Multiplicative Group of Integers Modulo n ($\mathbb{Z}_n^*$)

Parsa Tasbihgou, Saleh Mastani, Mohammadreza Motabar

July 19, 2022

Abstract

Structure and properties of $\mathbb{Z}_n^*$, especially when this group is cyclic are discussed in section 1 and related facts such as primitive root theorem are proved, assuming basic knowledge of group theory.

1 Structure and properties of $\mathbb{Z}_n^*$

Definition 1. *For a natural number n we define the multiplicative group of integers modulo n to be the set*

$$\mathbb{Z}_n^* = \left\{ a \in \mathbb{Z}_n^+ : \gcd(a, n) = 1 \right\}.$$

The operation of group on $\mathbb{Z}_n^*$ is multiplication of natural numbers modulo n.

Now we prove that $\mathbb{Z}_n^*$ satisfies the axioms of group.

I. Existence of identity
Proof. $\gcd(1, n) = 1$, so $1 \in \mathbb{Z}_n^*$ and by definition of multiplication on natural numbers, 1 is the identity of $\mathbb{Z}_n^*$.

II. Closure of product
Proof. Consider $a, b \in \mathbb{Z}_n^*$ and suppose $ab \notin \mathbb{Z}_n^*$. This means $d = \gcd(ab, n) > 1$ which implies there exists a prime number p such that $p|d$. Since d is a divisor of ab, $p|a$ or $p|b$. Without loss of generality, assume $p|a$. We also know that $p|n$ because $d|n$. Thus $\gcd(a, n) \geq n$ which contradicts the assumption $a \in \mathbb{Z}_n^*$. This proves that $ab \in \mathbb{Z}_n^*$.

III. Associativity of product
Proof. By definition of multiplication on natural numbers, we conclude than the operation of $\mathbb{Z}_n^*$ is associative.

IV. Existence of inverses
Proof. Let a be an arbitrary element of $\mathbb{Z}_n^*$. Therefore $gcd(a, n) = 1$, so by Bèzout's identity

(Lemma 1) there exists integers x and y such that $ax + ny = 1$. This identity holds modulo n, so $ax \stackrel{n}{\equiv} 1$. We claim that x and n are relatively prime. Let $d = \gcd(x, n)$. If we divide $ax + ny$ by d and denote the quotient by A then we can write $dA = 1$. Since A is an integer, 1 is an integer multiple of d. Hence $d = 1$ and therefore $x \in \mathbb{Z}_n^*$ which implies $ax \stackrel{n}{\equiv} 1$.

Lemma 1 (Bèzout's identity)**.** *Let $n, m \in \mathbb{N}$. Then there exists $a, b \in \mathbb{Z}$ such that $an + bm = $* $\gcd(n, m)$.

Proof. Consider the set $S = \{an + bm : a, b \in \mathbb{Z} \text{ and } an + bm > 0\}$. Note that S is not empty because at least one of a or b is in S. So by well-ordering principle, S has a least element d. We claim that $d = \gcd(n, m)$. Let $d = an + bm$. First, we prove that d is a common divisor of m and n. By division algorithm there are integers r and q such that $n = dq + r$ and $0 \leq r < d$.

$$r = n - dq = n - (an + bm)q = n(1 - aq) + m(bq)$$

Therefore $r = 0$ or $r \in S$. But if $r \in S$ then $d \leq r$ which is a contradiction. Thus $d|n$. Similarly $d|m$.

Now we prove that every common divisor t of n and m is less than or equal to d. Let $n = tu$ and $m = tv$. It follows since $t|d = t(ua + vb)$, that $t \leq d$. □

Theorem 2. *$\mathbb{Z}_n^*$ is an Abelian group.*

Proof. By commutative property of multiplication on natural numbers, we conclude that the operation of $\mathbb{Z}_n^*$ is also commutative. □

Now we turn our attention to the order of $\mathbb{Z}_n^*$.

Definition 3. *Euler's ϕ function is defined to be the order of multiplicative group of integers. In other words*

$$\phi \colon \mathbb{N} \to \mathbb{N}$$
$$\phi(n) = |\mathbb{Z}_n^*|$$

Euler introduced this function for the first time in 1763 and denoted it by π. But its modern form was introduced by Gauss in 1801. It should be noted that $\phi(n)$ was originally introduced to express the number of natural numbers smaller than n that are coprime with n.

Theorem 4. *Euler gave the following formula to calculate $\phi(n)$.*

$$\phi(n) = n \prod_{p|n} (1 - 1/p)$$

Proof. Assume $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ is the unique factorization of n into a product of primes. Let $A_i = \{k \in \mathbb{N} : p_i | k \text{ and } k \leq n\}$ for every $1 \leq i \leq r$. By inclusion-exclusion principle,

$$\begin{aligned}\phi(n) &= n - \Big|\bigcup_{i=1}^{r} A_i\Big| \\ &= n - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \cdots + (-1)^r |A_1 \cap \cdots \cap A_r|.\end{aligned}$$

Since elements of A_i are multiples of p_i, $|A_i| = n/p_i$. Also, Since for each distinct i and j, elements of $|A_i \cap A_j|$ are multiples of p_i and p_j, we have $|A_i \cap A_j| = n/(p_i p_j)$. Similarly, for all $i_1 < \cdots < i_m$

$$\Big|\bigcap_{k=1}^{m} A_{i_k}\Big| = \frac{n}{\prod_{k=1}^{m} p_{i_k}}.$$

Consequently,

$$\begin{aligned}\phi(n) &= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 p_2 \ldots p_r} \\ &= n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r).\end{aligned}$$

□

Corollary 5. *The following results are easily derived from Theorem 3.*

a. $\phi(nm) = \phi(n)\phi(m)\gcd(n,m)/\phi(\gcd(n,m))$

b. $\phi(p^k) = p^{k-1}(p-1)$

Theorem 2 states that $\mathbb{Z}_n^*$ is Abelian. But to understand it better, we need to know whether $\mathbb{Z}_n^*$ is cyclic or not.

Definition 6. *Suppose n and g are natural numbers. We say g is a primitive root of n if $g \overset{n}{\not\equiv} 0$ and for all natural number x coprime with n, $x \overset{n}{\equiv} g^k$ for some natural number k. In other words, g is primitive root of n if g is a generator of $\mathbb{Z}_n^*$.*

This concept was introduced by Euler, and Gauss discussed it extensively in his book "Disquisitiones Arithmeticae."

Definition 7. *By C_n and K_4 we mean the cyclic group of order n and Klein four-group respectively.*

Note that the notation C_n is justifies by the fact that all cyclic groups of order n are isomorphic.

Theorem 8. *For all naturals number n and d such that $d|n$, C_n has exactly one subgroup of order d. Furthermore, C_n has no other subgroup.*

Proof. Note that by Lagrange's theorem if $H \leq C_n$ then $|H|$ divides n which proves the second part of the theorem. For the first part, let $C_n = \langle g \rangle$ and assume that $d|n$. Therefore $\langle g^{n/d} \rangle \leq C_n$ and $|\langle g^{n/d} \rangle| = d$. We show that $\langle g^{n/d} \rangle$ is the unique subgroup of order d. Let $\langle g^{\alpha} \rangle$ be a subgroup of order d. By division algorithm we can find q and r such that $\alpha = (n/d)q + r$ and $r < n/d$. Hence, $rd < n$. Since $(g^{\alpha})^d = e$, we find that

$$(g^{q(n/d)+r})^d = g^{qn} g^{rd} = g^{rd} = e.$$

But $rd < n$, so $rd = 0$ which implies $r = 0$ since $d \neq 0$. This means that $g^{\alpha} \in \langle g^{n/d} \rangle$. We conclude that $\langle g^{\alpha} \rangle = \langle g^{n/d} \rangle$ because $\langle g^{n/d} \rangle$ is closed and both subgroups have d elements. □

Theorem 9. *Let G be a finite group. If there is $H \leq G$ such that $H \cong K_4$ then G is not cyclic.*

Proof. Suppose $G \cong C_n$ and let $H = \{e, a, b, c\} \leq G$. By Theorem 8, G has at most one subgroup of order two. But $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$ are subgroups of G and have order two. The contradiction proves the theorem. □

Definition 10. *Let G be a group. We define the function ψ_G to be*

$$\begin{aligned}
&\psi_G \colon \mathbb{N} \to \mathbb{N} \\
&\psi_G(m) = |\{x \in G : \operatorname{ord}(x) = m\}| .
\end{aligned}$$

We may write ψ instead of ψ_G if there is no ambiguity.

Theorem 11. *Let G be a finite group of order n. Then $\sum_{d|n} \psi(d) = n$.*

Proof. Every element of G has a specific order which divides n by Lagrange's theorem. Consequently, each element is counted exactly once in the above sum. Since there are n elements, the above sum is equal to n. □

Theorem 12. *C_n has exactly $\phi(n)$ generators.*

Proof. Firts, we show that C_n has at most $\phi(n)$ generators. Let $C_n = \langle g \rangle$. If g^k is a generator of C_n then $\operatorname{ord}(g^k) = n$. Let $d = \gcd(k, n)$. Therefore

$$(g^k)^{n/d} = (g^n)^{k/d} = e^{k/d} = e.$$

As a result, $n = \operatorname{ord}(g^k) \leq n/d$ which implies than $d = 1$ which proves the goal.

Next, we show that if $\gcd(n, k) = 1$ then $\operatorname{ord}(g^k) = n$. Assume that $\operatorname{ord}(g^k) = m$ so $g^{km} = e$. Therefore $n|km$. Since $\gcd(n, k) = 1$, $n|m$ and as a result, $n \leq m$. On the other hand, the order of an element in a group is less than or equal to the order of group. Therefore $m \leq n$. Thus $C_n = \langle g^k \rangle$ and the proof is complete. □

Theorem 13. $\sum_{d|n} \phi(d) = n$

Proof. Consider C_n and let $x \in C_n$. Then x generates a unique subgroup $\langle x \rangle$. Let t be the order of this subgroup. By Lagrange's theorem, $t|n$. For every $y \in C_n$ other than x such that $|\langle y \rangle| = t$, by Theorem 8, $\langle x \rangle = \langle y \rangle$. Therefore we can write H_t for the unique subgroup of order t which by Theorem 12, has $\phi(t)$ elements. Since for all $x \in C_n$, $\mathrm{ord}(x)|n$ and for all d such that $d|n$, H_d has $\phi(d)$ elements, we conclude that in the above sum each element is counted exactly once. There are n elements, so $\sum_{d|n} \phi(d) = n$. $\square$

Corollary 14. *From Theorem 13 and Theorem 11 we obtain that*

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

Theorem 15. *Let k be an integer greater than 2 and let $n = 2^k$. Then $\mathbb{Z}_n^*$ is not cyclic.*

Proof. Let $G = \{1, -1 \overset{n}{\equiv} 2^k - 1, 2^{k-1} - 1, 2^{k-1} + 1\}$. Then $G \leq \mathbb{Z}_n^*$. We shall show that $G \cong K_4$.

$$\begin{aligned}
(2^k - 1)^2 &\overset{n}{\equiv} 2^{2k} - 2 \cdot 2^k + 1 \overset{n}{\equiv} 0 - 0 + 1 \overset{n}{\equiv} 1 \\
(2^{k-1} \pm 1)^2 &\overset{n}{\equiv} 2^{2k-2} \pm 2^k + 1 \overset{n}{\equiv} 2^k \cdot 2^{k-2} \pm 2^k + 1 \overset{n}{\equiv} 0 \pm 0 + 1 \overset{n}{\equiv} 1
\end{aligned}$$

The result now follows from Theorem 9. $\square$

Theorem 16. *For every d in $\mathbb{Z}_n^*$, $\psi(d) = 0$ or $\phi(d) = \psi(d)$.*

Proof. If there is no $a \in \mathbb{Z}_n^*$ such that $\mathrm{ord}(a) = d$ then $\psi(d) = 0$ and we are done. Let $a \in \mathbb{Z}_n^*$ and $\mathrm{ord}(a) = d$. Since the equation $\Gamma\colon x^d \overset{p}{\equiv} 1$ has at most d solutions and all elements of $\langle a \rangle = \{e, a, a^2, \ldots, a^{d-1}\}$ satisfy Γ, we conclude that the solutions to Γ are precisely the elements of $\langle a \rangle$. As a result, if $b \in \mathbb{Z}_n^*$ and $\mathrm{ord}(b) = d$ then $b \in \langle a \rangle$. Moreover, since $\mathrm{ord}(b) = d$, d is a generator of $\langle a \rangle$. By Theorem 12, $\langle a \rangle$ has $\phi(d)$ generators, so $\psi(d)$, the number of elements of $\mathbb{Z}_n^*$ with order d, is equal to $\phi(d)$. $\square$

Corollary 17. *$\mathbb{Z}_p^*$ is cyclic. For, by Theorem 16 and Corollary 14 $\phi(d) = \psi(d)$ for all divisor d of $|\mathbb{Z}_p^*|$. Hence $\psi(|\mathbb{Z}_p^*|) \neq 0$ i.e., $\mathbb{Z}_p^*$ has an element of order $|\mathbb{Z}_p^*|$. This means that $\mathbb{Z}_p^*$ is cyclic.*

The proof of Corollary 17 is non-constructive. In the following theorem, we provide a constructive proof of the fact that $\mathbb{Z}_p^*$ is cyclic which requires the factorization of $|\mathbb{Z}_p^*| = \phi(p) = p - 1$.

Theorem 18. *$\mathbb{Z}_p^*$ is cyclic.*

Proof. Let $|\mathbb{Z}_p^*| = \prod_{i=1}^{r} q_i^{\alpha_i}$ be the unique factorization of $|\mathbb{Z}_p^*|$ into a product of prime numbers q_i's. Claim. for each q_i, there is a corresponding Q_i in $\mathbb{Z}_p^*$ such that $\mathrm{ord}(Q_i) = q_i^{\alpha_i}$.

Proof of claim. Let $g \in \mathbb{Z}_p^*$ be an element not satisfying the equation $x^{(p-1)/q_i} \stackrel{p}{\equiv} 1$ (such a g exists since degree of the preceding equation is less than $p-1$.) Let $h \stackrel{p}{\equiv} g^{(p-1)/q_i^{\alpha_i}}$. Hence $h^{q_i^{\alpha_i}} \stackrel{p}{\equiv} g^{p-1}$. We know that $g^{p-1} \stackrel{p}{\equiv} 1$ but $h^{q_i^{\alpha_i - t}} \stackrel{p}{\not\equiv} 1$ $(t > 0)$ because $h^{q_i^{\alpha_i - t}} \stackrel{p}{\equiv} g^{(p-1)/q_i^t}$ and if $g^{(p-1)/q_i^t} \stackrel{p}{\equiv} 1$ then $g^{(p-1)/q_i}$ should be congruent to 1 modulo p which is a contradiction. Therefore $\operatorname{ord}(h) = q_i^{\alpha_i}$. Thus we define Q_i to be $g^{(p-1)/q_i^{\alpha_i}}$.

Claim. $\operatorname{ord}(Q_1 Q_2 \ldots Q_r) = p-1$

Proof of claim. Assume that $t = \operatorname{ord}(Q_1 Q_2 \ldots Q_r)$ and $t < p-1$. We will obtain a contradiction. Since $t | p-1$, $(p-1)/t$ is an integer greater than 1, there is q_i such that $q_i | (p-1)/t$. Hence $t | (p-1)/q_i$. Consequently, $Q = Q_1 \ldots Q_r$ to the power of $(p-1)/q_i$ is 1. $Q^{(p-1)/q_i} \stackrel{p}{\equiv} Q_i^{(p-1)/q_i} \stackrel{p}{\equiv} 1$ since for distinct i and j, $q_i^{\alpha_i} | (p-1/q_i)$. As a result, $\operatorname{ord}(Q_i) = q_i^{\alpha_i} | (p-1)/q_i$. But this means that $q_i^{\alpha_i+1} | p-1$ which is a contradiction. Thus, $t = q-1$ and $\mathbb{Z}_p^*$ is cyclic. ☐

Theorem 19. *Let n be an odd number. Then $\mathbb{Z}_n^*$ has a primitive root if and only if $\mathbb{Z}_{2n}^*$ has a primitive root.*

Proof. Consider an odd number g. So $g^k \stackrel{2}{\equiv} 1$ for all $k \in \mathbb{N}$. Therefore by Chinese reminder theorem, $g^k \stackrel{n}{\equiv} 1$ if and only if $g^k \stackrel{2n}{\equiv} 1$ which proves the theorem. ☐

Note that every primitive root of $\mathbb{Z}_{2n}^*$ is odd but an even number h may be a primitive root of $\mathbb{Z}_n^*$. In this case $h+n$ is necessarily odd and since $h \stackrel{n}{\equiv} h+n$, $h+n$ is also a primitive root of $\mathbb{Z}_n^*$.

Theorem 20. *Let g be a primitive root of $\mathbb{Z}_p^*$ ($p > 2$ is a prime) and let $g^{p-1} \not\equiv 1 \mod p^2$. Then $g^{\phi(p^k)} \not\equiv 1 \mod p^{k+1}$ for all $k \geq 1$.*

Proof. We use induction on k. The base case is true by theorem hypothesis. Now assume that the theorem has already been proved for k. We want to prove it for $k+1$. By Euler's theorem $g^{\phi(p^k)} \equiv 1 \mod p^k$ which means that $g^{\phi(p^k)} = 1 + mp^k$ for some m such that $p \not| m$. By Corollary 5 (a),

$$g^{\phi(p^{k+1})} = g^{p\phi(p^k)} = (1 + mp^k)^p \equiv 1 + mp^{k+1} \mod p^{k+2}.$$

Since $p \not| m$, we have $g^{\phi(p^{k+1})} \not\equiv 1 \mod p^{k+2}$. ☐

Theorem 21. *Let g be a primitive root of $\mathbb{Z}_p^*$ where $p > 2$ is a prime number. Then g or $g+p$ is a primitive root of $\mathbb{Z}_{p^k}^*$ for all $k \geq 1$.*

Proof. We prove the result by induction on k. The base case is trivially true. Assume than the result is true for all values of k less than or equal to k. Let m be the order of g in $\mathbb{Z}_{p^{k+1}}^*$, so $g^m \equiv 1 \mod p^{k+1}$. As a result, $g^m \equiv 1 \mod p^k$. Hence $\phi(p^k) | m$ by Corollary 5 (b) and the induction hypothesis. By Lagrange's theorem, $m | \phi(p^{k+1})$ and since p is prime, m is $p^{k-1}(p-1)$ or $p^k(p-1)$. But by theorem 20, the order of g in $\mathbb{Z}_{p^{k+1}}^*$ is not equal to $\phi(p^k)$, so $m \neq p^{k-1}(p-1)$. Therefore $m = p^k(p-1) = \phi(p^{k+1})$ i.e., g is a primitive root of $\mathbb{Z}_{p^{k+1}}^*$. ☐

Corollary 22. *If n is of the form p^k or $2p^k$ then $\mathbb{Z}_n^*$ is cyclic.*

Theorem 23. *If $\mathbb{Z}_n^*$ is cyclic, $n = p^k$ or $n = 2p^k$.*

Proof. Let $n = mp^k$ such that $p \nmid m$. We show that if $m \geq 3$ then $\mathbb{Z}_n^*$ is not cyclic. Assume that $m \geq 3$. We know that $\phi(n) = \phi(m)\phi(p^k)$ and both $\phi(p^k)$ and $\phi(m)$ are even. Therefore by Euler's theorem, for $a \in \mathbb{Z}_n^*$ (a and n are coprime),

$$a^{\phi(n)/2} \equiv \left(a^{\phi(m)}\right)^{\phi(p^k)/2} \equiv 1^{\phi(p^k)/2} \equiv 1 \mod m$$
$$a^{\phi(n)/2} \equiv \left(a^{\phi(p^k)}\right)^{\phi(m)/2} \equiv 1^{\phi(m)/2} \equiv 1 \mod p^k.$$

By Chinese reminder theorem, $a^{\phi(n)/2} \overset{n}{\equiv} 1$ so $\mathrm{ord}(a) < \phi(n)$. As a result, a does not generate $\mathbb{Z}_n^*$. But a was arbitrary, so $\mathbb{Z}_n^*$ is not cyclic. $\square$

It is obvious that $\mathbb{Z}_1^*$, $\mathbb{Z}_2^*$ and $\mathbb{Z}_4^*$ are all cyclic. By considering Theorem 15, Theorem 23 and Corollary 22 we have the following result.

Theorem 24 (primitive root theorem)**.**
$\mathbb{Z}_n^*$ is cyclic if and only if $n \in \{1, 2, 4, p^k, 2p^k : k \geq 1 \text{ and } p > 2 \text{ is prime}\}$.

References

[1] Gauss, Carl Friedrich. *Disquisitiones arithmeticae*. Translated by Arthur A. Clarke. Springer, 1986

[2] Shoup, Victor. *A computational introduction to number theory and algebra*. Cambridge university press, 2009.

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