

A WORD ABOUT PRIMITIVE ROOTS

PETE L. CLARK

Let N be a positive integer. An integer g is said to be a **primitive root** modulo N if every element x of $(\mathbb{Z}/N\mathbb{Z})^\times$ is of the form g^i for some positive integer i . Equivalently, the finite group $(\mathbb{Z}/N\mathbb{Z})^\times$ is cyclic and $g \pmod{N}$ is a generator.

We'd like to find primitive roots mod N , if possible. There are really two problems:

Question 1. *For which N does there exist a primitive root modulo N ?*

Question 2. *Assuming there does exist a primitive root modulo N , how do we find one? How do we find all of them?*

We can and shall give a complete answer to Question 1. We already know that the group of units of a finite field is finite, and we know that $\mathbb{Z}/N\mathbb{Z}$ is a field if (and only if) N is prime. Thus primitive roots exist modulo N when N is prime.

When N is not prime we might as well ask a more general question: what is the structure of the unit group $(\mathbb{Z}/N\mathbb{Z})^\times$? From our work on the Chinese Remainder theorem, we know that if $N = p_1^{a_1} \cdots p_r^{a_r}$, there is an isomorphism of unit groups

$$(\mathbb{Z}/N\mathbb{Z})^\times = \mathbb{Z}/(p_1^{a_1} \cdots p_r^{a_r}\mathbb{Z})^\times \cong \prod_{i=1}^r (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times.$$

Thus it is enough to figure out the group structure when $N = p^a$ is a prime power.

Theorem 1. *The finite abelian group $(\mathbb{Z}/p^a\mathbb{Z})^\times$ is cyclic whenever p is an **odd** prime, or when $p = 2$ and a is 1 or 2. For $a \geq 3$, we have*

$$(\mathbb{Z}/2^a\mathbb{Z})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}}.$$

Before proving Theorem 1, let us nail down the answer it gives to Question 1.

Corollary 2. *Primitive roots exist modulo N in precisely the following cases:*

- (i) $N = 1, 2$ or 4 .
- (ii) $N = p^a$ is an odd prime power.
- (iii) $N = 2p^a$ is twice an odd prime power.

Proof: Theorem 1 gives primitive roots in cases (i) and (ii). If p is odd, then

$$(\mathbb{Z}/2p^a\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^a\mathbb{Z})^\times \cong (\mathbb{Z}/p^a\mathbb{Z})^\times$$

since $(\mathbb{Z}/2\mathbb{Z})^\times$ is the trivial group. Conversely, if N is not of the form (i), (ii) or (iii) then N is divisible either by 8 or by two distinct odd primes p and q . In the first case, write $N = 2^a \cdot M$ with $(2, M) = 1$ and $a \geq 3$. Then

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/2^a\mathbb{Z})^\times \times (\mathbb{Z}/M\mathbb{Z})^\times,$$

and $(\mathbb{Z}/N\mathbb{Z})^\times$, having the noncyclic subgroup $(\mathbb{Z}/2^a\mathbb{Z})^\times$, cannot itself be cyclic [Handout A2.5, Corollary 6]. In the second case write $N = p^a q^b M$; then

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/q^b\mathbb{Z})^\times \times (\mathbb{Z}/M\mathbb{Z})^\times.$$

Both $(\mathbb{Z}/p^a\mathbb{Z})^\times$ and $(\mathbb{Z}/q^b\mathbb{Z})^\times$ have even order, hence their orders are not relatively prime and the product group cannot be cyclic [Handout A2.5, Corollary 10].

Proof of Theorem 1: The idea – for odd p – is as follows: if g is a primitive root mod p , then [Handout A2.5, Corollary 2] the order of g mod p^a is divisible by $p - 1$, hence of the form $p^k \cdot (p - 1)$ for some $k \leq a - 1$. Therefore $g' = g^{p^k}$ has order $p - 1$ [Handout A2.5, Proposition 7]. We claim $z = 1 + p$ has order p^{a-1} ; since $\gcd(p^{a-1}, p - 1) = 1$, $g'z$ has order $p^{a-1}(p - 1)$ [Handout A2.5, Example 4].

Lemma 3. *Let p be an odd prime and z an integer which is congruent to 1 (mod p).*

a) $\text{ord}_p(z^p - 1) = \text{ord}_p(z - 1) + 1$.

b) For all $k \in \mathbb{Z}^+$, $\text{ord}_p(z^{p^k} - 1) = \text{ord}_p(z - 1) + k$.

Proof: We may write $z = 1 + xp$ for some integer x , so $\text{ord}_p(z - 1) = 1 + \text{ord}_p(x)$. Then

$$(1) \quad z^p - 1 = (1 + xp)^p - 1 = \binom{p}{1}(xp) + \binom{p}{2}(xp)^2 + \dots + \binom{p}{p-1}(xp)^{p-1} + (xp)^p.$$

For the first term on the right hand side of (1), we have

$$\text{ord}_p\left(\binom{p}{1}xp\right) = 2 + \text{ord}_p(x) = \text{ord}_p(z - 1) + 1.$$

The remaining terms have larger p -orders, so the p -order of $z^p - 1$ is $\text{ord}_p(z - 1) + 1$, whence part a). Since $z^{p^k} - 1 = (z^{p^{k-1}})^p - 1$, part b) follows by induction.

Applying Lemma 3 to $z = 1 + p$ gives $\text{ord}_p(z^{p^{k-1}} - 1) = k$ for all $k \in \mathbb{Z}^+$. So $z^{p^{a-2}} \not\equiv 1 \pmod{p^a}$ and $z^{p^{a-1}} \equiv 1 \pmod{p^a}$: z has order exactly p^{a-1} in $(\mathbb{Z}/p^a\mathbb{Z})^\times$. Therefore, with notation as above, $g'z$ has order $p^{a-1}(p - 1) = \#(\mathbb{Z}/p^a\mathbb{Z})^\times$, so is a primitive root mod p^a .

Now for $p = 2$. Note that $(\mathbb{Z}/2\mathbb{Z})^\times$ and $(\mathbb{Z}/4\mathbb{Z})^\times$ have orders 1 and 2 respectively so are certainly cyclic, and we may take $a \geq 3$. We claim that the subgroup of $(\mathbb{Z}/2^a\mathbb{Z})^\times$ generated by 5 has order 2^{a-2} and is disjoint from the subgroup generated by -1 , of order 2. It follows that the group is isomorphic to $Z_2 \times Z_{2^{a-2}}$.

When $p = 2$ Lemma 3 breaks down because the right hand side of (1) becomes just $4x + 4x^2 = 4x(x + 1)$, whose 2-order is at least $3 + \text{ord}_2(x)$ if x is odd. So instead we take x even. In fact we may just take $x = 2$, so $z = 1 + 2x = 5$,

$$\text{ord}_2(z^2 - 1) = \text{ord}_2(z - 1) + \text{ord}_2(z + 1) = \text{ord}_2(z - 1) + \text{ord}_2(6) = \text{ord}_2(z - 1) + 1.$$

Again, inductively, we get

$$\text{ord}_2(z^{2^k} - 1) = \text{ord}_2(z - 1) + k,$$

or $\text{ord}_2(5^{2^k} - 1) = k + 2$. Thus for $a \geq 2$, 5 has order 2^{a-2} in $(\mathbb{Z}/2^a\mathbb{Z})^\times$. Moreover $5^k + 1 \equiv 2 \pmod{4}$ for all k , so $5^k \not\equiv -1 \pmod{2^a}$, so the subgroups generated by the classes of 5 and of -1 are disjoint. This completes the proof of Theorem 1.

Question 2 remains: when there is a primitive root, then $(\mathbb{Z}/N\mathbb{Z})^\times$ is a cyclic group, so has $\varphi(n)$ generators, where n is its order. Since the order of $(\mathbb{Z}/N\mathbb{Z})^\times$ is $n = \varphi(N)$, if there is one primitive root there are in fact exactly $\varphi(\varphi(N))$ of them, which is interesting. When $N = p$ is a prime, we get that there are $\varphi(p-1)$ primitive roots. But how many is that?? We will turn to questions like this shortly.

Suppose now that $N = p$ is prime, so we know that there are a fair number of primitive roots modulo p , but how do we find one? This is a much deeper question. Suppose for instance we ask whether 2 is a primitive root modulo p . Well, it depends on p . Among odd primes less than 100, 2 is a primitive root modulo

3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83

and *is not* a primitive root modulo

7, 17, 23, 31, 41, 43, 47, 71, 73, 79, 89, 97;

each list has 12 members. If you extend the list you will find that the “chance” that 2 is a primitive root modulo p seems to dip below $\frac{1}{2}$ and approach a number closer to 37%. In fact Emil Artin conjectured that with 2 replaced by any prime number a , a is a primitive root modulo $(100C)\%$ of the primes, with

$$C = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\dots,$$

and in particular that a is a primitive root modulo infinitely many primes.

This is yet another example of a classical problem which has seen dramatic progress in our own lifetime. Following work of Gupta and Murty in 1984 and Heath-Brown in 1986, it is now known that there are at most two “bad” prime numbers a such that a is a primitive root modulo only finitely many primes p . So, for instance, if 2 is not a primitive root modulo infinitely many primes and 3 is not either, then we can be sure that 5 is a primitive root modulo infinitely many primes!

There are further concrete questions of great interest: for instance, what can be said about the smallest primitive root mod p ? Or, suppose we are given p and want to find a primitive root of p very quickly: what do we do? An extremely large literature exists on such matters.