Multiplicative group of integers

Z_n^*

Parsa Tasbihgou Saleh Mastani Mohammadreza Motabar

University of Tehran
Department of Mathematics and Computer Science July 18, 2022

July 18, 2022

Contents

Introduction

Introduction

- The multiplicative group of integers modulus n is widley used in cryptography. By understanding the underlying structure of this group, the mathematical properties that make Z_n^* suitable for cryptography can be generalized so that we can use other groups to improve cryptography algorithms.

- formal definition:

$$Z_n^* = \{a \in Z^+ | gcd(a, n) = 1\}$$

With natural numbers multiplication modulus n.

Introduction

- The multiplicative group of integers modulus n is widley used in cryptography. By understanding the underlying structure of this group, the mathematical properties that make Z_n^* suitable for cryptography can be generalized so that we can use other groups to improve cryptography algorithms.

- formal definition:

$$Z_n^* = \{a \in Z^+ | gcd(a, n) = 1\}$$

With natural numbers multiplication modulus n.

Exploration

Z_n^* is group

1. Has identity: 1 is the identity element.
2. Is closed under group operation (Modular Multiplication).
3. Is assosiative.
4. Every element has a unique multiplicative inverse (from Bezout's lemma).

Bezout's lemma

Lemma

Bezout's lemma: Let $n, m \in \mathbb{N}$, then $a, b \in \mathbb{Z}$ exist such that:

$$an + bm = gcd(n, m)$$

Proof.

Let $S = \{an + bm | a, b \in \mathbb{Z} \wedge an + bm > 0\}$. Let d be the minimum element in S (it exists since S is non-empty and well ordered).
we can show that $d = gcd(n, m)$. □

Z_n^* is abelian

Theorem

For all $n \in \mathbb{N}$ Z_n^* is an abelian group.

Proof.

From the definition of multiplication on natural numbers, it follows that modular multiplication is commutative. $\square$

Euler's totient function

Totient function was first defined by Leonhard Euler in 1763, and was denoted by π. But the modern notation and definition was introduced by Carl Friedrich Gauss in 1801 (1).

Figure: Leonhard Euler

Figure: Carl Friedrich Gauss

Euler's totient function

Definition

We denote Euler's totient function with $\phi(n)$, and it shows the number of natural numbers less than n, that are coprime to n.

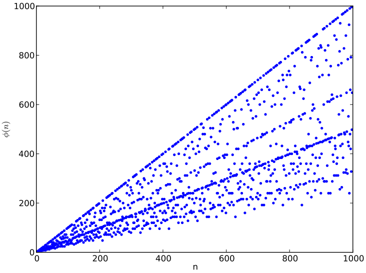
$$\phi\colon \mathbb{N} \to \mathbb{N}$$
$$\forall n \in \mathbb{N}\ \phi(n) = |Z_n^*|$$

Computing totient function

Euler intruduced the following formula to compute totient function:

Theorem

$$\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$



Computing totient function

Proof.

Let $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.
for all $1 \leq i \leq r$, let $A_i = \{k \in \mathbb{N} | p_i | k \wedge k \leq n\}$.
From inclusion-exclusion principle we have:
$\phi(n) = n - |\cup_{i=1}^{r} A_i| = n - \sum |A_i| + \sum |A_i \cap A_j| + \cdots + (-1)^r |\cap_{i=1}^{r} A_i|$.
Since for each $1 \leq i \leq r$, members of A_i are multiples of p_i, $|A_i| = \dfrac{n}{p_i}$.
More generally we can see that for all $m \leq r$ and $i_1 \leq i_2 \leq \cdots \leq i_m$,
$|\cap_{k=1}^{m} A_k| = \dfrac{n}{\prod_{k=1}^{m} p_{i_k}}$.

$$\Rightarrow \phi(n) = n - \sum \frac{n}{p_i} + \sum \frac{n}{p_i, p_j} + \cdots + (-1)^r \frac{n}{p_1, p_2, \cdots, p_r}$$

$$= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_r}).$$

□

Computing totient function

Corollary

1. $\phi(nm) = \phi(n)\phi(m)\dfrac{gcd(n,m)}{\phi(gcd(n,m))}$
   $\phi(p^k) = p^{k-1}(p-1)$

Cyclic groups

Definition

We know all cyclic groups of order $n \in \mathbb{N}$ are equal upto isomorphism, therefor we can denote all of them with a single symbol.
Let C_n be the cyclic group of order n.

Theorem

For all $n \in \mathbb{N}$, C_n has a unique cyclic subgroup of order d, where $d|n$. And C_n has no other subgroups.

Theorem

Let G be a group and $H \leq G$, where H is isomorph with Klein 4-group. G is not cyclic.

Proof.

Let $G \cong C_n$ for some $n \in \mathbb{N}$ from theorem 7, we know that G can have at most 2 subgroups of order 2, however since $\{e, a, b, c\} = H \leq G$ and $H \cong k_4$, $a^2 = b^2 = c^2 = e$, therefor $\langle a \rangle, \langle b \rangle, \langle c \rangle$ are all subgroups of order 2 of G. So G can not be cyclic. □

Definition

Let G be a group, define ψ_G as follow:

$$\psi_G\colon \mathbb{N} \to \mathbb{N}$$
$$\psi_G(m) = |\{x \in G | ord(x) = m\}$$

Theorem

$$\sum_{d|n} \psi_{C_n}(d) = n.$$

Proof.

Every element in C_n has some order that divides n (from Lagrange's theorem). So every element is exactly counted once in the above sum. □

Theorem

C_n has exactly $\phi(n)$ generators.

Theorem

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

Corollary

$$\sum_{d|n} \phi(d) = \sum_{d|n} \psi_{Z_n^*}(d).$$

Theorem

Let $k \in \mathbb{N} \wedge k > 2$, if $n = 2^k$ the Z_n^* is not cyclic.

Proof.

Let $G = \{1, -1(\cong 2^k - 1 \mod n, 2^{k-1} - 1, 2^{k-1} + 1)\}$. It is easy to verify that $G \leq Z_n^*$. Now we show that $G \cong K_4$:
$(2^k - 1)^2 \cong 2^{2k} - 2 \cdot 2^k + 1 \cong 0 - 0 + 1 \cong 1 \mod n$.
$(2^{k-1} - 1)^2 \cong 2^{2k-2} - 2^k + 1 \cong 2^k \cdot 2^{k-2} - 2^k + 1 \cong 0 - 0 + 1 \cong 1 \mod n$.
$2^{k-1} + 1^2 \cong 2^{2k-2} + 2^k + 1 \cong 2^k \cdot 2^{k-2} + 2^k + 1 \cong 0 + 0 + 1 \cong 1 \mod n$.
From theorem 8, Z_n^* cannot be cyclic. □

Theorem

Let p be a prime number, for all $d \leq n$, $\psi_{Z_p^*}(d) = 0 \wedge \psi_{Z_p^*}(d) = \phi(d)$.

Proof.

If there is no $a \in Z_p^*$ such that $ord(a) = d$, $\psi(d) = 0$. Let $a \in Z_p^*$ such that $ord(a) = d$, since $\Gamma\colon x^d \cong 1 \mod p$ has at most d solutions, and all the elemnts of the sequence $D\colon a, a^2, a^3, \cdots, a^d$ are different, and $(a^i)^d \cong 1 \mod p$, therefor all the solutions to Γ are contained in D. So for any $b \in Z_p^*$ such that $ord(b) = d$, b is in D.

It is obvious that elements of D and $< a >$ are equal, therefor $| < a > | = d$, also any $b \in Z_p^*$ such that $ord(b) = d$ is a generator for $< a >$. We know $< a >$ has exactly $\phi(d)$ generators, therefor there are exactly $\phi(d)$ members of Z_p^* of order d.

So $\phi(d) = \psi_{Z_p^*}(d)$. □

Corollary

For all $d||Z_p^*|\phi(d) = \psi_{Z_p^*}(d)$, *therefor* $\psi_{Z_p^*}(|Z_p^*|) \neq 0$, *So* Z_p^* *containt an element like* g *of order* $|Z_p^*|$, *hence* g *is a generator for* Z_p^*.
We can conclude that Z_p^* *is cyclic.*

Primitive root

Primitive root

Definition

Primitive root: Let $n \in \mathbb{N}$, we say g is a primitive root for n iff for all $x \in \mathbb{N} \wedge x \leq n$ there exist $k \in \mathbb{N}$ such that $x \equiv g^k \mod n$.

Corollary

There exists a primitive root for $n \in \mathbb{N}$ iff Z_n^* is cyclic group.

Corollary

All prime integers have primitive roots.

Theorem

Primitive root theorem:

Number class	Primitive root
$\{1, 2, 4\}$	has primitive root
For all prime p and $k \in \mathbb{N}$, p^k	has primitive root
For all prime p and $k \in \mathbb{N}$, $2p^k$	has primitive root
All other numbers	does'nt have primitive root

Corollary

If $n \in \mathbb{N}$ has a primitive root, then n has $\phi(\phi(n))$ primitive roots.

[1] Carl F. Gauss (1801), Disquisitiones Arithmaticae (Investigations on Arithmatics)

[2] Victor Shoup, A computational introduction to number theory and algebra, Non-commercial version

[3] Amin Witno, Premitive root theorem, www.witno.com/numbers/chap5.pdf