Multiplicative group of integers modulo n

Not to be confused with Integers modulo n.

In modular arithmetic the set of congruence classes relatively prime to the modulus number, say n, form a group under multiplication called the **multiplicative group of integers modulo *n***. It is also called the group of **primitive residue classes modulo *n***. In the theory of rings, a branch of abstract algebra, it is described as the group of units of the ring of integers modulo n. (Units refers to elements with a multiplicative inverse.)

This group is fundamental in number theory. It has found applications in cryptography, integer factorization, and primality testing. For example, by finding the order of this group, one can determine whether n is prime: n is prime if and only if the order is $n - 1$.

1 Group axioms

It is a straightforward derivation exercise to show that, under multiplication, the set of congruence classes modulo n that are relatively prime to n satisfy the axioms for an abelian group.

Because $a \equiv b \pmod{n}$ implies that $\gcd(a, n) = \gcd(b, n)$, the notion of congruence classes modulo n that are relatively prime to n is well-defined.

Since $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ implies $\gcd(ab, n) = 1$ the set of classes relatively prime to n is closed under multiplication.

The natural mapping from the integers to the congruence classes modulo n that takes an integer to its congruence class modulo n respects products. This implies that the class containing 1 is the unique multiplicative identity, and also the associative and commutative laws hold. In fact it is a ring homomorphism.

Given a, $\gcd(a, n) = 1$, finding x satisfying $ax \equiv 1 \pmod{n}$ is the same as solving $ax + ny = 1$, which can be done by Bézout's lemma. The x found will have the property that $\gcd(x, n) = 1$.

2 Notation

The (quotient) ring of integers modulo n is denoted $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/(n)$ (i.e., the ring of integers modulo the ideal $n\mathbb{Z} = (n)$ consisting of the multiples of n) or by $\mathbb{Z}_n$ (though the latter can be confused with the p-adic integers when n is a prime number). Depending on the author, its group of units may be written $(\mathbb{Z}/n\mathbb{Z})^*$, $(\mathbb{Z}/n\mathbb{Z})^\times$, $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$, $\mathrm{E}(\mathbb{Z}/n\mathbb{Z})$ (for German *Einheit*, which translates as *unit*) or similar notations. This article uses $(\mathbb{Z}/n\mathbb{Z})^\times$.

The notation C_n refers to the cyclic group of order n.

3 Structure

3.1 *n* = 1

Modulo 1 any two integers are congruent, i.e. there is only one congruence class. Every integer is relatively prime to 1. Therefore, the single congruence class modulo 1 is relatively prime to the modulus, so $(\mathbb{Z}/1\,\mathbb{Z})^\times \cong \mathrm{C}_1$ is trivial. This implies that $\varphi(1) = 1$. Since the first power of any integer is congruent to 1 modulo 1, $\lambda(1)$ is also 1.

Because of its trivial nature, the case of congruences modulo 1 is generally ignored. For example, the theorem " $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $\varphi(n) = \lambda(n)$" implicitly includes the case $n = 1$, whereas the usual statement of Gauss's theorem " $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 2$, 4, any power of an odd prime or twice any power of an odd prime," explicitly excludes 1.

3.2 Powers of 2

Modulo 2 there is only one relatively prime congruence class, 1, so $(\mathbb{Z}/2\mathbb{Z})^\times \cong \mathrm{C}_1$ is the trivial group.

Modulo 4 there are two relatively prime congruence classes, 1 and 3, so $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathrm{C}_2$, the cyclic group with two elements.

Modulo 8 there are four relatively prime classes, 1, 3, 5 and 7. The square of each of these is 1, so $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathrm{C}_2 \times \mathrm{C}_2$, the Klein four-group.

Modulo 16 there are eight relatively prime classes 1, 3, 5, 7, 9, 11, 13 and 15. $\{\pm 1, \pm 7\} \cong \mathrm{C}_2 \times \mathrm{C}_2$, is the 2-torsion subgroup (i.e. the square of each element is 1), so $(\mathbb{Z}/16\mathbb{Z})^\times$ is not cyclic. The powers of 3, $\{1, 3, 9, 11\}$ are a subgroup of order 4, as are the powers of 5, $\{1, 5, 9, 13\}$. Thus $(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathrm{C}_2 \times \mathrm{C}_4$.

The pattern shown by 8 and 16 holds[1] for higher powers 2^k, $k > 2$: $\{\pm 1, 2^{k-1} \pm 1\} \cong \mathrm{C}_2 \times \mathrm{C}_2$, is the 2-torsion subgroup (so $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is not cyclic) and the powers of 3 are a subgroup of order 2^{k-2}, so $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathrm{C}_2 \times$

$C_{2^{k-2}}$.

3.3 Powers of odd primes

For powers of odd primes p^k the group is cyclic:[2][3]

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong C_{p^{k-1}(p-1)} = C_{\varphi(p^k)}.$$

3.4 General composite numbers

The Chinese remainder theorem[4] says that if $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots$, then the ring $\mathbb{Z}/n\mathbb{Z}$ is the direct product of the rings corresponding to each of its prime power factors:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \mathbb{Z}/p_3^{k_3}\mathbb{Z} \ldots$$

Similarly, the group of units $(\mathbb{Z}/n\mathbb{Z})^\times$ is the direct product of the groups corresponding to each of the prime power factors:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z})^\times \times (\mathbb{Z}/p_3^{k_3}\mathbb{Z})^\times \ldots .$$

3.4.1 Subgroup of false witnesses

If n is composite, there exists a subgroup of the multiplicative group, called the "group of false witnesses", in which the elements, when raised to the power $n - 1$, are congruent to 1 modulo n (since the residue 1, to any power, is congruent to 1 modulo n, the set of such elements is nonempty).[5] One could say, because of Fermat's Little Theorem, that such residues are "false positives" or "false witnesses" for the primality of n. 2 is the residue most often used in this basic primality check, hence 341 = 11 × 31 is famous since 2^{340} is congruent to 1 modulo 341, and 341 is the smallest such composite number (with respect to 2). For 341, the false witnesses subgroup contains 100 residues and so is of index 3 inside the 300 element multiplicative group mod 341.

Examples

***n* = 9** The smallest example with a nontrivial subgroup of false witnesses is 9 = 3 × 3. There are 6 residues relatively prime to 9: 1, 2, 4, 5, 7, 8. Since 8 is congruent to −1 modulo 9, it follows that 8^8 is congruent to 1 modulo 9. So 1 and 8 are false positives for the "primality" of 9 (since 9 is not actually prime). These are in fact the only ones, so the subgroup {1,8} is the subgroup of false witnesses. The same argument shows that $n - 1$ is a "false witness" for any odd composite n.

***n* = 91** For $n = 91$, there are $\varphi(91) = 72$ residues relatively prime to 91, half of them (i. e. 36 of them) are false witnesses of 91, namely 1, 3, 4, 9, 10, 12, 16, 17, 22, 23, 25, 27, 29, 30, 36, 38, 40, 43, 48, 51, 53, 55, 61, 62, 64, 66, 68, 69, 74, 75, 79, 81, 82, 87, 88, and 90, since for these xs, x^{90} is congruent to 1 mod 91.

***n* = 561** 561 is a Carmichael number, thus n^{560} is congruent to 1 modulo 561 for any number n coprime to 561. Thus the subgroup of false witnesses is in this case not proper; it is the entire group of multiplicative units modulo 561, which consists of 320 residues.

4 Properties

4.1 Order

The order of the group is given by Euler's totient function: $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. This is the product of the orders of the cyclic groups in the direct product. (sequence A000010 in the OEIS)

4.2 Exponent

The exponent is given by the Carmichael function $\lambda(n)$, the least common multiple of the orders of the cyclic groups. Thus, $\lambda(n)$ is the smallest number for a given n such that for each a relatively prime to n, $a^{\lambda(n)} \equiv 1 \pmod{n}$ holds. (sequence A002322 in the OEIS)

4.3 Generators

The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if its order $\varphi(n)$ is equal to its exponent $\lambda(n)$. This is the case when n is 1, 2, 4, p^k or $2p^k$, where p is an odd prime and $k > 0$. For all other values of n the group is not cyclic.[6][7][3] The single generator in the cyclic case is called a **primitive root modulo n**.[8]

Since all the $(\mathbb{Z}/n\mathbb{Z})^\times$, $n \le 7$ are cyclic, another way to state this is: If $n < 8$ then $(\mathbb{Z}/n\mathbb{Z})^\times$ has a primitive root. If $n \ge 8$ then $(\mathbb{Z}/n\mathbb{Z})^\times$ has a primitive root unless n is divisible by 4 or by two distinct odd primes.[9] All ns which have a primitive root are listed in OEIS A033948.

In the general case there is one generator for each cyclic direct factor.

5 Examples

This table shows the cyclic decomposition of $(\mathbb{Z}/n\mathbb{Z})^\times$ and a generating set for $n \le 128$. The generating sets are not unique; e.g. modulo 16 both {15, 3} and {15, 5} will work, in the list, we list the smallest values, (thus, for

n with primitive root, we list the smallest primitive root modulo n) for example, for modulo 12, we list {5, 7} instead of {5, 11} or {7, 11} . The generators are listed in the same order as the direct factors.

For example, we take $n = 20$. $\varphi(20) = 8$ means that the order of $(\mathbb{Z}/20\mathbb{Z})^\times$ is 8 (i.e. there are 8 numbers less than 20 and coprime to it); $\lambda(20) = 4$ that the fourth power of any number relatively prime to 20 is congruent to 1 (mod 20); and as for the generators, 19 has order 2, 3 has order 4, and every member of $(\mathbb{Z}/20\mathbb{Z})^\times$ is of the form $19^a \times 3^b$, where a is 0 or 1 and b is 0, 1, 2, or 3.

The powers of 19 are {±1} and the powers of 3 are {3, 9, 7, 1}. The latter and their negatives modulo 20, {17, 11, 13, 19} are all the numbers less than 20 and coprime to it. That the order of 19 is 2 and the order of 3 is 4 implies that the fourth power of every member of $(\mathbb{Z}/20\mathbb{Z})^\times$ is congruent to 1 (mod 20).

Smallest primitive root mod n are (0 if no root exists)

> 0, 1, 2, 3, 2, 5, 3, 0, 2, 3, 2, 0, 2, 3, 0, 0, 3, 5,
> 2, 0, 0, 7, 5, 0, 2, 7, 2, 0, 2, 0, 3, 0, 0, 3, 0, 0,
> 2, 3, 0, 0, 6, 0, 3, 0, 0, 5, 5, 0, 3, 3, 0, 0, 2, 5,
> 0, 0, 0, 3, 2, 0, 2, 3, 0, 0, 0, 0, 2, 0, 0, 0, 7, 0,
> 5, 5, 0, 0, 0, 0, 3, 0, 2, 7, 2, 0, 0, 3, 0, 0, 3, 0,
> ... (sequence A046145 in the OEIS)

Numbers of the elements in a minimal generating set of mod n are

> 0, 0, 1, 1, 1, 1, 1, 2, 1, 1, 1, 2, 1, 1, 2, 2, 1, 1,
> 1, 2, 2, 1, 1, 3, 1, 1, 1, 2, 1, 2, 1, 2, 2, 1, 2, 2,
> 1, 1, 2, 3, 1, 2, 1, 2, 2, 1, 1, 3, 1, 1, 2, 2, 1, 1,
> 2, 3, 2, 1, 1, 3, 1, 1, 2, 2, 2, 2, 1, 2, 2, 2, 1, 3,
> 1, 1, 2, 2, 2, 2, 1, 3, 1, 1, 1, 3, 2, 1, 2, 3, 1, 2,
> ... (sequence A046072 in the OEIS)

6 See also

- Lenstra elliptic curve factorization

7 Notes

[1] (Gauss & Clarke 1986, arts. 90–91)

[2] (Gauss & Clarke 1986, arts. 52–56, 82–891)

[3] (Vinogradov 2003, pp. 105–121, § VI PRIMITIVE ROOTS AND INDICES)

[4] Riesel covers all of this. (Riesel 1994, pp. 267–275)

[5] Erdős, Paul; Pomerance, Carl (1986). "On the number of false witnesses for a composite number". *Math. Comput.* **46**: 259–279. doi:10.1090/s0025-5718-1986-0815848-x. Zbl 0586.10003.

[6] Weisstein, Eric W. "Modulo Multiplication Group". *MathWorld*.

[7] Primitive root, Encyclopedia of Mathematics

[8] (Vinogradov 2003, p. 106)

[9] (Vinogradov 2003, pp. 116f)

8 References

The *Disquisitiones Arithmeticae* has been translated from Gauss's Ciceronian Latin into English and German. The German edition includes all of his papers on number theory: all the proofs of quadratic reciprocity, the determination of the sign of the Gauss sum, the investigations into biquadratic reciprocity, and unpublished notes.

- Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), *Disquisitiones Arithmeticae (Second, corrected edition)*, New York: Springer, ISBN 0-387-96254-9
- Gauss, Carl Friedrich; Maser, H. (translator into German) (1965), *Untersuchungen uber hohere Arithmetik (Disquisitiones Arithemeticae & other papers on number theory) (Second edition)*, New York: Chelsea, ISBN 0-8284-0191-8
- Riesel, Hans (1994), *Prime Numbers and Computer Methods for Factorization (second edition)*, Boston: Birkhäuser, ISBN 0-8176-3743-5
- Vinogradov, I. M. (2003), "§ VI PRIMITIVE ROOTS AND INDICES", *Elements of Number Theory*, Mineola, NY: Dover Publications, pp. 105–121, ISBN 0-486-49530-2

9 External links

- Weisstein, Eric W. "Modulo Multiplication Group". *MathWorld*.
- Weisstein, Eric W. "Primitive Root". *MathWorld*.
- Web-based tool to interactively compute group tables by John Jones

10 Text and image sources, contributors, and licenses

10.1 Text

- **Multiplicative group of integers modulo n** *Source:* https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n?oldid=760210965 *Contributors:* Patrick, Michael Hardy, Dan Koehl, Charles Matthews, David Shay, Gandalf61, Giftlite, Creidieki, Perey, Helohe, Superninja, EmilJ, Remuel, Ciphergoth2, Alai, Rjwilmsi, MarSch, Maxal, Algebraist, RussBot, Ksnortum, Xaosflux, Manavkataria, DHN-bot~enwiki, GoodDay, Daqu, Richard L. Peterson, BenRayfield, Wstomv, CRGreathouse, Gyopi, Keyi, JamesBWatson, Fruits Monster, Enoksrd, Dmcq, Jdgilbey, Virginia-American, Addbot, Emiliocba~enwiki, SpBot, Zrd202, FrescoBot, RedAcer, Double sharp, EmausBot, KHamsun, Wtuvell, Ddimensões, Quondum, Quandle, Helpful Pixie Bot, ChrisGualtieri, Deltahedron, Alprobit, Enrique Santos L., Klarn and Anonymous: 48

10.2 Images

- **File:Cyclic_group.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/5f/Cyclic_group.svg *License:* CC BY-SA 3.0 *Contributors:*
- Cyclic_group.png *Original artist:*
- derivative work: Pbroks13 (talk)
- **File:OEISicon_light.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d8/OEISicon_light.svg *License:* Public domain *Contributors:* Own work *Original artist:* Watchduck (a.k.a. Tilman Piesk)

10.3 Content license

- Creative Commons Attribution-Share Alike 3.0