We use the notation

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$
$$\mathbb{N} = \{1, 2, \cdots\}$$
$$\mathbb{N}_0 = \{0, 1, 2, \cdots\}$$

(along with addition, subtraction, and multiplication)

Def. For $n, d \in \mathbb{Z}$, we write $d \mid n$ (d divides n) if $\exists q \in \mathbb{Z}$ $n = qd$. n is called a multiple of d and d is called a divisor of n.

Note that the set of divisors of 0 is $\mathbb{Z}$ and the set of multiples of 0 is $\{0\}$.

Ex. (i) $\forall m, n, n' \in \mathbb{Z}$, $m \mid n \rightarrow m \mid nn'$

(ii) $\forall m, n, n' \in \mathbb{Z}$, $m \mid n$ and $m \mid n'$ implies $m \mid n + n'$.

(iii) $\forall m, n, n' \in \mathbb{Z}$, $m \mid n$ and $n \mid n'$ implies $m \mid n'$.

(iv) $\forall m, n, n' \in \mathbb{Z}$, if $mn' \mid nn'$ and $n' \neq 0$, then $m \mid n$.

(v) $\forall m, n \in \mathbb{Z}$, if $m \mid n$ and $n \neq 0$, then $|m| \leq |n|$

Theo. [Quotient Remainder Theorem]. For any two integers m, n with $m \neq 0$, there is a unique "quotient" q and "remainder" r such that

$$n = qm + r \quad \text{where} \quad 0 \leq r < |m|$$

Proof. We prove it for all $n \geq 0$, $m \geq 0$. All the other cases can be derived from this (how?).

Fix some $m > 0$. We use strong induction on m.

Base cases: $[0, m)$. Then $q = 0$ and $r = n$ satisfies.

Induction step:

Induction hypothesis: $\forall n \in \mathbb{N}, n < k \; \exists q, r$ s.t. $n = qm + r$ and $0 \le r < m$

Consider $k' = k - m$. By the hypothesis, $\exists q', r'$ s.t. $k' = q'm + r'$

$q^* = q' + 1$ and $r^* = r' + 1$ satisfies the requirements.

(This algorithm to get q and r is known as the division algorithm.)

Proof of uniqueness:

Let $n = q_1 m + r_1 = q_2 m + r_2$ where $0 \le r_1, r_2 < |m|$.

W.l.o.g., assume $r_1 \ge r_2$. Then $0 \le (r_1 - r_2) < |m|$.

We also have $(r_1 - r_2) = (q_1 - q_2)m$. However, the only multiple of m in $[0, |m|)$ is $0 \Rightarrow r_1 = r_2 \underset{\text{since } m \neq 0}{\Rightarrow} q_1 = q_2$. ■

Def. m is a common divisor of integers a, b if $m | a$ and $m | b$.

For $(a, b) \neq (0, 0)$, $\gcd(a, b)$ is the largest common divisor of a, b.

This is well-defined. The set of divisors is finite because a divisor of a, b is $\le a, b$. This set is non-empty as 1 belongs to it. If $a | b$ and $(a, b) \neq (0, 0)$, then $\gcd(a, b) = |a|$. Note that $\gcd(a, 0) = a$ for any a.

$\forall a, b, n \in \mathbb{Z}$, the set of common divisors of a,b is the set of common divisors of $a, b+na$.

$$(x|a \wedge x|b) \leftrightarrow (x|a \wedge x|b+na)$$

$\Rightarrow \gcd(a,b) = \gcd(a,r)$ where $b = aq+r$, $0 \le r < a$.

This is the idea behind Euclid's gcd algorithm.

Eg. $\gcd(6,16)$
$= \gcd(6,4)$
$= \gcd(2,4) = 2$.

repeat this until one of them divides the other.

This algorithm gives a bit more insight into the gcd.

$$2 = 6-4 = 6-(16-2\cdot 6) = 3\cdot 6 - 1\cdot 16$$
$$= a\cdot 6 + b\cdot 16 \text{ for } a,b \in \mathbb{Z}$$

More generally, $\forall a,b \in \mathbb{Z}$ $\exists u,v \in \mathbb{Z}$ $\gcd(a,b) = ua+vb$.
In fact, the following stronger result holds:

Theo: Given $a,b \in \mathbb{Z}$, let
$$L(a,b) = \{au+bv : u,v \in \mathbb{Z}\}$$
L for lattice.

Then $\forall x \in L(a,b)$ $\gcd(a,b) | x$. Further, $\gcd(a,b) \in L(a,b)$.

Proof. The first part is straightforward as $\gcd(a,b) | a$ and b.
Let d be the least element in $L^+(a,b) = L(a,b) \cap \mathbb{N}$. (well-ordering)

Then $d = au+bv$ for some $u,v \in \mathbb{Z}$. Now, use the quotient-remainder theorem and write $a = dq+r$, $0 \le r < d$

$r \in L^+(a,b)$ as $r<d$. However, $r = a-(au+bv)q$

$\Rightarrow r = 0$

$\Rightarrow d \mid a$.

As $\underbrace{d \mid a,\ d \mid b,}_{\Rightarrow\, d \le \gcd(a,b)}$ and $\underbrace{\gcd(a,b) \mid d}_{\Rightarrow\, \gcd(a,b) \le d}$, $d = \gcd(a,b)$ $\blacksquare$

As a corollary, note that $\gcd(a,b) = \min(L^+(a,b))$

Theo. For $a,b \in \mathbb{Z}$, $L(a,b)$ contains exactly the multiples of $\gcd(a,b)$.

Proof. Let $G = \{x \cdot \gcd(a,b) : x \in \mathbb{Z}\}$. As $\forall x \in L(a,b)$, $\gcd(a,b) \mid x$, $X \subseteq G$. As $g \in L(a,b)$ and $L(a,b)$ is closed under multiplication, $G \subseteq X$.

Therefore, $G = X$.

Def. $p \in \mathbb{Z}$ is said to be a **prime number** if $p \geq 2$ and the only positive divisors of p are 1 and p itself.

Theo. [Euclid's Lemma]

$\forall a,b,p \in \mathbb{Z}$ s.t. p is prime, $p \mid ab \rightarrow (p \mid a \vee p \mid b)$

Proof. Either $\gcd(a,p) = p$ or $\gcd(a,p) = 1$.

If $\gcd(a,p) = p$, then $p \mid a$.

If $\gcd(a,p) = 1$, $\exists u,v$ s.t. $ua + vp = 1$ $\Rightarrow b = uab + vpb$

$\Rightarrow p \mid b$

Theo. [Generalization of Euclid's Lemma]

$\forall a_1, a_2, \cdots, a_n, p \in \mathbb{Z}$ s.t. p is prime, $(p \mid a_1 a_2 \cdots a_n) \rightarrow \exists i\ p \mid a_i$.

(Proved by induction)

Theo. [Fundamental Theorem of Arithmetic]
For all $a \in \mathbb{Z}$, if $a \geq 2$ then $\exists$ unique $(p_1, \cdots, p_t, d_1, \cdots, d_t)$ such that $p_1 < \cdots < p_t$ are primes, $d_1, d_2, \cdots, d_t \in \mathbb{Z}^+$, and
$$a = p_1^{d_1} p_2^{d_2} \cdots p_t^{d_t}.$$

Proof. We already saw earlier that a prime factorization exists for any number (as an exercise in strong induction)

Proof of uniqueness:

Let z be the smallest positive integer with two distinct prime factorizations
$$z = p_1 \cdots p_m = q_1 \cdots q_n \quad \text{(with repetition)}$$
Let $p_1 \leq \cdots \leq p_m$
$q_1 \leq \cdots \leq q_n$

We have that $\max\{p_1, \cdots, p_m\} \neq \max\{q_1, \cdots, q_n\}$ (Due to the minimality of z)
W.l.o.g. assume $p_m > q_i$, $1 \leq i \leq n$.
However, $p_m \mid q_1 q_2 \cdots q_n \Rightarrow p_m \mid q_i$ for some i which is a contradiction as $p_m > q_i$!

$\blacksquare$

Now, suppose $a = \prod_{p \text{ prime}} p^{\alpha_p}$ and $b = \prod_{p \text{ prime}} p^{\beta_p}$.

(Only finitely many α_p or β_p are positive)

Then $a \mid b$ is equivalent to $\alpha_p \leq \beta_p$ for each p.

Similarly, $\gcd(a,b) = \prod_{p \text{ prime}} p^{\min\{\alpha_p, \beta_p\}}$

This algorithm is not practical (compared to Euclid's algorithm), however, as prime factorization is not efficient.

Similar to common divisors, we can also talk about common multiples

Def. Let a, b be non-zero. The least common multiple $\mathrm{lcm}(a,b)$ is the smallest common positive multiple of a and b.

This is well-defined as ab is a common multiple.

Similar to the gcd, if $a = \prod_{p \text{ prime}} p^{\alpha_p}$ and $b = \prod_{p \text{ prime}} p^{\beta_p}$,

$$\mathrm{lcm}(a,b) = \prod_{p \text{ prime}} p^{\max\{\alpha_p, \beta_p\}}$$

Note that as a consequence,

$$\gcd(a,b) \cdot \mathrm{lcm}(a,b) = |ab|$$

The above also provides an algorithm to calculate the lcm which is more efficient than prime factorization.

Def. We say two numbers are congruent with respect to "modulus" m and write $a \equiv b \pmod{m}$ if $m \mid a-b$.

We typically consider $m > 0$.

$\left(\begin{array}{ll} \text{because} & a \equiv b \pmod{0} \text{ iff } a = b \\ \text{and} & a \equiv b \pmod{m} \leftrightarrow a \equiv b \pmod{|m|} \end{array} \right)$

Going back to the quotient-remainder theorem, note that a and b are congruent iff they leave the same remainder with m. (Why?)

This enables us to partition $\mathbb{Z}$ into m "equivalence classes" based on the remainder they leave with m.

Modular Arithmetic:

Fix some modulus $m > 0$.

Let $\overline{a}$ be the equivalence class containing m.

$$\overline{a} = \{ b \in \mathbb{Z} : m \mid b-a \}$$

Let $\mathbb{Z}_m = \{ \overline{0}, \overline{1}, \dots, \overline{m-1} \}$.

We define modular addition by $\overline{a} + \overline{b} = \overline{a+b}$

This is well-defined as for any $x \in \overline{a}$ and $y \in \overline{b}$, $x+y \in \overline{a+b}$

$\left((\overline{a} = \overline{a'} \wedge \overline{b} = \overline{b'}) \leftrightarrow \overline{a+b} = \overline{a'+b'} \right)$ Why?

Note that modular addition is commutative, associative, and is closed under additive inverses. (just like regular addition)

(so it has an additive identity)

We define modular multiplication by $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Check that this is similarly well-defined.

Note that modular multiplication is commutative, associative, and has an identity ($\overline{1}$). (just like regular multiplication)

We often abuse notation and refer to $a \in \mathbb{Z}_M$ by its corresponding value in $\mathbb{Z}$.

$a \in \mathbb{Z}_m$ has a multiplicative inverse iff a is co-prime to m.

$\gcd(a,m) = 1 \iff \exists u,v \;\; au + mv = 1 \iff \exists u \;\; \bar{a} \cdot \bar{u} = \bar{1}$

So for a prime modulus m, all elements except $\bar{0}$ have a multiplicative inverse.

The Chinese Remainder Theorem:

Suppose we have $a,b \in \mathbb{N}$ and $r,s \in \mathbb{N}_0$ such that $r<a$ and $s<b$. Does there exist an $n \in \mathbb{N}_0$ such that

$$n \equiv r \pmod{a} \quad \text{and} \quad n \equiv s \pmod{b} \; ?$$

We may assume $n \leq \operatorname{lcm}(a,b)$.

A similar question is: what are all pairs (r,s) such that such an n exists?

For $a=3$ and $b=5$, all possible pairs are reached.

We can consider this as a map from $\mathbb{Z}_{\operatorname{lcm}(a,b)}$ to $\mathbb{Z}_a \times \mathbb{Z}_b$ where $x \mapsto (x \bmod 3, \; x \bmod 5)$

For which a,b is every pair reached?

Theo. [Chinese Remainder Theorem]

If $\gcd(a,b)=1$, then $\forall r,s$, there is a unique solution (modulo ab) to the system

$$x \equiv r \pmod{a} \quad \text{and} \quad y \equiv s \pmod{b}$$

Proof. Proof of existence of x:

Let us solve for $(r,s)=(0,1)$ and $(r,s)=(1,0)$

$\exists u,v \quad au+bv=1$

Then let $\alpha = 1-au = bv$ and $\beta = 1-bv = au$

Note that α and β are solutions to the above.

Now, given any (r,s), $\alpha r + \beta s$ is a solution.

($x = bvr + aus$ is a solution to (r,s) where $au+bv=1$)

Proof of uniqueness:

wlog, we can assume $r<a$ and $b<s$ (Why?).

There are ab such pairs (r,s).

There are only ab values of $x \pmod{ab}$

$\Rightarrow$ As each x is a solution for at most one (r,s), we have a bijection between the two and no pair (r,s) has two solutions.

(Just a consequence of the fact that $|\mathbb{Z}_{ab}| = |\mathbb{Z}_a| \cdot |\mathbb{Z}_b|$)

You can thus represent any $x \in \mathbb{Z}_{ab}$ as a pair

$$(r,s) \in \mathbb{Z}_a \times \mathbb{Z}_b .$$

$x \bmod a$

$x \bmod b$

(and this representation is a bijection)

We can then easily do arithmetic in $\mathbb{Z}_{ab}$ using arithmetic in $\mathbb{Z}_a$ and $\mathbb{Z}_b$: Addition and multiplication in $\mathbb{Z}_{ab}$ are just pairwise addition and multiplication in $\mathbb{Z}_a \times \mathbb{Z}_b$!

(Why?)

As a consequence, even additive/multiplicative inverses are just coordinate-wise inverses!
(If they exist)

Thus x has a multiplicative inverse modulo ab iff it has inverses modulo a and b.

Theo. [Generalized Chinese Remainder Theorem]

Suppose $m = a_1 a_2 \cdots a_n$ where $\gcd(a_i, a_j) = 1 \ \forall i \neq j$.
For any $(r_1, \cdots, r_n)$ where $0 \le r_i < a_i$, there is a unique solution in $[0, m)$ for the system

$$x \equiv r_i \pmod{a_i} \quad \text{for } i = 1, 2, \cdots, n$$

Proof. We shall use (weak) induction to show existence.

Base case: $n=1$ clearly holds.

Induction. For all $k \ge 1$, if every system of k congruences with pairwise coprime moduli has a solution, then so does every system of $k+1$ congruences.

Given $(a_1, \cdots, a_k, a_{k+1}, r_1, \cdots, r_k, r_{k+1})$, let s be a solution of $(a_1, \cdots, a_k, r_1, \cdots, r_k)$. Let $a = a_1 a_2 \cdots a_k$. Note that $\gcd(a, a_{k+1}) = 1$.
Then the given system is equivalent to

$$x \equiv s \pmod{a} \quad \text{and} \quad x \equiv r_{k+1} \pmod{a_{k+1}}$$

We can use the Chinese Remainder Theorem to get a solution to this system of (two) congruences.
This proves existence.
Uniqueness can be proved similar to in the normal Chinese Remainder Theorem.

$\mathbb{Z}_m^\times$

For some m, $\mathbb{Z}_m^\times$ denotes the set of elements in $\mathbb{Z}_m$ that have multiplicative inverses.

$\Rightarrow \mathbb{Z}_m^\times = \{a \in \mathbb{Z}_m : \exists b \in \mathbb{Z}_m \ ab = \bar{1}\} = \{a \in \mathbb{Z}_m : \gcd(a,m) = 1\}$

Such an element is called a unit of $\mathbb{Z}_m$

For example,

$$\mathbb{Z}_3^\times = \{\bar{1}, \bar{2}\}, \quad \mathbb{Z}_6^\times = \{\bar{1}, \bar{5}\}, \quad \mathbb{Z}_8^\times = \{1,3,5,6,7\}$$

How big is $\mathbb{Z}_m^\times$?

If m is prime, it has $m-1$ elements.

If $m = p^2$ (where p is prime), it will contain all elements that are not divisible by p, which is $p^2 - p$ in number.

In fact, if $m = p^k$, then there are $p^k - p^{k-1} = m\left(1 - \frac{1}{p}\right)$ units.

What if $m = p_1^{d_1} \cdots p_n^{d_n}$? (where $p_1, \dots, p_n$ are prime and $p_i \neq p_j$ for $i \neq j$)

For example, $\mathbb{Z}_{15}^\times = \{1,2,4,7,8,11,13,14\}$

$\hookrightarrow$ There are $8 = (3-1)\cdot(5-1)$ elements.

By the Chinese Remainder Theorem, units have the form $(r_1, \dots, r_n)$ where each r_i is invertible modulo $p_i^{d_i}$.

$\hookrightarrow$ There are $p_i^{d_i}\left(1 - \frac{1}{p_i}\right)$ such elements

Thus, the total number of units in $\mathbb{Z}_m$ is

$$\prod p_i^{d_i}\left(1 - \frac{1}{p_i}\right) = m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

Def. For $m = p_1^{d_1} \cdots p_n^{d_n}$ where each p_i is prime and $p_i \neq p_j$ for $i \neq j$, we define the function φ, called Euler's Totient Function, by

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

The cardinality of $\mathbb{Z}_m^\times$ is given by $\varphi(m)$.

Ex. Prove that if $\gcd(a,b)=1$, $\varphi(ab)=\varphi(a)\varphi(b)$.

Such a function is known as a multiplicative function.

Some properties of $\mathbb{Z}_m^\times$

- If $a \in \mathbb{Z}_m \setminus \mathbb{Z}_m^\times$, then $\exists \underbrace{u}_{\in \mathbb{Z}_m} \neq 0$ s.t. $au = \bar{0}$.
  This implies $\gcd(a,m) > 1$.
- Conversely, if $a \in \mathbb{Z}_m^\times$, then $\forall \underbrace{u}_{\in \mathbb{Z}_m} \neq 0$ $au \neq 0$.
  (If there does exist a $u \neq 0$ such that $au = 0$, then $u = a^{-1}au = a^{-1} \cdot 0 = 0$)
- If $a \in \mathbb{Z}_m^\times$, then $a^{-1} \in \mathbb{Z}_m^\times$. (Closed under inverses)
- $a, b \in \mathbb{Z}_m^\times \Rightarrow ab \in \mathbb{Z}_m^\times$ (Closed under multiplication)
  $(ab)(b^{-1}a^{-1}) = \bar{1}$
- For each $a \in \mathbb{Z}_m^\times$, $a \cdot \mathbb{Z}_m^\times := \{ab : b \in \mathbb{Z}_m^\times\} = \mathbb{Z}_m^\times$.
  → Since $\mathbb{Z}_m^\times$ is closed under multiplication, $a \cdot \mathbb{Z}_m^\times \subseteq \mathbb{Z}_m^\times$.
  Similarly, $a^{-1} \cdot \mathbb{Z}_m^\times \subseteq \mathbb{Z}_m^\times \Rightarrow \mathbb{Z}_m^\times \subseteq a \cdot \mathbb{Z}_m^\times$
  $\Rightarrow \mathbb{Z}_m^\times = a \cdot \mathbb{Z}_m^\times$

Modular Exponentiation

For $\bar{a} \in \mathbb{Z}_m$ and $d \in \mathbb{N}$, we define

$$a^d := \underbrace{a \cdot a \cdots a}_{d \text{ times}}$$

We can also define it as $a^1 = a$ and $\forall d > 1$, $a^d = a \cdot a^{d-1}$.

We can also define it using integer exponentiation as

$$(a \bmod m)^d = (a^d \bmod m)$$

For $\mathbb{Z}_m^\times$, we can expand this to $d \in \mathbb{Z}$ as $a^0 = \bar{1}$ and $a^{-d} = (a^{-1})^d$ for $d \in \mathbb{N}$.

We have $a^e \cdot a^d = a^{e+d}$ in $\mathbb{Z}_m$ as well.

Although we cannot take d modulo m, we can take it modulo something else.

Theo. [Euler's Totient Theorem]
For all $a \in \mathbb{Z}_m^\times$, $a^{\varphi(m)} = \bar{1}$.

Proof. Fix any $m > 1$ and $a \in \mathbb{Z}_m^\times$.
Let $\mathbb{Z}_m^\times = \{x_1, \cdots, x_n\}$ where $n = \varphi(m)$
Let $u = x_1 \cdots x_n$ and $w = (ax_1) \cdots (ax_n)$.
As $a\mathbb{Z}_m^\times = \mathbb{Z}_m^\times$, $u = w$.

$$\Rightarrow a^n = \bar{1}$$
$$\Rightarrow a^{\varphi(m)} = \bar{1}.$$

Corollary. For $a \in \mathbb{Z}_m$, $a^{\varphi(m)-1} = a^{-1}$.

Corollary. [Fermat's Little Theorem]
For prime p and a not a multiple of p, $a^{p-1} = \bar{1}$.

Note the $\varphi(m)$ need not be the smallest integer k such that $a^k = \bar{1}$.

Cyclic structure of $\mathbb{Z}_p^\times$

If p is a prime, then there exists a g such that every element in $\mathbb{Z}_p^\times$ is of the form g^k.

(This is in general true for $p \in \{1, 2, 4\} \cup \{p^j, 2p^j : p \text{ is an odd prime}, j \in \mathbb{N}\}$)

(the proof invokes some results from group theory so we do not include it here. Interested readers can find some proofs at https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicmodp.pdf)

For $p=5, g=2$ and $p=7, g=3$ is a valid choice.
$\hookrightarrow 1,2,4,3$ $\quad$ $\hookrightarrow 1,3,2,6,4,5$

Such a g is called a generator of $\mathbb{Z}_p^\times$ (or a primitive root of p)

$\Rightarrow$ There is a "copy" of $\mathbb{Z}_{p-1}$ in $\mathbb{Z}_p^\times$.
(We can label $g^k \in \mathbb{Z}_p^\times$ by $k \in \mathbb{Z}_{p-1}$ in this. Then multiplication in $\mathbb{Z}_p^\times$ is equivalent to addition in $\mathbb{Z}_{p-1}$)

Given $x \in \mathbb{Z}_p^\times$ and a generator g of $\mathbb{Z}_p^\times$, we can define the discrete log of x w.r.t. g as the k such that $g^k = x$.

Return to Modular Exponentiation:

Although we define a^d for $a \in \mathbb{Z}_m^\times$ and $d \in \mathbb{Z}$, we might as well restrict ourselves to $d \in \mathbb{Z}_{\varphi(m)}$.

$$\left(c \equiv d \pmod{\varphi(m)} \Rightarrow a^c = a^d\right)$$

Now say we want to find the e^{th} root of some element in $\mathbb{Z}_m^\times$.
Given x^e and e, find x.
If we have some d s.t. $ed \equiv 1 \pmod{\varphi(m)}$, then $(x^e)^d = x$.
$(\Rightarrow \gcd(e, \varphi(m)) = 1)$
Euler's Totient function is incredibly useful in calculating exponents.

Eg. $\bar{9}^{10}$ in $\mathbb{Z}_{13}$.
$\varphi(13) = 12$.
$\Rightarrow \bar{9}^{10} = \bar{9}^{-2} = (\bar{9}^{-1})^2 = (\bar{3})^2 = \bar{9}$.
$\hookrightarrow$ calculated using Extended Euclidean Algorithm

Suppose $m = pq$ with $\gcd(p,q)=1$ and $a \mapsto (x,y)$ by Chinese R.T.

If $x \in \mathbb{Z}_p^\times$ and $y \in \mathbb{Z}_q^\times$, then
$$\begin{aligned} a^{\varphi(m)} &= a^{\varphi(p)\cdot\varphi(q)} \\ &\mapsto \left(x^{\varphi(p)\cdot\varphi(q)}, y^{\varphi(p)\cdot\varphi(q)}\right) \\ &= (\overline{1}, \overline{1}) \\ &\leftarrow\!\shortmid \overline{1} \quad \text{(as expected)} \end{aligned}$$

If $x \in \mathbb{Z}_p^\times$ and $y = 0$, then $a^{\varphi(m)} \mapsto (\overline{1}, \overline{0})$.

So $a^{\varphi(m)} \neq \overline{1}$ but $a^{\varphi(m)+1}$ is still a.

When p,q are prime, these and $a=0$ cover all cases.

$\Rightarrow$ If m is a product of distinct primes, then for all $a \in \mathbb{Z}_m$

- $a^{k\cdot\varphi(m)+1} = a$
- If $\gcd(e,\varphi(m)) = 1$, $\exists\, d$ s.t. $a^{ed} = a$. ($d = e^{-1}$ in $\mathbb{Z}_{\varphi(m)}$)

E.g. does $\overline{15}^{1/3}$ exist in $\mathbb{Z}_{33}$? (Note that $\overline{15} \notin \mathbb{Z}_{33}^\times$)

As $\varphi(33) = 20$ and $\gcd(3,20)=1$, $\overline{3} \in \mathbb{Z}_{20}$.

$(\overline{3}^{-1} = \overline{7})$

$$\Rightarrow \overline{15}^{(\overline{3})^{-1}} = \overline{15}^7$$

We can efficiently calculate exponents using binary exponentiation.

$$\begin{aligned} &\overline{15} \\ &\overline{15}^2 = \overline{27} \\ &\overline{15}^4 = \overline{27}^2 = \overline{3} \\ &\overline{15}^7 = \overline{15}^4 \cdot \overline{15}^2 \cdot \overline{15} = \overline{27} \end{aligned}$$

(We take advantage of the binary representation of 15)

Alternatively, $\mathbb{Z}_{33} \cong \mathbb{Z}_3 \times \mathbb{Z}_{11}$

$$\overline{15} \mapsto (\overline{0}, \overline{4})$$

$$\overline{15}^7 \mapsto (\overline{0}, \overline{4}^7) = (0, \overline{5}) \leftarrow\!\shortmid \overline{27}$$

$$(\overline{4}^{\overline{7}} = \overline{4}^{-3} = \overline{3}^3 = \overline{5})$$

Does $\overline{15}^{1/2}$ exist in $\mathbb{Z}_{33}$?

$\rightarrow \overline{2}^{-1}$ does not exist in $\mathbb{Z}_{20}$

↳ just says that not <u>every</u> element has a square root.

However, $\overline{9}^2 = \overline{24}^2 = \overline{15}$

$$\left(\begin{array}{l} \overline{15} \mapsto (\overline{0}, \overline{4}) \\ \overline{15}^{1/2} \mapsto (\overline{0}, \pm\overline{2}) \\ \qquad = \overline{24} \text{ or } \overline{9} \end{array} \right)$$

So when do e^{th} roots exist?

Let us restrict ourselves to $e=2$.

Squaring is not invertible in $\mathbb{Z}_m$ for $m \geq 2$ as $2 \mid \varphi(m)$ for $m>2$.

(This is more obviously seen as $a^2 = (-a)^2$ and $a \neq -a$ for $m>2$)

As some elements have multiple square roots, many elements have no square roots.

Quadratic residues are elements in $\mathbb{Z}_m^\times$ of the form x^2.

(We could equally well define it in $\mathbb{Z}_m$, but we shall mainly study $\mathbb{Z}_m^\times$)

Squares in $\mathbb{Z}_p^\times$

Let g be a generator of $\mathbb{Z}_p^\times$.

Exactly the elements $1, g^2, g^4, \cdots, g^{p-3}$ are quadratic residues.

(Why no other elements?)

Let us call this subset of $\mathbb{Z}_p^\times$ $\mathbb{QR}_p^\times$.

An obvious question to ask is: given (z,p), can we efficiently check if $z \in \mathbb{QR}_p^\times$?

A naive (terrible) way is to find a generator and check if the discrete log is even.

The method is terrible because finding the discrete log efficiently for higher n is problematic.

A far more efficient way is to see if $z^{\frac{p-1}{2}} = \bar{1}$.

If $z = g^{2k}$, then $z^{p-1/2} = g^{k(p-1)+1} = \bar{1}$.

If $z = g^{2k+1}$, then $z^{p-1/2} = g^{p-1/2} \neq \bar{1}$.

What are all the square roots of x^2 in $\mathbb{Z}_p^\times$?

Let $x^2 = \bar{1}$.

$$x^2 = \bar{1} \iff (x+\bar{1})(x-\bar{1}) = \bar{0} \iff x+\bar{1} = \bar{0} \text{ or } x-\bar{1} = \bar{0}$$

(because x is in $\mathbb{Z}_p^\times$)

$$\iff x = \bar{1} \text{ or } x = -\bar{1}$$

$\Rightarrow$ as $\left(g^{\frac{p-1}{2}}\right)^2 = \bar{1}$ and $g^{\frac{p-1}{2}} \neq \bar{1}$, $g^{\frac{p-1}{2}} = -\bar{1}$ for any generator g.

Similarly, the square roots of a^2 are only $\pm a$.

Ex. In $\mathbb{Z}_p^\times$, prove that $(a^e)^{1/e}$ has exactly $\gcd(e, p-1)$ values.

Square Roots in $QR_p^\times$

Each element in $QR_p^\times$ has exactly two square roots in $\mathbb{Z}_p^\times$.

How many square roots are in $QR_p^\times$?

Unsurprisingly, this depends on p.

If $-\bar{1} \in QR_p^\times$, then $x \in QR_p^\times \Rightarrow -x \in QR_p^\times$.

$-\bar{1} \in QR_p^\times$ iff $p-1/2$ is even. (as $-\bar{1} = g^{p-1/2}$)

$\Rightarrow$ If $p-1/2$ is odd, each element in $QR_p^\times$ has a unique square root.

(Consider $QR_{11}^\times$)

In fact, if $\frac{p-1}{2}$ is odd, $\sqrt{z}$ is just $z^{\frac{p+1}{4}} \in QR_p^\times$.

Digression 1

06 September 2020 19:43

Efficiency

Although we can't count up to large numbers fast, we can quickly add, multiply, divide, exponentiate and even find gcd for them!

(They can be computed for n-bit numbers in n or n^2 steps)

For some problems however, we do not know algorithms that are much faster than 2^n or $2^{n/2}$.

In fact, we believe that no better algorithms even exist for some problems.
just a belief.

This difficulty is the basis for most modern cryptography.

Cryptography in $\mathbb{Z}_m^\times$.

Def. A trapdoor one-way permutation is a bijection that is "easy" to compute but "hard" to invert; but if you have some (secret) information (trapdoor), it becomes easy to invert.

We discuss two such functions. Both use a modulus $m = pq$ for large primes p, q and can easily be inverted if we know p and q (using CRT).

Rabin's Function:

This is based on square roots in $QR_m^\times$.

If $\frac{p-1}{2}$ is odd, squaring is a permutation of $\mathbb{Z}_p^\times$ that is also easy to invert.

Define $\text{Rabin}_m(x) = x^2$ in $QR_m^\times$ where $m = pq$ for large primes p, q. If $p, q \equiv 3 \pmod 4$, then this function is a permutation that can easily be inverted if we know (p, q).

Digression 2

06 September 2020 20:08

$$\left(\text{As } \sqrt{x} \mapsto (\sqrt{a}, \sqrt{b}) = \left(a^{\frac{p+1}{4}}, b^{\frac{q+1}{4}}\right)\right)$$

We conjecture that Rabin_m is a one-way function.

RSA Function

Define $RSA_{m,e}(x) = x^e$ in $\mathbb{Z}_m$ where $m = pq$ for large primes p, q and $\gcd(e, \varphi(m)) = 1$.
A commonly used version fixes $e = 3$.

$RSA_{m,e}$ is a permutation that has inverse $RSA_{m,d}$ where $d = e^{-1}$ in $\mathbb{Z}_{\varphi(m)}$.

(by CRT, as $m = pq$)

It is also thus a trapdoor function as knowing d makes it trivial to invert.

We conjecture that $RSA_{m,e}$ is a one-way function.