between $a \pmod{mn}$ and $(a_1 \pmod{m}, a_2 \pmod{n})$, where

$$\begin{cases} a \equiv a_1 \pmod{m} \\ a \equiv a_2 \pmod{n} \end{cases}$$

Then $\gcd(a, mn) = 1 \iff \gcd(a_1, m) = 1 \wedge \gcd(a_2, n) = 1$.

There are $\phi(m)$ choices for a_1 and $\phi(n)$ choices for a_2.

Then there are $\phi(m)\phi(n)$ choices for a.

Then $\phi(mn) = \phi(m)\phi(n)$. □

5.3.4 Find the ϕ function

Theorem 16. *Let $n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ be the prime factorization of n where $p_1, p_2, \ldots, p_k$ are distinct primes and $r_1, r_2, \ldots, r_k$ are positive integers.*

Then

$$\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k}) = p_1^{r_1-1}(p_1-1)p_2^{r_2-1}(p_2-1)\ldots p_k^{r_k-1}(p_k-1)$$

Basically, it is a direct application of the previous 2 lemmas.

Proof. Using the previous phi morphism lemma and phi power lemma recursively, we can find that

$$\phi(n) = \phi(p_1^{r_1})\phi(p_2^{r_2})\dots\phi(p_k^{r_k}) = p_1^{r_1-1}(p_1-1)p_2^{r_2-1}(p_2-1)\dots p_k^{r_k-1}(p_k-1)$$

□

For example: $\phi(100) = \phi(2^2)\phi(5^2) = 2^1(2-1)5^1(5-1) = 40$.

Note that we need the prime decomposition of n to find $\phi(n)$. Otherwise, it is hard to find $\phi(n)$ directly.

5.3.5 More on ϕ funciton

Theorem 17. $\sum_{d|n}\phi(d) = n$.

Here the sum is taken over all positive divisors of n.

Note the use of the formula with the prime decomposition of n:

$$\phi(n) = p_1^{r_1-1}(p_1-1)p_2^{r_2-1}(p_2-1)\dots p_k^{r_k-1}(p_k-1)$$

For example: $n = 6$ then $\sum_{d|6}\phi(d) = \phi(1)+\phi(2)+\phi(3)+\phi(6) = 1+1+2+2 = 6$.

For example: $n = 12$ then $\sum_{d|12}\phi(d) = \phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12) = 1+1+2+2+2+4 = 12$.

For example: $n = 81 = 3^4$ then $\sum_{d|81}\phi(d) = \phi(1)+\phi(3)+\phi(9)+\phi(27)+\phi(81) = 1+2+6+18+54 = 81$.

Now try to prove it:

Proof. Subdivide the integers $[0, n-1]$ into classes C_e where $C_e = \{x \in [0, n-1] : \gcd(x, n) = e\}$ for $e = 1, 2, \dots, n$. Note that $|C_e| = \phi(e)$ since $x \in C_e \iff \gcd(x, n) = e$.

More generally, the number of elements in C_e is $\phi(\frac{n}{e})$.

It is because $\gcd(x, n) = e \iff e|n \wedge e|x \iff \gcd(\frac{x}{e}, \frac{n}{e}) = 1$. Then the number of elements in C_e is $\phi(\frac{n}{e})$.

Since the classes C_e are disjoint and their union is $[0, n-1]$, then $|C_1|+|C_2|+\dots+|C_n| = n$. Then we conclude

$$n = \sum_{e|n}|C_e| = \sum_{e|n}\phi(\frac{n}{2}) = \sum_{d|n}\phi(d)$$

Here $d = \frac{n}{e}$ ranges over the positive divisors of n. □

To illustrate the proof, consider $n = 12$. Then

$$\begin{aligned} C_{12} &= \{0\} & \phi(\frac{12}{12}) &= 1 \\ C_6 &= \{6\} & \phi(\frac{12}{6}) &= 2 \\ C_4 &= \{4, 8\} & \phi(\frac{12}{4}) &= 2 \\ C_3 &= \{3, 9\} & \phi(\frac{12}{3}) &= 2 \\ C_2 &= \{2, 10\} & \phi(\frac{12}{2}) &= 2 \\ C_1 &= \{1, 5, 7, 11\} & \phi(\frac{12}{1}) &= 4 \end{aligned}$$

Then $|C_{12}| + |C_6| + |C_4| + |C_3| + |C_2| + |C_1| = 1 + 1 + 2 + 2 + 2 + 4 = 12$.

Note that how the sets are disjoint.

5.4 Multuplicative

The Euler ϕ function is multiplicative. That is, if $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Here "arithmetic" means defined on the set of positive integers, "multiplicative" means $f(mn) = f(m)f(n)$ for all m, n such that $\gcd(m, n) = 1$.

Lemma. *If $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ is the prime factorization of n where $p_1, p_2, \dots, p_k$ are distinct primes and $r_1, r_2, \dots, r_k$ are positive integers, then*

$$f(n) = \prod_{i=1}^{k} f(p_i^{r_i})$$

This can be proved by recursively applying the multiplicative property of $f(n)$.

Theorem 18. *If $f(n)$ is a multiplicative arithmetic function, then so is $F(n) = \sum_{d|n} f(d)$.*

Here the sum is taken over all positive divisors of n.

Example: If $f(n)$ is the Euler ϕ function, then $F(n) = \sum_{d|n} \phi(d) = n$ by the previous theorem

Proof. Consider the prime decomposition os $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $n = q_1^{b_1} q_2^{b_2} \dots q_l^{b_l}$ where $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$ are distinct primes and $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_l$ are positive integers given that $\gcd(m, n) = 1$.

Any divisor d of mn has a subset of $\{p_1, \dots, p_k, q_1, \dots, q_l\}$ as its prime factors.

- Collect the p_i's into a set A and let the product of the elements in A be d_1.
- Collect the q_i's into a set B and let the product of the elements in B be d_2.

Now $d = d_1 d_2, d_1 | m, d_2 | n$. Moreover, d_1 and d_2 are relatively prime, uniquely determined by d.

Then $F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) = \sum_{d_1|m, d_2|n} f(d_1) f(d_2) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = F(m)F(n)$.

It shows that $F(n)$ is multiplicative. □

Corollary. *The following two arithmetic functions are multiplicative:*

$\sigma(n) =$ *sum of all positive divisors of* n.

$\tau(n) =$ *number of positive divisors of* n.

Example: $n = 100 = 2^2 \times 5^2$.

Then $\sigma(100) = \sigma(2^2)\sigma(5^2) = (1 + 2 + 4)(1 + 5 + 25) = \frac{2^3 - 1}{2 - 1} \frac{5^3 - 1}{5 - 1} = 217$.

$\tau(100) = \tau(2^2)\tau(5^2) = 3 \times 3 = 9$.

Proof. If $f(n) = 1$, then $F(n) = \sum_{d|n} f(d) = \tau(n)$.

If $f(n) = n$, then $F(n) = \sum_{d|n} d = \sigma(n)$. □

Knowing that $F(n)$ is multiplicative, we can write $F(n) = \prod_{i=1}^{k} F(p_i^{r_i})$ where $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ is the prime factorization of n.

This is by using the multiplicative property of $F(n)$ and the prime factorization of n.

It leads to the following formula:

$$\tau(n) = \prod_{i=1}^{k} \tau(p_i^{r_i}) = (r_1 + 1)(r_2 + 1) \dots (r_k + 1)$$

This is because $\tau(p_i^{r_i}) = r_i + 1$, which is the number of divisors of $p_i^{r_i}$. Divisors of $p_i^{r_i}$ are $1, p_i, p_i^2, \dots, p_i^{r_i}$.

5.5 Perfect numbers

Theorem 19. *Let n be a positive integer. Then n is a perfect number if and only if $\sigma(n) = 2n$.*

Equivalently, n is the sum of its proper divisors.

For example: $n = 6$ is perfect because $\sigma(6) = 1 + 2 + 3 + 6 = 12 = \frac{2^2-1}{2-1} = \frac{3^2-1}{3-1} = 2 \times 6$.Or the other way: the proper divisors of 6 are 1,2,3. Then $1 + 2 + 3 = 6$.

Theorem 20. *Suppose $m \geq 2$ is a prime and $p = 2^m - 1$ is also a prime. Then $n = 2^{m-1}p$ is a perfect number.*

Proof. $\sigma(n) = \sigma(2^{m-1})\sigma(p) = \frac{2^m-1}{2-1}\frac{p^2-1}{p-1} = (2^m - 1)(p + 1) = 2^m p = 2n$ □

Lemma. *If $2^m - 1$ is prime, then m is prime.*

Proof. If $m = ab$ is composite, $a, b \geq 2$, then $2^m - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1)$ is also composite. □

However, it does not work the other way around. If m is prime, $2^m - 1$ may or may not be prime.

In fact only 51 **Mersenne prime** is known, largest known is $2^{82589933} - 1$.

$p = 2$	$\implies 2^2 - 1 = 3$	Mersenne prime
$p = 3$	$\implies 2^3 - 1 = 7$	Mersenne prime
$p = 5$	$\implies 2^5 - 1 = 31$	Mersenne prime
$p = 7$	$\implies 2^7 - 1 = 127$	Mersenne prime
$p = 11$	$\implies 2^{11} - 1 = 2047 = 23 \times 89$	Composite
$p = 13$	$\implies 2^{13} - 1 = 8191$	Mersenne prime
$p = 17$	$\implies 2^{17} - 1 = 131071$	Mersenne prime
$p = 19$	$\implies 2^{19} - 1 = 524287$	Mersenne prime
$p = 23$	$\implies 2^{23} - 1 = 47 \times 178481$	Composite
$p = 29$	$\implies 2^{29} - 1 = 233 \times 1103 \times 2089$	Composite
$p = 31$	$\implies 2^{31} - 1 = 2147483647$	Mersenne prime

Theorem 21. *Even numbers of the form $n = 2^{m-1}(2^m - 1)$ where $2^m - 1$ is prime are perfect numbers.*

*Prime numbers of the form $2^m - 1$ are called **Mersenne primes**.*

5.5.1 Euler's Perfect Number Theorem

Theorem 22. *Let n be an even perfect number, then there exists a prime number $m \geq 2$ such that $n = 2^{m-1}(2^m - 1)$ and $2^m - 1$ is prime.*

Proof. Write $n = 2^s t$ where t is odd. Our goal is to show that $t = 2^{s+1} - 1$ is prime. Note that if we set $m = s + 1$, then $n = 2^{m-1}t$ and $2^m - 1 = t$. We can do it since n is even, $s \geq 1$ and t is odd.

Since n is perfect, then $\sigma(n) = 2n$. Then $\sigma(n) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t) = 2n = 2^{s+1}t$.

We conclude that $2^{s+1}|\sigma(t)$ since $2^{s+1} - 1$ and 2^{s+1} are relatively prime. Then $\sigma(t) = 2^{s+1}q$ for some $q \in \mathbb{N}$.

Substitute it in we obtain $(2^{s+1} - 1)q = t$. Thus $1 \leq q < t, q|t$.

Claim that $q = 1$. If $q > 1$, then t has a proper divisor q such that $q < t$. Then $\sigma(t) \geq 1 + q + t = 2t + q > 2t$. On the other hand, $\sigma(t) = 2^{s+1}q = q + t$ since $(2^{s+1} - 1)q = t$. Then we have a contradiction.

Therefore $q = 1$ and $t = 2^{s+1} - 1$ is prime. Moreover, $\sigma(t) = 2^{s+1}q = 2^{s+1} = t + 1$

So t is a prime. In Summary, $n = 2^{s+1} - 1$ is prime and $n = 2^{s+1}(2^{s+1} - 1)$. □

Euler's Theorem shows that the problems of finding all even perfect numbers and finding all Mersenne primes are equivalent.

5.5.2 Mobius Inversion Formula

Let $f(n)$ be a multiplicative function. We know that $F(n) = \sum_{d|n} f(d)$ is also multiplicative. Can we recover $f(n)$ from $F(n)$?

Mobius function: $\mu(n) = \begin{cases} 0 & \text{if } n \text{ has a square factor} \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \end{cases}$

In particular, $\mu(1) = 1$, since 1 is a product of 0 distinct primes.

Let the prime decomposition of n be $n = p_1^{a_1} \cdots p_r^{a_r}$, then $\mu(n) = 0$ if $\exists a_i \geq 2$ for some i and $\mu(n) = (-1)^r$ if n is a product of r distinct primes where $a_i = 1$ for all i.

Mobius Inversion Formula:

$$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d})$$

For example: $f(n) = 1$ for every n, then $F(n) = \sum_{d|n} 1 = \tau(n)$ which is the number of positive divisors of n. By the inversion formula, $\sum_{d|n} \tau(d)\mu(\frac{n}{d}) = 1$.

Similarly, taking $f(n) = n$, we obtain $F(n) = \sum_{d|n} d = \sigma(n)$. It is the sum of the positive divisors of n. Then $\sum_{d|n} \sigma(d)\mu(\frac{n}{d}) = n$.

Lemma. *$\mu(n)$ is multiplicative.*

Proof. Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $m = q_1^{b_1} q_2^{b_2} \dots q_l^{b_l}$ where $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$ are distinct primes and $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_l$ are positive integers. We can do that since $\gcd(m, n) = 1$.

Then $\mu(nm) = \begin{cases} 0 & \text{if } n \text{ has a square factor} \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \end{cases}$

Where is my real proof?

Then $\mu(nm) = \mu(n)\mu(m)$. □

Lemma. *If n is a positive integer, then*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Proof. Let $M(n) = \sum_{d|n} \mu(d)$. Then $M(1) = \mu(1) = 1$.

Note that $M(n)$ is multiplicative.

If $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then $M(n) = \sum_{d|n} \mu(d) = \prod_{i=1}^{k} M(p_i^a)$

Observe that for any $M(p^a) = \sum_{d|p^a} = 1 + (-1) + 0 + \dots + 0 = 0$ if $a > 1$ and $M(p) = 1 - 1 = 0$ if $a = 1$.

Then $M(n) = 0$ if $n > 1$. □

Now come back to the Mobius Inversion Formula. We can write it as

$$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d}) = \sum_{d|n} F(\frac{n}{d})\mu(d)$$

Proof. The idea is to change the order of summation. Note that $F(\frac{n}{d}) = \sum_{e|\frac{n}{d}} f(e)$.

Then

$$f(n) = \sum_{d|n} F(\frac{n}{d})\mu(d) = \sum_{d|n} \sum_{e|\frac{n}{d}} f(e)\mu(d) = \sum_{e|n} \sum_{d|\frac{n}{e}} f(e)\mu(d) = \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d)$$

□

5.6 Primality Testing

Given a positive integer n, how can we determine whether n is prime?

- factoring means n into a product of ab where $1 < a, b < n$.
- testing n for primality means checking whether n has any divisors other than 1 and n. In other words, check whether or not a factorization of n exists.

There are fast tests for primality but no fast factorization algorithms are known. This discrepancy is the foundation for RSA cryptography.

5.6.1 Fermat's Primality Test

One way to know if a number is not prime is to find a witness to its compositeness.

If there exisits an integer b in $[1, n-1]$ such that $b^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime.

We can do it fast since we can do repeating squaring to find b^{n-1} in $O(\log n)$ time.

Note that we cannot compute b^{n-1} using Euler's Theorem since we do not know the prime factorization of n.

So if b exists we know something, but we cannot find it.

Example: $n = 15, b = 2$. Then $2^{15-1} = 2^{14} \equiv 2^{4\times3+2} \equiv 16^3 \times 2^2 \equiv 4 \pmod{15}$. Then 15 is not prime.

Claim: n is **pseudo-prime** to base b if $b^{n-1} \equiv 1 \pmod{n}$.

A pseudo prime of 1 base does not imply it is a prime for all bases. For example, 341 is a pseudo prime to base 2, but it is not a prime.

$$2^{341-1} \equiv 2^{340} \equiv 1 \pmod{341}$$

while $341 = 11 \times 31$.

Proof. By CRT, we can show that $\begin{cases} 2^{341-1} \equiv 1 \pmod{11} \\ 2^{341-1} \equiv 1 \pmod{31} \end{cases}$ □

By Fermat's Little Theorem:

$$\begin{aligned} 2^{10} \equiv 1 \pmod{11} &\implies 2^{340} \equiv 1 \pmod{11} \\ 2^{5} \equiv 1 \pmod{31} &\implies 2^{340} \equiv 1 \pmod{31} \end{aligned}$$

We can find that 341 is not a pseudo prime to base 3.

$$3^{340} \equiv (3^{30})^{11} \times 3^{10} \equiv 1^{11} \times 3^{10} \equiv 3^{10} \equiv 3^{3^3} \times 3 \equiv (-4)^3 \times 3 \equiv 25 \pmod{341}$$

Procedure for Fermat's Primality Test:

1. Choose a random integer b in $[2, n-2]$.
2. Compute $b^{n-1} \pmod{n}$.
3. If $b^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime.
4. If $b^{n-1} \equiv 1 \pmod{n}$, then n is a pseudo prime to base b.
5. Repeat the test with a different b.
6. If n is a pseudo prime to enough bases, then n is **probably** prime.
7. It is possible that n is a pseudo prime to all bases and still not prime. Such numbers are called **Carmichael numbers**.

Note that it is a probabilistic test instead of an extensive test. It is not possible to go through all the bases to test the primality of a number.

5.6.2 Carmichael Numbers

Proposition. *Suppose $n = p_1 p_2 \cdots p_r$ where $p_1, p_2, \ldots, p_r$ are distinct primes. If $p_i - 1 \mid n - 1$ for all i, then n is a Carmichael number.*

Proof. Let b be any integer not divisible by $p_i, \forall i$. In other words, $\gcd(b, n) = 1$. Then by Fermat's Little Theorem, $b^{p_i - 1} \equiv 1 \pmod{p_i}$. Then $b^{n-1} \equiv 1 \pmod{p_i}$.

Then $b^{n-1} \equiv 1 \pmod{p_i}$ for all i.

Let $x = b^{n-1} - 1$. Then $x \equiv 1 \pmod{p_i}, \forall i$. By Chinese remainder theorem, $x \equiv 1 \pmod{n}$. Then $b^{n-1} \equiv 1 \pmod{n}$.

Then n is a Carmichael number. □

For example $561 = 3 \times 11 \times 17$. Then $3 - 1, 11 - 1, 17 - 1 \mid 561 - 1$. Then 561 is a Carmichael number.

Another example: $6601 = 7 \times 23 \times 41$. Then $7 - 1, 23 - 1, 41 - 1 \mid 6601 - 1$. Then 6601 is a Carmichael number.

5.6.3 Miller-Rabin Primality Test

The Miller-Rabin Primality Test is a more efficient probabilistic primality test than Fermat's Primality Test. It is a refined version of Fermat's Primality Test which captures the idea of Carmichael numbers.

Say we want to test n for primality.

1. Start out the same way as Fermat's Primality Test. Choose a random integer b in $[2, n-2]$. Then compute $b^{n-1} \pmod{n}$.
2. If $b^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime.
3. If $b^{n-1} \equiv 1 \pmod{n}$, then we probe a bit deeper by computing $x \equiv b^{(n-1)/2} \pmod{n}$. (Here we are assuming that $n-1$ is even. If $n-1$ is odd, then n is not prime since $b \geq 2$)
4. Note that $x^2 = b^{n-1} \equiv 1 \pmod{n}$. If n is a prime, then $x \equiv \pm 1 \pmod{n}$.
5. If $x \equiv 1 \pmod{n}$, and $\frac{n-1}{2}$ is odd, We cannot say anything here, pick another b and repeat the test.
6. If $x \equiv -1 \pmod{n}$, then n is **probably** prime. We cannot say anything here, pick another b and repeat the test.
7. However, if $x \equiv 1 \pmod{n}$, and $\frac{n-1}{2}$ is even, then we can dig deeper by computing $y \equiv b^{(n-1)/4} \pmod{n}$.
8. Same idea: If $y \equiv -1 \pmod{n}$, or $y \equiv 1 \pmod{n}$ and $\frac{n-1}{4}$ is odd, then pick another b and repeat the test.
9. If $y \equiv 1 \pmod{n}$, and $\frac{n-1}{4}$ is even, then repeat checking.
10. The only stop criterion is when we conclude that n is composite.
11. We never conclude with 100% certainty that n is prime. We can only say that n is **probably** prime. It is a probabilistic test!

Use the smallest Carmichael Number 561 again. Perform the Miller-Rabin Primality Test with $b = 5$:

- $5^{560} \equiv 1 \pmod{561}$.

- $5^{280} \equiv 67 \pmod{561}$. (By performing repeating squaring, a pain to do but the easiest method we can find already)

Note that $561 = 3 \times 11 \times 17$.

- Assume $\gcd(b, 561) = 1$.
- $b^{280} \equiv (b^2)^{140} \equiv 1 \pmod{3}$
- $b^{280} \equiv (b^{10})^{28} \equiv 1 \pmod{11}$
- $b^{280} \equiv b^8 \pmod{17}$
- When $b = 5$, $5^{280} \equiv 5^8 \equiv 25^4 \equiv 8^4 \equiv 64^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$
- Now with CRT: $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{11} \\ x \equiv -1 \pmod{17} \end{cases} \implies x \equiv 67 \pmod{561}$

5.6.4 Rabin's Theorem

Theorem 23. *Fix a composite integer n. Pick $a, b \in [2, n-2]$ at random. Then the probability that n fails Miller's test is greater than or equal to $\frac{1}{4}$.*

In other words, Miller's test will detect that n is composite with probability at least $\frac{1}{4}$ for all possible choices

Equivalently, if we run Miller's test k times, with k different choices of b, and n passes each of the test, then the probability that n is composite is less than or equal to $(\frac{3}{4})^k$.

5.7 Pollard's Factorization Method

Goal: Factor a given (large) integer n.

1. Choose $r_0 \equiv 2^{0!} \pmod{n}$.
2. Compute the next one using the formula $r_k \equiv r_{k-1}^k \pmod{n}$.
3. For each k compute $\gcd(r_k - 1, n) = g_k$. Note that $1 \leq g_k \leq r_{k-1} \leq n - 2$ and g_k divides n.

4. For each k So if $g_k > 1$, then we have found a factor of n which is greater than 1.

5. Repeat the process till we find a factor of n.

The idea here is that if n has a prime factor p such that $p-1$ divides $k!$, then $2^{k!} \equiv 1 \pmod{p}$. By Fermat's theorem, $2^{k!} \equiv 1 \pmod{n}$ and $g_k > 1$.

In ohter words, p divides both $r_k - 1$ and n implies that p divides $g_k = \gcd(r_k - 1, n)$.

The method works well if $p-1 \mid k!$ for some prime factor p of n for small k. Informally, this means that $p-1$ has "small" prime factors. Thus the weakness of this algorithm is that we do not know which k will work.

5.7.1 Example

Factor 689 using Pollard's method:

$$\begin{aligned}
r_1 &\equiv 2 \pmod{689} & \gcd(r_1 - 1, 689) &= 1 \\
r_2 &\equiv 2^2 \equiv 4 \pmod{689} & \gcd(r_2 - 1, 689) &= 1 \\
r_3 &\equiv 4^3 \equiv 64 \pmod{689} & \gcd(r_3 - 1, 689) &= 1 \\
r_4 &\equiv 64^4 \equiv 66 \pmod{689} & \gcd(r_4 - 1, 689) &= 13 \\
\gcd(65, 689) &= 13 & 689 &= 13 \times 53
\end{aligned}$$

Factor 10403:

$$\begin{aligned}
r_2 &\equiv 2^2 \equiv 4 \pmod{10403} & \gcd(r_2 - 1, 10403) &= 1 \\
r_3 &\equiv 4^3 \equiv 64 \pmod{10403} & \gcd(r_3 - 1, 10403) &= 1 \\
r_4 &\equiv 64^4 \equiv 7580 \pmod{10403} & \gcd(r_4 - 1, 10403) &= 1 \\
r_5 &\equiv 7580^5 \equiv 4438 \pmod{10403} & \gcd(r_5 - 1, 10403) &= 1 \\
r_6 &\equiv 4438^6 \equiv 6862 \pmod{10403} & \gcd(r_6 - 1, 10403) &= 1 \\
r_7 &\equiv 6862^7 \equiv 137 \pmod{10403} & \gcd(r_7 - 1, 10403) &= 1 \\
r_8 &\equiv 137^8 \equiv 196 \pmod{10403} & \gcd(r_8 - 1, 10403) &= 1 \\
r_9 &\equiv 196^9 \equiv 3619 \pmod{10403} & \gcd(r_9 - 1, 10403) &= 1 \\
r_{10} &\equiv 3619^{10} \equiv 9798 \pmod{10403} & \gcd(r_{10} - 1, 10403) &= 101 \\
\gcd(9799, 10403) &= 101 & 10403 &= 101 \times 103
\end{aligned}$$

$p = 101$ is a prime factor of 10403. Then $p - 1 = 100$. Then $100 = 2^2 5^2 \mid 10!$. Then $p - 1 \mid 10!$ when $k = 10$.

6 Cryptography

A cryptosystem consists of:

- A set 'P' of possible **plaintexts**. (unencrypted messages)
- A set 'C' of possible **ciphertexts**. (encrypted messages)
- An enciphering function/transmission f that maps P into C. f should be a bijection.
- A deciphering function g that maps C into P. g should be the inverse of f. $g \circ f(x) = x$ for all $x \in P$.
- P and C usually consist of integers or congruence classes mod n for some n.

In a **classical cryptography** system, both f and f^{-1} are unknown to the public. The security of the system depends on the secrecy of f and f^{-1}. Knowing one can get the other.

In a **public key cryptosystem**, f is public and f^{-1} is private. The security of the system depends on the difficulty of computing f^{-1} from f.

First example: $P = C = \{0, 1, \ldots, 25\} = \mathbb{Z} \pmod{26}$. This corresponds to the 26 letters of the English alphabet.

$f(x) = x + b \pmod{26}$ for some $b \in \mathbb{Z} \pmod{26}$. b is the key. It is called shift cipher, b is both the encryption and decryption key.

6.1 Classcial Cryptography

6.1.1 Shift Cipher

Consider the shift cipher $P = C = \mathbb{Z}_n$

$f(x) = x + b \pmod{n}$	Encryption key b
$g(x) = x - b \pmod{n}$	Decryption key b

Since there are 26 letters in the English alphabet, we can set $n = 26$.

$P = C = \mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$. Then $f(x) = x + b \pmod{26}$ and $g(x) = x - b \pmod{26}$.

6.1.2 Breaking cryptosystems

To break a cryptosystem, one needs two types of information:

- The general nature of the system: P, C, f, g.
- The specific key used in the system.

We usually assume that the cryptanalyst knows the general nature of the system but not the specific key.

One way of breaking shift cipher is to use frequency analysis. The frequency of letters in English text is not uniform. For example, the letter 'e' is the most common letter in English text.

Let's say we are given a ciphertext "FQOCUDEM", then we try encryption function $f : E \to$ for each of the letters in the text.

$$f : E \to U \implies b = 16 \qquad \text{FQOCUDEM} \to \text{PAYMENOW}$$

6.1.3 Affine Cipher

The affine cipher is a generalization of the shift cipher. It is a type of monoalphabetic substitution cipher. It is a combination of shift and multiplication.

$P = C = \mathbb{Z}_{26}$. Let $a, b \in \mathbb{Z}_{26}$ with $\gcd(a, 26) = 1$. Then $f(x) = ax + b \pmod{26}$ and $g(x) = a^{-1}(x - b) \pmod{26}$.

Note that a^{-1} exists if and only if $\gcd(a, 26) = 1$. To solve for a^{-1}, we can use the Euclidean algorithm and back substitution. $as + a^{-1}t \equiv 1 \pmod{26}$.

To break it, we can try to use frequency analysis again:

$$f(x) = ax + b \pmod{26} \qquad g(x) = a^{-1}(x - b) \pmod{26}$$

For example, let's break a ciphtertext where the most frequent letters are 'K' and 'D'. In English, the most frequent letters are 'E' and 'T'. Then we can try to find a, b such that $f(K) = E$ and $f(D) = T$.

Now we need to solve the system of equations:

$$\begin{aligned} g : K(10) \to E(4) \qquad & 10c + d \equiv 4 \pmod{26} \\ g : D(3) \to T(19) \qquad & 3c + d \equiv 19 \pmod{26} \end{aligned}$$

Want to solve the system of linear congruence for c, d.

Subtract both equations to eliminate d to get $7c \equiv 11 \pmod{26}$. Then $c \equiv 7^{-1} \cdot 11 \equiv 9 \pmod{26}$. Then $d \equiv 4 - 10 \cdot 9 \equiv 20 \pmod{26}$.

Then $f(x) = 9x + 20 \pmod{26}$ and $g(x) = 15(x - 20) \pmod{26}$.

Another example: $n = 28$. Elements corresponds to $\mathbb{Z}_{28}$ where $0 \to 25 \implies$ 'A'$\to$'Z', $26 \to$ ' ' (space), $27 \to$ '?'.

Suppose the most frequent letters are 'B' and '?'. By frequency analysis, most frequent should be ' ' and 'E'.

So $1 \to 26, 27 \to 4$. We need to solve for

$$\begin{aligned} c + d &\equiv 26 \pmod{28} \\ 27c + d &\equiv 4 \pmod{28} \end{aligned}$$

Subtract both sides, we get $26c \equiv -22 \pmod{28}$. Then $2c \equiv 22 \pmod{28}$. Note that $\gcd(2, 22) = 2$ so 2 does not have an inverse modulo 28. We have two possible solutions for it.

Solve for $c \equiv 11 \pmod{\frac{28}{22}}$ to get $c_1 = 11, c_2 = 11 + 14 = 25$. Then $d_1 \equiv 26 - 11 \equiv 15 \pmod{28}$ and $d_2 \equiv 26 - 25 \equiv 1 \pmod{28}$.

We try both to see which works better.

6.2 Exponentiation Cipher

Here $P = C = \mathbb{Z}_p$ where p is a prime number.

- Encryption: $f(x) = x^e \pmod{p}$ where e is the encryption key.
- Decryption: $g(x) = x^d \pmod{p}$ where d is the decryption key.
- Note the range is $\mathbb{Z}_p$.

This requires that $g(f(x)) = x$ for all $x \in \mathbb{Z}_p$. For example, $(x^e)^d \equiv x^{ed} \equiv x \pmod{p}$.

Lemma. $de \equiv 1 \pmod{p-1} \implies g(f(x)) = x$ *for all* $x \in \mathbb{Z}_p$.

Proof. It follows one of the corollaries from Fermat's Little Theorem. $m \equiv n \pmod{p-1} \implies x^m \equiv x^n \pmod{p}$. □

Note that it requires that e, d are inverses modulo $p - 1$. To make sure that an inverse exists, we need to make sure that $\gcd(e, p - 1) = 1$. Then we can get $d = e^{-1} \pmod{p-1}$.

For example, $p = 29$, $e = 5$. Then $f(x) = x^5 \pmod{29}$ and $g(x) = x^{17} \pmod{29}$ given by:

$$5a \equiv 1 \pmod{28}$$
$$17 \equiv 5^{-1} \pmod{28} \text{ by Euclidean algorithm}$$

Then decoding can be done by repetitively squaring. For example, to decode $f(3) = 3^5 \pmod{29}$, we can do $3^5 \equiv 3^{1+4} \equiv 3 \cdot 3^4 \equiv 3 \cdot 81 \equiv 243 \equiv 3 \pmod{29}$.

6.2.1 Breaking Exponentiation Cipher

Note that exponentiation cipher is slightly safer than affine cipher. It is not as easy to break by frequency analysis.

To break it, we need to solve congruences of the form $y^d \equiv x \pmod{p}$ for y. If $x, y \in \mathbb{R}$, d can be recovered by taking the discrete logarithm of x to the base y. This is called the discrete logarithm problem.

For large p, the problem is computationally difficult. For example, if p is a 1000-bit prime, then the discrete logarithm problem is computationally infeasible.

6.3 RSA Cryptosystem

RSA is a public key cryptosystem. It was invented by Rivest, Shamir, and Adleman in 1977. It is based on the difficulty of factoring large integers.

Each user chooses two large primes p and q and an encryption exponent e. The public key is (n, e) where $n = pq$ and e is the encryption exponent. Here we need $\gcd(e, \phi(n)) = 1$ where $\phi(n) = (p-1)(q-1)$.The private key is (n, d) where d is the decryption exponent.

- Encryption: $f(x) = x^e = y \pmod{n}$.
- Decryption: $g(y) = y^d = x \pmod{n}$. $d = e^{-1} \pmod{\phi(n)}$ where $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$.

Theorem 24. $x^{ed} \equiv x \pmod{n}$ *for all* $x \in \mathbb{Z}_n$.

The difference between RSA and the exponentiation cipher is that n is not prime. The security of RSA is based on the difficulty of factoring large integers.

Note that Euler's Theorem can only handle some cases since x might not be relatively prime to n.

To prove the theorem, we need to show that $ed \equiv 1 \pmod{\phi(n)}$. Then $x^{ed} \equiv x \pmod{n}$.

Need to show that $\begin{cases} y \equiv x \pmod{p} \\ y \equiv x \pmod{q} \end{cases}$. If we can do that then by CRT, we can show that $y \equiv x \pmod{n}$.

Proof. Given that $ed \equiv 1 \pmod{\phi(n) = (p-1)(q-1)}$. Then $\begin{cases} ed \equiv 1 \pmod{p-1} \\ ed \equiv 1 \pmod{q-1} \end{cases}$

Apply Corollary 2 of Fermat's theorem. $ed \equiv 1 \pmod{(p-1)(q-1)}$. Then $\begin{cases} ed \equiv 1 \pmod{p-1} \\ ed \equiv 1 \pmod{q-1} \end{cases} \implies \begin{cases} x^{ed} \equiv x^1 \pmod{p} \\ x^{ed} \equiv x^1 \pmod{q} \end{cases}$

Now apply CRT, we can show that $x^{ed} \equiv x \pmod{n}$. □

For example: $p = 281, q = 167, n = pq = 46927$. Let $(n, e) = (46927, 39423)$ as the public key. Transmit blocks of 3 letters: there are 26 letters, then there are $26^3 = 17576$ possible blocks.

If the message is "YES", which corresponds to 24, 4, 18. View them as a three digit number $(24, 4, 18)_{26}$ which is $24 \cdot 26^2 + 4 \cdot 26 + 18 = 16346$.

Encode will get me $16346^{39423} \pmod{46927} = 21166$ using repetitively squaring. Now separate the letter into base 26: $21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2$. Then decode it to get "BFIC".

To decipher, first need to find $d \equiv e^{-1} \pmod{\phi(n)}$. Here $\phi(n) = (p-1)(q-1) = 280 \cdot 166$. Using the Euclidean algorithm we can find $d = 26767$. Then $21166^{26767} \pmod{46927} = 16346$. Then decode it to get "YES".

Note that we can solve it here since we know both p and q. In practice, we do not know p and q.

6.4 Implementing RSA

6.4.1 Find large primes

To implement RSA, we need to find large primes. We can use the Miller-Rabin primality test to find large primes.

To get a prime about 200 digits long, we can pick integer x between 1 and 10^{200} and test if x is prime. If it is not, then we can try another x. According to the prime number theorem, the number of finding a prime is about $\frac{10^{200}}{\ln(10^{200})}$. This probability is about $\frac{1}{\ln(10^{200})} = \frac{1}{200\ln(10)} \approx \frac{1}{460}$. And we know we will only choose

x that is not divisible by $2, 3, 5, 7, 11$ since these can be found to be obviously wrong. So the probability is even higher.

Note that p, q should not be close to each other because of Fermat's factorization method. If p, q are close, then n is small and can be factored easily. Also, each $p-1.q-1$ should have large prime factors because of Pollard's factorization method.

6.4.2 Choosing encryption exponent

The encryption exponent e should be relatively prime to $\phi(n)$. Although we can choose at random and it might work, it is better to choose another large prime that is larger than p and q.

6.4.3 Procedure

1. Find large primes p and q in 200 digits range by Miller-Rabin primality test. Set $n = pq$.
2. Choose an encryption exponent e that is relatively prime to $\phi(n) = (p-1)(q-1)$. Now the public key is (n, e).
3. Use Euclidean Algorithm to find d such that $ed \equiv 1 \pmod{\phi(n)}$. Now the private key is (n, d). (Solve for $ex + \phi(n)y = 1$, then $d \equiv x \pmod{\phi(n)}$)
4. Encrypt the message by $f(x) = x^e \pmod{n}$.
5. Decrypt the message by $g(y) = y^d \pmod{n}$. Use repeated squaring to compute y^d.

6.5 Attacks on RSA

6.5.1 Fermat's Factorization Method

Want to factor n:

Let s range over the integers $> \sqrt{n}$ until $s^2 - n$ is a square. Then $s^2 - n = t^2$. Then $s^2 - t^2 = n$. Then $(s+t)(s-t) = n$. Then n is a product of $s+t$ and $s-t$. $s = \frac{p+q}{2}$ and $t = \frac{p-q}{2}$.

Number of steps to find s and t is about $s - \sqrt{n} = \frac{p+q}{2} - \sqrt{pq} = \frac{p-2\sqrt{pq}+q}{2} = \frac{(\sqrt{p}-\sqrt{q})^2}{2}$. s is small if p and q are close. But if $p >> q$, then $\approx \sqrt{p}$ steps are needed.

For example: Factor 5959 using Fermat's factorization method.

1. Find that $77 < \sqrt{5959} < 78$. Then $78 \leq s$.
2. $s = 78 \implies s^2 - n = 78^2 - 5959 = 125$. Not a square.
3. $s = 79 \implies s^2 - n = 79^2 - 5959 = 282$. Not a square.
4. $s = 80 \implies s^2 - n = 80^2 - 5959 = 441 = 21^2$. Then $s = 80, t = 21$.
5. Then $5959 = 80^2 - 21^2 = 101 \times 59$.
6. Then $p = 101, q = 59$.

Thus to keep RSA secure, p and q should be not close to each other. A good strategy might be to choose them a few digits apart.

One can also try to factor $n = pq$ using Pollard's factorization method. To be safe, need at least one of $p - 1, q - 1$ to have a large prime factor.

6.5.2 Chose ciphertext attack

We use the fact that:

$$(x_1 x_2)^e \equiv x_1^e x_2^e \pmod{n} \quad (y_1 y_2)^d \equiv y_1^d y_2^d \pmod{n}$$

Suppose we want to decrypt a cipher text message $M \pmod{n}$. We do not know the decryption key d. Choose a mask r such that $\gcd(r, n) = 1$. Now we need to convince the holder of the private key to decrypt $M \cdot r^e \pmod{n}$. Note that e is public.

Decrypted message is $(M \cdot r^e)^d \equiv M^d r \pmod{n}$. Now we can recover M by multiplying by $r^{-1} \pmod{n}$. Note how we choose r such that $\gcd(r, n) = 1$.

6.5.3 Small exponent attack

If e is small, then the encryption function $f(x) = x^e \pmod{n}$ can be broken by brute force. We can try to compute $\sqrt[e]{y*} \pmod{n}$ where $y* = x^e + kn \pmod{n}$ for some $k \in \mathbb{Z}$.

If e is small, there are a few k we need to try to find the correct x. For example, if $e = 3$, then we only need to try $k = 0, 1, 2$ to find the correct x.