Notes on Number Theory and Computation

Pramook Khungurn

December 11, 2019

1 Divisions

- If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$.

  When a divides b, we say that a is a *factor* of b and that b is a *multiple* of a.

  We use the notation $a \mid b$ to denote the fact that a divides b.

  For examples, $2 \mid 6$ and $7 \mid 14$.

- Let a and b be integers. Then

  1. if $a \mid b$ and $b \mid c$, then $a \mid c$;
  2. if $a \mid b$, then $a \mid bc$ for all integer c;
  3. if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

- **Division Algorithm:** Let a be an integer and d a positive integer. Then there are unique integers q and r such that $a = qd + r$ and $0 \leq r < d$.

  We call q the *quotient* and r the *remainder* of dividing a with d. For example, since $4649 = 110 \times 42 + 29$, we have that 110 is the quotient of dividing 4649 with 42, and 29 is the remainder.

  We use the notation $a \bmod b$ to denote the remainder of dividing a by b; i.e., $4649 \bmod 42 = 29$.

  With modern CPUs, you can compute quotients and remainders in $O(1)$ time. However, computing remainders is consider a very slow operating, consuming quite a lot of CPU cycles.

- An integer a is said to be a *common divisor* of b and c if $a \mid b$ and $b \mid c$.

  For example, 15 is a common divisor of 30 and 45.

- The *greatest common divisor* (GCD) of integers a and b, one of which is not zero, is the largest positive integer that is a common divisor of both a and b. We denote the GCD of a and b with the symbol $\gcd(a, b)$.

  For examples, $\gcd(30, 45) = 15$, $\gcd(2, 7) = 1$, and $\gcd(42, 39) = 3$.

- The GCD have the following properties:

  1. $\gcd(a, b) = \gcd(b, a)$;
  2. $\gcd(a, b) = \gcd(-a, b)$;
  3. $\gcd(a, b) = \gcd(|a|, |b|)$;
  4. $\gcd(a, 0) = |a|$;
  5. $\gcd(a, ka) = |a|$ for all integer k;
  6. (**) $\gcd(a, b)$ is the smallest positive integer in the set $\{ax + by : x, y \in \mathbb{Z}\}$ of *linear combinations* of a and b;

7. if d is a common divisor of a and b, then $d \mid \gcd(a, b)$;
8. $\gcd(na, nb) = n \gcd(a, b)$ for all positive integer n;
9. $\gcd(a, b) = \gcd(a, b + ax)$ for all x;
10. for all positive integer n, a, and b, if $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.

- *Exercise:* Let us prove the last property of GCD above.

  Since $\gcd(a, n) = 1$, we can find x and y such that $ax + ny = 1$. Now, $n = \gcd(n, ab) \leq \gcd(n, axb) \leq n$. So, it must be the case that $\gcd(n, axb) = n$ as well. Using Property 9, we have that

  $$n = \gcd(n, axb) = \gcd(n, axb + nyb) = \gcd(n, (ax + ny)b) = \gcd(n, b).$$

  This implies that $n \mid b$.

- **GCD Recursion Theorem:** If $b > 0$, then $\gcd(a, b) = \gcd(b, a \bmod b)$.

- **Euclid's algorithm** is an algorithm that computes the GCD of two non-negative integers. It makes use of the GCD recursion theorem to compute the GCD as follows:

  ```
  EUCLID(a, b)
  1  if b = 0
  2      then return a
  3      else return EUCLID(b, a mod b)
  ```

  For example,

  $$\begin{aligned}\textsc{Euclid}(4649, 42) &= \textsc{Euclid}(42, 29) = \textsc{Euclid}(29, 13) = \textsc{Euclid}(13, 3)\\ &= \textsc{Euclid}(3, 1) = \textsc{Euclid}(1, 0) = 1.\end{aligned}$$

  What is the time complexity of this algorithm? We know that, each time it is called,EUCLID spends $O(1)$ time deciding whether $b = 0$ and calculating $a \bmod b$. Thus, the running time depends on the number of times EUCLID is called recursively.

  The analysis of the running time of Euclid's algorithm involves the Fibonacci number F_k, defined as follow: $F_0 = 0$, $F_1 = 1$, and $F_k = F_{k-1} + F_{k-2}$ for all $k \geq 2$.

  Lemma 1.1. *If $a > b \geq 1$ and $\textsc{Euclid}(a, b)$ performs $k \geq 1$ recursive calls, then $a \geq F_{k+2}$ and $b \geq F_{k+1}$.*

  Proof. The proof is by induction on k. In the base case, $k = 1$, if $\textsc{Euclid}(a, b)$ performs 1 recursive call, then $b \neq 0$. So, $b \geq 1 = F_2$. Since $a > b$, we have that $a \geq 2 = F_3$. The base case is established.

  Inductively, assume the lemma is true if at least $k - 1$ calls are made. Consider a and b such that $\textsc{Euclid}(a, b)$ makes at least k recursive calls. This implies that $\textsc{Euclid}(b, a \bmod b)$ makes at least $k - 1$ recursive calls. This implies that $b \geq F_{k+1}$ and $(a \bmod b) \geq F_k$. Since $a = qb + (a \bmod b)$ for some $q \geq 1$, we have that

  $$a \geq b + (a \bmod b) \geq F_{k+1} + F_k = F_{k+2}.$$

  We have established the fact that $a \geq F_{k+2}$ and $b \geq F_{k+1}$. So, by induction, the lemma is true for all $k \geq 1$. □

  The contrapositive of the above lemma is the following theorem:

  Theorem 1.2 (Lamé's Theorem). *Let $k \geq 1$. If $a > b \geq 1$ and $b < F_{k+1}$, then $\textsc{Euclid}(a, b)$ performs fewer than k recursive calls.*

So what's the running time of EUCLID(a, b)? It is $O(k)$ where k is the smallest integer such that $F_{k+1} > b$. We know that $F_k \approx \phi^k/\sqrt{5}$, where $\phi = (1 + \sqrt{5})/2$. So, $k = O(\log b)$. That is, Euclid's algorithm runs in time *linear* in the number of bits used to represent the inputs. In other words, it is linear in the size of the input.

- **Extended Euclid's Algorithm:** We shall see later that it is sometimes useful not only to compute $\gcd(a, b)$ but to also compute x and y such that $\gcd(a, b) = ax + by$.

  Doing so by hand is quite easy. Let us compute $\gcd(48, 30)$:

$$\begin{aligned} 48 &= 1(30) + 18, \\ 30 &= 1(18) + 12, \\ 18 &= 1(12) + 6, \\ 12 &= 2(6). \end{aligned}$$

  Looking at two lines before the last, we have that $6 = 1(18) - 1(12)$ and $12 = 1(30) - 1(18)$. Substituting, we have that $6 = 1(18) - 1\big(1(30) - 1(18)\big) = -1(30) + 2(18)$. Looking at the first line, we have that $18 = 1(48) - 1(30)$. So, $6 = -1(30) + 2\big(1(48) - 1(30)\big) = 2(48) - 3(30)$. So $x = 2$ and $y = -3$.

  Let us codify the process we just went through a little bit. When we compute $\gcd(a, b)$ where $b \neq 0$, we compute $\gcd(b, r)$ where $r = a \bmod b$. Let us be wishful and assume that $\gcd(b, r)$ return x' and y' such that $bx' + ry' = \gcd(b, r) = \gcd(a, b)$. Then, let q be such that $a = qb + r$. We then have $r = a - qb$, and so

$$\gcd(a, b) = bx' + ry' = bx' + (a - qb)y' = ay' + (x' - qy')b.$$

  Thus, we can return $x = y'$ and $y = x' - qy'$.

  The remaining case is when $b = 0$. In this case, it is safe to return $x = 1$ and $y = 0$.

  Let us the above description into pseudocode.

```
EXTENDED-EUCLID(a, b)
1  if b = 0
2     then return (a, 1, 0)
3     else q ← ⌊a/b⌋
4          r ← a mod b
5          (d, x', y') ← EXTENDED-EUCLID(b, r)
6          return (d, y', x' − qy')
```

2 Modular Arithematic

- A *group* $(S, \oplus)$ is a set S together with a binary operation $\oplus : S \times S \to S$ with the following properties:

  1. *Identity:* There exists an element $e \in S$ called the *identity* of the group such that $e \oplus s = s \oplus e$ for all $s \in S$.
  2. *Associativity:* For all $a, b, c \in S$, we have $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
  3. *Inverses:* For all $a \in S$, there exists $b \in S$. called the *inverse* of a such that $a \oplus b = b \oplus a = e$.

  Examples of groups includes $(\mathbb{Z}, +)$ and $(\mathbb{R} - \{0\}, \times)$. What is the identity of $(\mathbb{R} - \{0\}, \times)$? What is the inverse of a in $(\mathbb{Z}, +)$?

- A group $(S, \oplus)$ is called an *abelian group* if, for all $a, b \in S$, $a \oplus b = b \oplus a$. In other words, $(S, \oplus)$ is abelian if $\oplus$ is commutative.

  $(\mathbb{Z}, +)$ and $(\mathbb{R}, \times)$ are abelian groups.

- Let n be a natural number. Let us consider the binary operation $+_n$ defined as follows: for any $a, b \in \mathbb{Z}$, $a +_n b = (a + b) \bmod n$.

  The operator $+_n$ and the set $\{0, 1, 2, \ldots, n-1\}$ forms a group called the *additive group modulo* n, and it is denoted by the symbol $\mathbb{Z}_n$.

  For example, in $\mathbb{Z}_6$, we have that $1 +_6 5 = 0$ and $4 +_6 5 = 3$.

- Two integers a and b are said to be *congruent modulo* m, for some positive integer m, if $m \mid (a - b)$. This fact is denoted by the symbol $a \equiv b \pmod{m}$.

  For examples, $10 \equiv 1 \pmod{3}$ and $-1 \equiv 14 \pmod{5}$.

- Congruence modulo m has the following properties:

  1. $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$;
  2. if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$;
  3. $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$;
  4. if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$;
  5. if $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for all non-negative integer k.

  Congruence is pretty much like equality. There's a catch though. In general, if $ac = bc$ and $c \neq 0$, then we know that $a = b$. However, this needs not be true in congruences. For example, we have that $2 \times 4 \equiv 4 \times 4 \pmod{8}$, but $2 \not\equiv 4 \pmod{8}$.

- **Recursive Squaring:** You are given an integer a, a non-negative integer k, and a positive integer m. You are asked to find b such that $0 \leq b < m$ and $a^k \equiv b \pmod{m}$; in other words, $a^k \bmod m$. What's an efficienty to compute this?

  Observe that

$$a^k \bmod m = \begin{cases} 1 & \text{if } k = 0, \\ (a^{k/2} \bmod m)^2 \bmod m, & \text{if } k \text{ is even}, \\ a(a^{(k-1)/2} \bmod m)^2 \bmod m, & \text{if } k \text{ is odd}. \end{cases}$$

  So, we can compute $a^k \bmod m$ by computing $a^{\lfloor k/2 \rfloor}$, squaring it, and multiply by a if k is odd. Putting the idea into pseudocode, we have

```
EXPONENT(a, k, m)
1  if k = 0
2      then return 1
3  elseif k is even
4      then e = EXPONENT(a, k/2, m)
5           return e^2 mod m
6  elseif k is even
7      then e = EXPONENT(a, (k − 1)/2, m)
8           return (ae^2) mod m
```

  The running time of this algorithm is $O(\log k)$.

- What's the solutions to the equation $ax \equiv b \pmod{n}$ for $a > 0$ and $n > 0$?

  First, let us determine if the equation has any solution at all. The equation is equivalent to the statement $n \mid (ax - b)$; in other words, there exist an integer y such that $ny = ax - b$ or $b = ax - ny$. That is, b is in the set of linear combinations of a and n. Using the properties of GCD two pages above, we conclude that b must be divisible by $\gcd(a, n)$.

Proposition 2.1. *The equation* $ax \equiv b \pmod{n}$ *is solvable if and only if* $\gcd(a, n) \mid b$.

Next, if the equation is solvable, what are the solutions then?

Let $d = \gcd(a, n)$. We can use EXTENDED-EUCLID(a, n) to find x' and y' such that $ax' + ny' = d$. Multiplying both sides by b/d, we have $a((b/d)x') + n((b/d)y') = b$, which means $a((b/d)x') \equiv b \pmod{n}$. Hence, $x = (b/d)x'$ is a solution.

If the equation is solvable, then there are infinitely many solutions. For each integer i, observe that

$$a((b/d)x' + i(n/d)) + n((b/d)y' - i(a/d)) = a((b/d)x') + n((b/d)y') + an/d - an/d = b.$$

So, $(b/d)x' + i(n/d)$ is a solution for all i. We shall show that these are all the solutions.

Observe that if x is a solution, then $x + i(n/d)$ is also a solution. Thus, if there are solutions other than $(b/d)x' + i(n/d)$, then there must be one solution which is equal to $(b/d)x' + k$, where $k < n/d$. So, assume by way of contradiction that such a k exists. We have that $a((b/d)x' + k) \equiv b \pmod{n}$, which implies $ak \equiv 0 \pmod{n}$; in other words, $n \mid ak$. would imply that n/d has to divide $(a/d)k$. Since $\gcd(n/d, a/d) = 1$, n/d must divides k. However, $k < n/d$ so this is impossible. Contradiction.

Theorem 2.2. *Let* x' *and* y' *are integers such that* $\gcd(a, n) = ax' + ny'$. *Suppose that the equation* $ax \equiv b \pmod{n}$ *is solvable. Then, all the solutions of this equation can be written as* $(b/d)x' + i(n/d)$ *for some* $i \in \mathbb{Z}$.

Collorary 2.3. *If* $\gcd(a, n) = 1$, *then the equation* $ax \equiv 1 \pmod{n}$ *has a unique solution modulo* n. *(In other words, there exists one and only one* x *such that* $0 \leq x < n$ *and* x *satisfies the equation.)*

- For integer a and positive integer n, a *multiplicative inverse modulo* n of a is an integer such b that $ab \equiv 1 \pmod{n}$.

  From the above corollary, we know that the multiplicative inverse is unique modulo n. We let a^{-1} denotes the unique inverse modulo n of a.

- Two integers a and b, both not 0, are *relatively prime* if $\gcd(a, b) = 1$.

  Integers $a_1, a_2, \ldots, a_k$, none of them 0, are *pairwisely relatively prime* if $\gcd(a_i, a_j) = 1$ for all i, j.

  For example, 6, 5, and 143 are pairwisely relatively prime.

  The nice property of mutually relatively prime set of integers is that, if you pick any two numbers from the set, say x and y, then you can always find x^{-1} modulo y and y^{-1} modulo x. More generally, you can partition the set into two sets, and the products of the numbers in the two sets are relatively prime.

- Consider the following question. A brigade of marines has x soldiers. If the commander makes them line up so that there are 3 soldiers in each row, the last row has 2 soldiers. If the commander makes them line up so that there are there are 4 soldiers in each row, the last row has 1 soldiers. If the commander makes them line up so that there are 5 soldiers in each row, the last row has 3 soldiers. What's the minimum number of soldiers in this brigade?

  This type of question can be answered by making use of the following theorem:

  Theorem 2.4. *(Chinese Remainder Theorem) Let* n_1, n_2, $\ldots$, n_k *be pairwisely relatively prime numbers. The system of equation*

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

  has a unique solution modulo $n_1 n_2 \cdots n_k$.

Proof. Let us proof first that there exists at most one solution modulo $n_1 n_2 \cdots n_k$. Suppose that there are x_1 and x_2 that satisfies the above system of equations. Then, $x_1 - x_2 \equiv 0 \pmod{n_i}$ for all i. Since $n_i \mid (x_1 - x_2)$, let us say that $x_1 - x_2 = n_1 y_1$. For any other n_i such that $i \neq 1$, we have that $n_i \mid (n_1 y_1)$ and $\gcd(n_1, n_i) = 1$, so $n_i | y_1$. In the same way, we can prove that $y_1 = n_2 y_2$ for some integer y_2, and so on. Hence, we can show that $x_1 - x_2 = n_1 n_2 \cdots n_k y_k$ for some integer y_k. This shows that $x_1 \equiv x_2 \pmod{n_1 n_2 \cdots n_k}$.

Next, we have to show that there exists at least one solution. Let $N = n_1 n_2 \cdots n_k$, and let $N_i = N/n_i$ for all i. Since N_i is relatively prime to n_i, there exists a number I_i such that $N_i I_i \equiv 1 \pmod{n_i}$.

Consider the number $M = N_1 I_1 a_1 + N_2 I_2 a_2 + \cdots + N_k I_k a_k$. We have that

$$\begin{aligned} M &\equiv N_1 I_1 a_1 + N_2 I_2 a_2 + \cdots + N_k I_k a_k && \pmod{n_i} \\ &\equiv N_i I_i a_i + n_i((N_1/n_i) I_1 a_1 + (N_2/n_i) I_2 a_2 + \cdots + (N_k/n_i) I_k a_k) && \pmod{n_i} \\ &\equiv N_i I_i a_i && \pmod{n_i} \\ &\equiv a_i && \pmod{n_i} \end{aligned}$$

for all i. So there exists at least one solution. We are done. □

3 Primes

- A positive integer $p > 1$ is called prime if its only factors are 1 and itself.

  2, 3, 5, 7, 11, 13, 17 are the seven smallest prime numbers.

- Let S be a set, and $\oplus$ and $\otimes$ be binary operations on S. The tuple $(S, \oplus, \otimes)$ is called a *field* if the following properties hold:

  1. *Associativity:* For any $a, b, c \in S$, we have that $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ and $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.
  2. *Commutativity:* For any $a, b \in S$, we have that $a \oplus b = b \oplus a$ and $a \otimes b = b \otimes a$.
  3. *Distributivity:* For any $a, b, c \in S$, we have that $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.
  4. *Identity:* There exists e and i in S such that $a \oplus e = e \oplus a = a$ and $a \otimes i = i \otimes a = a$ for all a. Here, e is called the *additive identity* and *multiplicative identity.*
  5. *Additive Inverse:* For every $a \in S$, there exists a number b, called the *addtive inverse* of a and denoted by $-a$, such that $a \oplus b = e$.
  6. *Multiplicative Inverse:* For every $a \neq e$ in S, there exists a number b, called the *multiplicative inverse* of a and denoted by a^{-1}, such that $a \otimes b = i$.

  $(\mathbb{R}, +, \times)$ and $(\mathbb{Q}, +, \times)$ are fields. What are their identities?

- Consider the group $\mathbb{Z}_p$ where p is a prime number. Define operator $\cdot_p$ as follows:

  $$a \cdot_p b = (ab) \bmod p.$$

  We have that $(\mathbb{Z}_p, +_p, \cdot_p)$ is a field. We often use $\mathbb{Z}_p$ to denote the field without mentioning the two binary operations. What are the identities of $\mathbb{Z}_p$?

- Given $a \in \mathbb{Z}_p$ such that $a \neq 0$, how does one calculate a^{-1}?

  Well, by using Extended-Euclid.

  Remember that a^{-1} is a number such that $aa^{-1} \equiv 1 \pmod{p}$. Therefore, we can run Extended-Euclid(a, p) to get x and y such that $ax + py = 1$. It follows that $a^{-1} \equiv x \pmod{p}$.

- The following lemma leads to a fundamental theorem in mathematics:

Lemma 3.1. *Let a and b be integers and p be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Assume that p divides ab and p does not divide a. Let $ab = cp$. We have that $\gcd(a, p) = 1$, so there exist x and y such that $ax + py = 1$. This implies that $b = b(ax + py) = bax + bpy = cpx + bpy = p(cx + by)$. Hence, p divides b. □

Theorem 3.2. *(Fundamental Theorem of Arithemetic) Every non-zero integer n can be expressed as*

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where the p_i are distinct primes and the e_i are positive integers. Moreover, this expression is unique up to a reordering of the primes.

- Another consequence of $\mathbb{Z}_p$ being a field is the following famous theorem:

  Theorem 3.3. *(Wilson's Theorem) If p is a prime, then*

  $$(p-1)! \equiv -1 \pmod{p}.$$

  Proof. Consider the set $\{1, 2, \ldots, p-1\}$. Every number except 1 and $p-1$ can be paired with its multiplicative inverse. Hence, $(p-1)! \equiv 1(-1) \equiv -1 \pmod{p}$. □

- We also have another useful theorem:

  Theorem 3.4. *(Fermat's Little Theorem) If a is an integer and p a prime, then*

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

  Proof. The claim is trivially true for all a such that $p \mid a$. So let us assume that a is not a multiple of p. Consider the set $S = \{a, 2a, 3a, \ldots, (p-1)a\}$. We have that there are no two different elements ia and ja in S such that $ia \equiv ja \pmod{p}$ because that would imply that $i \equiv j \pmod{p}$. Note also that none of the elements in S is divisible by p. So, the elements of S, when reduced into $\mathbb{Z}_p$, is equal to the set $\{1, 2, \ldots, p-1\}$. Therefore,

  $$\begin{aligned} a(2a)(3a)\cdots((p-1)a) &\equiv (p-1)! \pmod{p} \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

  It follows that $a^p \equiv a \pmod{p}$. □

4 Euler's Phi Function

- Let (n) denote the number of positive integers less than n that are relatively prime to n. This is called the *Euler's phi function* or the *Euler's totient function.*
- If p is prime, then $\phi(p) = p - 1$.
- Also, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1 - 1/p)$.
- **Definition 4.1.** *A* reduced residue system (RRS) modulo n *is a set of $\phi(n)$ integers R such that*
  - *for any $x \in R$,* $\gcd(x, n) = 1$, *and*
  - *for any $x, y \in R$ such that $x \neq y$, we have that $x \not\equiv y \pmod{n}$.*

  For example, a reduced residue system for 9 is $\{1, 2, 4, 5, 6, 7\}$. Another RRS is $\{\pm 1, \pm 2, \pm 4\}$.

- **Lemma 4.2.** *Let* $\gcd(a, n) = 1$. *Then,* $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ *is a reduced residue system modulo* n *if and only if* $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$. *is also a reduced residue system modulo* n.

  Proof. ($\rightarrow$) Suppose $R = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ be an RRS. Consider the set $aR = \{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$. We first note that there are exactly $\phi(n)$ members of the system.

  For any $ar_i \in aR$, we have that ar_i has a multiplicative inverse module n because both a and r_i have one because they are relatively prime with n. Let $z \equiv (ar_i)^{-1} \pmod{n}$. We have that $(ar_i)z \equiv 1 \pmod{n}$, which shows that $\gcd(ar_i, n) = 1$.

  Let ar_i, ar_j be two different members of aR. We have that $ar_i \equiv ar_j \pmod{n} \iff r_i \equiv r_j \pmod{n}$ because we can multiply a^1 to both sides of the equation. It follows that none of the ar_i's are congruent modulo n. So aR is a reduced residue system.

  ($\leftarrow$) Note that $r_i \equiv a^{-1}ar_i \pmod{n}$. So we can prove this side of the lemma by the same argument above. □

- Euler's theorem is the generalization of Fermat's little theorem to general modulus.

  Theorem 4.3 (Euler's). *If* $\gcd(a, n) = 1$, *then* $a^{\phi(n)} \equiv 1 \pmod{n}$ *for any positive integer* n.

  Proof. Let $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ be an RSS modulo n. By the last lemma, $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ as also an RSS. Now, we have that

  $$a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \equiv (ar_1)(ar_2)\cdots(ar_{\phi(n)}) \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}$$

  because $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ should be the same set as $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ modulo n. Since $r_1 r_2 \cdots r_{\phi(n)}$ has a multiplicative inverse, we have that $a^{\phi(n)} \equiv 1 \pmod{n}$. □

- **Theorem 4.4.** *If* $\gcd(m, n) = 1$, *then* $\phi(mn) = \phi(m)\phi(n)$.

  Proof. Let M be an RSS modulo m, N an RSS modulo n, and MN be an RSS modulo mn. We show that $|MN| = |M \times N|$.

  We first show that $|MN| \leq |M \times N|$. Let $x \in MN$. Consider the ordered pair $(x \bmod m, x \bmod n)$. Since $\gcd(x, mn) = 1$, we have that $\gcd(x \bmod m, m)$ should be 1 as well. Otherwise, x has a common factor with m, and $\gcd(x, mn)$ would not be 1. We can argue similarly for the fact that $\gcd(x \bmod n, n) = 1$. So $(x \mod m, x \mod n) \in M \times N$ and we can send x to this ordered pair to have an injection from MN to $M \times N$.

  Next, we show that $|M \times N| \leq |MN|$. Let $(a, b) \in M \times N$. By the Chinese Remainder theorem, there exists a unique x modulo mn such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. We claim that $\gcd(x, mn) = 1$. Otherwise, let us say that $\gcd(x, mn) = d > 1$. Since $d \mid mn$ and $\gcd(m, n) = 1$, then d divides either m or n. Let us say $d \mid m$. Then, $d \leq \gcd(x, m) = \gcd(x \mod m, m) = \gcd(a, m)$, which is impossible because $\gcd(a, m) = 1$. Hence, $x \in MN$, and we can send (a, b) to x to have an injection from $M \times N$ to MN. □

- **Theorem 4.5.** *If* $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ *where* p_i*'s are prime numbers and* k_i *are positive integers, then*

  $$\phi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\cdots\Big(1 - \frac{1}{p_k}\Big).$$

  Proof.

  $$\begin{aligned}
  \phi(n) &= \phi\big(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\big) \\
  &= \phi(p_1^{e_1})\phi(p_2^{e_2})\cdots\phi(p_k^{e_k}) \\
  &= p_1^{e_1}\Big(1 - \frac{1}{p_1}\Big)p_2^{e_2}\Big(1 - \frac{1}{p_2}\Big)\cdots p_k^{e_k}\Big(1 - \frac{1}{p_k}\Big) \\
  &= n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\cdots\Big(1 - \frac{1}{p_k}\Big).
  \end{aligned}$$

5 Primitive Roots

- In this section, we are going to study the equation $x^k \equiv a \pmod{n}$.
- When talking about the equation $x^k \equiv a \pmod{n}$, we often restrict to a such that $\gcd(a, n) = 1$ because these are the case where solutions often exist. Note that this makes $\gcd(x, n) = 1$ as well.
- The tool we are going to employ is the primitive roots.

  Definition 5.1. *Let n be a positive integer. If there exists g such that the equation $g^k \equiv a \pmod{n}$ can be solved for k for all a such that $\gcd(a, n) = 1$, then g is called a* primitive root modulo n.

  We will characterize which n has primitive roots, and how to find one if it exists.
- Suppose the n has a primitive root g. Consider the infinite sequence

  $$1 \bmod n, g \bmod n, g^2 \bmod n, g^3 \bmod n, \ldots$$

  This sequence must be periodic because there are only n elements in $\mathbb{Z}_n$. Note that since $\gcd(g, n) = 1$, we have that the period of the sequence is at most $\phi(n)$. Moreover, the period must be exactly $\phi(n)$ because we can solve $g^k \equiv a \pmod{n}$ for all a such that $\gcd(a, n) = 1$, and there are $\phi(n)$ such numbers. This fact leads to the following lemma.

  Lemma 5.2. *g is a primitive root modulo n if and only if $\{1, g, g^2, \ldots, g^{\phi(n)}\}$ is a reduced residue system modulo n.*
- We are going to study properties of primitive roots. However, before doing so, it is useful to study the concept of *order* first.

  Definition 5.3. *Let n be a positive integer and let $\gcd(a, n) = 1$. The* order of a modulo n *is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. We denote the order of a by $\mathrm{ord}_n(a)$ or $\mathrm{ord}(a)$ when it is clear what n is.*

  Note that g is a primitive root if and only if $\mathrm{ord}(g) = \phi(n)$.
- **Lemma 5.4.** *The following statements are true:*

  (a) $a^k \equiv 1 \pmod{n}$ *if and only if* $\mathrm{ord}(a) \mid k$.

  (b) $a^j \equiv a^k \pmod{n}$ *if and only if* $j \equiv k \pmod{\mathrm{ord}(n)}$.

  (c) $\mathrm{ord}(a^k) = \mathrm{ord}(a)/\gcd(k, \mathrm{ord}(a))$ *for any* $k > 1$.

  (d) If $\gcd(a, b) = 1$, *then* $\mathrm{ord}(ab) = \mathrm{ord}(a)\mathrm{ord}(b)$.

  Proof. (a) If $\mathrm{ord}(a) \mid k$, then $k = q \cdot \mathrm{ord}(a)$ for some integer q. So

  $$a^k \equiv a^{q \cdot \mathrm{ord}(a)} \equiv (a^{\mathrm{ord}(a)})^q \equiv 1^q \equiv 1 \pmod{n}.$$

  If $\mathrm{ord}(a)$ does not divide k, then we can write $k = q \cdot \mathrm{ord}(a) + r$ where $0 \leq r < \mathrm{ord}(a)$. We have that $a^k \equiv a^{q \cdot \mathrm{ord}(a) + r} \equiv a^r \pmod{n}$. Since $r < \mathrm{ord}(a)$, we have that $a^r \not\equiv 1 \pmod{n}$.

  (b) $a^j \equiv a^k \pmod{n}$ if and only if $a^{j-k} \equiv 1 \pmod{n}$. Using (a), we have that $\mathrm{ord}(a) \mid (j - k)$. In other words, $j \equiv k \pmod{\mathrm{ord}(n)}$.

  (c) Suppose $(a^k)^x \equiv 1 \pmod{n}$. Using (b), we have that $kx \equiv 0 \pmod{\mathrm{ord}(a)}$. The solution to the last equation has the form $i \cdot \mathrm{ord}(a)/\gcd(k, \mathrm{ord}(a))$. Hence, the least positive solution is $\mathrm{ord}(a)/\gcd(k, \mathrm{ord}(a))$. □