CYCLICITY OF $(\mathbf{Z}/(p))^\times$

KEITH CONRAD

1. Introduction

For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic. We will give *six* proofs of this fundamental result. A common feature of the proofs that $(\mathbf{Z}/(p))^\times$ is cyclic is that they are non-constructive. Up to this day, there is no algorithm known for finding a generator of $(\mathbf{Z}/(p))^\times$ other than a brute force search: try $a = 2, 3, \ldots$ until you find an element with order $p-1$.

While the proof that a generator of $(\mathbf{Z}/(p))^\times$ exists is non-constructive, in practice it does not take long to find a generator by a brute-force search. The non-constructive proof that a generator exists gives us the confidence that our search for a generator will be successful before we even begin. By comparison, for most (but not all) non-prime m the group $(\mathbf{Z}/(m))^\times$ is *not* cyclic. For example, $(\mathbf{Z}/(12))^\times$ is not cyclic: it has size 4 but each element has order 1 or 2.

While the cyclicity of $(\mathbf{Z}/(p))^\times$ is important in algebra, it also has practical significance. A choice of generator of $(\mathbf{Z}/(p))^\times$ is one of the ingredients in two public key cryptosystems: Diffie-Hellman (this is the original public key system, if we discount earlier classified work by British intelligence) and ElGamal. You can find out how these cryptosystems work by doing a web search on their names.

The following result is needed in all but one proof that $(\mathbf{Z}/(p))^\times$ is cyclic, so we state it first.

Theorem 1.1. *For any $r \geq 1$, there are at most r solutions to the equation $a^r = 1$ in $\mathbf{Z}/(p)$.*

A proof of Theorem 1.1 is given in Appendix A. Theorem 1.1 is a special case of a broader result on polynomials: any polynomial with coefficients in $\mathbf{Z}/(p)$ has no more roots in $\mathbf{Z}/(p)$ than its degree. (The link to Theorem 1.1 is that the equation $a^r = 1$ is satisfied by the roots of the polynomial $T^r - 1$, whose degree is r.) This upper bound breaks down in $\mathbf{Z}/(m)$ for non-prime m, *e.g.*, the polynomial $T^2 - 1$ has *four* solutions in $\mathbf{Z}/(8)$.

2. First Proof: A φ-identity

For our first proof that $(\mathbf{Z}/(p))^\times$ is cyclic, we are going to count the elements with various orders. In $(\mathbf{Z}/(p))^\times$, which has size $p-1$, the order of any element divides $p-1$. For each positive divisor of $p-1$, say d, let $N_p(d)$ be the number of elements of order d in $(\mathbf{Z}/(p))^\times$. For instance, $N_p(1) = 1$ and the cyclicity of $(\mathbf{Z}/(p))^\times$, which we want to prove, is equivalent to $N_p(p-1) > 0$. Every element has some order, so counting the elements of the group by order yields

$$\sum_{d|(p-1)} N_p(d) = p - 1. \tag{2.1}$$

Theorem 2.1. *Let $d|p-1$. If $N_p(d) > 0$, then $N_p(d) = \varphi(d)$.*

Proof. When $N_p(d) > 0$, there is an element of order d in $(\mathbf{Z}/(p))^\times$, say a. Then the different solutions to $x^d = 1$ are $1, a, a^2, \ldots, a^{d-1}$. There are at most d solutions, by Theorem 1.1, and there are d different powers of a, so the powers of a provide *all* the solutions to $x^d = 1$ in $\mathbf{Z}/(p)$. Any element of order d is a solution to $x^d = 1$, and therefore the elements of order d in $(\mathbf{Z}/(p))^\times$ are exactly the powers a^k which have order d. Since a^k has order $d/(k,d)$, which is d exactly when $(k,d) = 1$, $N_p(d)$ is the number of k from 1 to d which are relatively prime to d. That number is $\varphi(d)$. □

Now we can say, for any d dividing $p-1$, that

$$N_p(d) \leq \varphi(d). \tag{2.2}$$

Indeed, Theorem 2.1 tells us that $N_p(d) = 0$ or $N_p(d) = \varphi(d)$. We now feed (2.2) into (2.1):

$$p - 1 = \sum_{d|(p-1)} N_p(d) \leq \sum_{d|(p-1)} \varphi(d). \tag{2.3}$$

We have obtained an inequality for any prime p:

$$p - 1 \leq \sum_{d|(p-1)} \varphi(d). \tag{2.4}$$

If the inequality in (2.2) is strict (that is, $<$) for some d dividing $p-1$, then the inequality in (2.3) is strict, and thus the inequality in (2.4) is strict. How sharp is (2.4)? Let's look at some examples.

Example 2.2. If $p = 5$, then $\sum_{d|4} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4) = 1 + 1 + 2 = 4$.

Example 2.3. If $p = 11$, then $\sum_{d|10} \varphi(d) = \varphi(1)+\varphi(2)+\varphi(5)+\varphi(10) = 1+1+4+4 = 10$.

Example 2.4. If $p = 29$, then $\sum_{d|28} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(7) + \varphi(14) + \varphi(28) = 1 + 1 + 2 + 6 + 6 + 12 = 28$.

It appears that (2.4) might be an equality! This inspires us to prove it, and the number being of the form $p-1$ is completely irrelevant.

Theorem 2.5. *For any $n \geq 1$, $\sum_{d|n} \varphi(d) = n$. In particular, for a prime p we have $\sum_{d|(p-1)} \varphi(d) = p - 1$.*

Proof. We will count the n fractions

$$\frac{1}{n}, \frac{2}{n}, \cdots \frac{n-1}{n}, \frac{n}{n} \tag{2.5}$$

according to their denominator when put in reduced form.

For such a fraction m/n with denominator n, its reduced form denominator is a divisor of n. How many of these reduced form fractions have a given denominator? Writing $m/n = a/d$, where $(a,d) = 1$, the condition $1 \leq m \leq n$ is equivalent to $1 \leq a \leq d$. Therefore the number of fractions in (2.5) with reduced form denominator d is the number of a between 1 and d with $(a,d) = 1$. There are $\varphi(d)$ such numbers. Thus, counting the fractions in (2.5) according to the reduced form denominator, we get

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

□

Theorem 2.5 tells us (2.4) is an equality, so the inequalities in (2.2) must all be equalities: we can't have $N_p(d) = 0$ at all. (Reread the discussion right after (2.4) if you don't see this.) In particular, $N_p(p-1) > 0$, so there is an element of order $p-1$. We've (non-constructively) proved the existence of a generator!

Let's summarize the argument again.

Theorem 2.6. *For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic.*

Proof. For $d|(p-1)$, let $N_p(d)$ be the number of elements of order d in $(\mathbf{Z}/(p))^\times$. By Theorem 2.1, $N_p(d) \leq \varphi(d)$. Therefore

$$p - 1 = \sum_{d|(p-1)} N_p(d) \leq \sum_{d|(p-1)} \varphi(d).$$

By Theorem 2.5, the sum on the right is $p-1$, so the $\leq$ is an equality. That means the inequalities $N_p(d) \leq \varphi(d)$ for all d have to be equalities. In particular, $N_p(p-1) = \varphi(p-1)$, which is positive, so there is an element of $(\mathbf{Z}/(p))^\times$ with order $p-1$. □

3. Second Proof: One Subgroup per Size

We begin our second proof by establishing a divisibility property among orders of elements which is peculiar to finite *abelian* groups. In any finite group, all elements have order dividing the size of the group. In the abelian setting all orders also divide something else: the maximal order.

Lemma 3.1. *Let G be a finite abelian group. If n is the maximal order among the elements in G, then the order of every element divides n.*

For example, in $(\mathbf{Z}/(56))^\times$, which has size 24, the orders of elements turn out to be 1, 2, 3, and 6. All orders divide the maximal order 6. In S_4, also of size 24, the orders of elements are 1, 2, 3, and 4. Note 3 does not divide the maximal order 4. (Lemma 3.1 does not apply to S_4, as S_4 is non-abelian.)

The reader might want to jump ahead to Theorem 3.3 to see how Lemma 3.1 gets used, before diving into the proof of Lemma 3.1.

Proof. Let g have the maximal order n. Pick any other $h \in G$, and let $h \in G$ have order m. We want to show $m|n$. We will assume m does not divide n (this forces $m > 1$) and use this non-divisibility to construct an element with order exceeding n. That would be a contradiction, so $m|n$.

For instance, if $(m, n) = 1$, then gh has order $mn > n$. But that is too easy: we can't expect m to have no factors in common with n. How can we use g and h to find an element with order larger than n just from knowing m (the order of h) does not divide n (the order of g)? The following example will illustrate the idea before we carry it out in general.

Example 3.2. Suppose $n = 96$ and $m = 18$. (That is, g has order 96 and h has order 18.) Look at the prime factorizations of these numbers:

$$96 = 2^5 \cdot 3, \quad 18 = 2 \cdot 3^2.$$

Here m does not divide n because there are more 3's in m than in n. The least common multiple of m and n is $2^5 \cdot 3^2$, which is larger than n. We can get an element of that order by reduction to the relatively prime order case: kill the 3 in 96 by working with g^3 and kill the 2 in 18 by working with h^2. That is, g^3 has order $96/3 = 2^5$ and h^2 has order $18/2 = 9$.

These orders are relatively prime, and the group is abelian, so the product g^3h^2 has order $2^5 \cdot 9 > 96$. Thus, 96 is not the maximal order in the group.

Now we return to the general case. If m does not divide n, then there is some prime p whose multiplicity (exponent) as a factor of m exceeds that of n. Let p^e be the highest power of p in m and p^f be the highest power of p in n, so $e > f$. (Quite possibly $f = 0$, although in Example 3.2 both e and f were positive.)

Now consider g^{p^f} and h^{m/p^e}. The first has order n/p^f, which is *not* divisible by p, and the second has order p^e, which is a pure p-power. These orders are relatively prime. Since G is abelian, the product $g^{p^f}h^{m/p^e}$ has order

$$\frac{n}{p^f}p^e = np^{e-f} > n.$$

This contradicts the maximality of n as an order in G, so we have reached a contradiction. □

The following will be our criterion for showing a group is cyclic. Recall that in a cyclic group there is just one subgroup of any size. Assuming the group is abelian, the converse holds.

Theorem 3.3. *Let G be a finite abelian group with at most one subgroup of any size. Then G is cyclic.*

Proof. Let n be the maximal order among the elements of G, and let $g \in G$ be an element with order n. We will show every element of G is a power of g, so $G = \langle g \rangle$.

Pick any $h \in G$, and say h has order d. Since $d|n$ by Lemma 3.1, we can write down another element of order d: $g^{n/d}$. Thus we have two subgroups of size d: $\langle h \rangle$ and $\langle g^{n/d} \rangle$. By hypothesis, these subgroups are the same: $\langle h \rangle = \langle g^{n/d} \rangle$. In particular, $h \in \langle g^{n/d} \rangle \subset \langle g \rangle$, so h is a power of g. Since h was arbitrary in G, $G = \langle g \rangle$. □

Remark 3.4. Is the abelian hypothesis in Theorem 3.3 necessary? That is, are there any non-abelian groups with one subgroup of each size? No. A finite group with at most one subgroup of each size must be cyclic, even if we don't assume at first that the group is abelian. However, to prove this without an abelian hypothesis is quite a bit more involved than the proof of Theorem 3.3. (Where did we use the abelian hypothesis in the proof of Theorem 3.3?)

Now we are ready to show $(\mathbf{Z}/(p))^\times$ is cyclic.

Theorem 3.5. *For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic.*

Proof. We will show $(\mathbf{Z}/(p))^\times$ satisfies the hypothesis of Theorem 3.3: it has at most one subgroup of any size. Let $H \subset (\mathbf{Z}/(p))^\times$ be a subgroup, with size (say) d. Then every $a \in H$ satisfies $a^d = 1$ in $\mathbf{Z}/(p)$, so every element of H is a d-th root of unity: H is a subset of the solutions to $x^d = 1$. By Theorem 1.1, there are at most d solutions to $x^d = 1$ in $\mathbf{Z}/(p)$. Since d is the size of H (by definition), we filled up the d-th roots of unity using H:

$$H = \{x \in \mathbf{Z}/(p) : x^d = 1\}.$$

The right side is completely determined by d. We have shown there is at most one subgroup of $(\mathbf{Z}/(p))^\times$ with size d, for any d, so Theorem 3.3 applies. □

4. Third Proof: Bounding with the Maximal Order

Our third proof that $(\mathbf{Z}/(p))^\times$ is cyclic will apply Lemma 3.1 from the second proof, but in a different way. That lemma says that in any finite abelian group, the order of any element divides the maximal order of the elements in the group. Review Lemma 3.1 after seeing how it gets used here.

Theorem 4.1. *For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic.*

Proof. Let n be the maximal order among the elements in $(\mathbf{Z}/(p))^\times$. We want to show $n = p-1$, so there is an element of order $p-1$. Obviously $n \leq p-1$. (More precisely, $n|(p-1)$, but the crude inequality will suffice.)

Every element has order dividing n, by Lemma 3.1, so each $a \in (\mathbf{Z}/(p))^\times$ satisfies $a^n = 1$. Theorem 1.1 says the equation $x^n = 1$ has at most n solutions in $\mathbf{Z}/(p)$. We already produced $p-1$ different solutions (namely all of $(\mathbf{Z}/(p))^\times$), so $p-1 \leq n$.

Comparing the two inequalities, $n = p-1$. Thus there is an element of order $p-1$, so $(\mathbf{Z}/(p))^\times$ is cyclic. □

5. Fourth Proof: Prime-Power Subgroups are Cyclic

Our next proof that $(\mathbf{Z}/(p))^\times$ is cyclic is going to use the theory of polynomials over $\mathbf{Z}/(p)$ in a more substantial manner than just Theorem 1.1. We will need to know that polynomials with coefficients in $\mathbf{Z}/(p)$ have unique factorization into irreducible polynomials.

Example 5.1. With coefficients in $\mathbf{Z}/(3)$, the irreducible factorization of $T^7 + 2T^6 + T^5 + T^4 + T + 2$ is

$$(T^2 + T + 2)^2(T^3 + 2T + 2).$$

This is analogous to the unique factorization of integers into primes; both are consequences of the division theorem (for integers or for polynomials). Find a proof of unique factorization in the integers in a book and check the proof carries over almost *verbatim* to the case of polynomials with coefficients in $\mathbf{Z}/(p)$. (We are not saying there is unique factorization in $\mathbf{Z}/(p)$, but in polynomials with coefficients in $\mathbf{Z}/(p)$, like $T^2 + T + 3$ and so on.) While the proof for unique factorization uses induction on the size of integers, the proof for polynomials uses induction on the degree of polynomials. That is about the only difference between the two proofs.

We start our study of $(\mathbf{Z}/(p))^\times$ with a polynomial factorization.

Theorem 5.2. *Working with coefficients in $\mathbf{Z}/(p)$, the polynomial $T^{p-1} - 1$ is a product of linear factors:*

$$T^{p-1} - 1 = (T-1)(T-2)(T-3)\cdots(T-(p-1)).$$

Proof. For every $a \not\equiv 0 \bmod p$, $a^{p-1} \equiv 1 \bmod p$, or $a^{p-1} = 1$ in $\mathbf{Z}/(p)$. Therefore the polynomial $T^{p-1} - 1$, considered over $\mathbf{Z}/(p)$, has a as a root. Since a is a root, $T - a$ is a factor (see Lemma A.2). Thus, $T^{p-1} - 1$ is divisible by each $T - a$ as a runs over $(\mathbf{Z}/(p))^\times$. This gives us factors $T-1, T-2, \ldots, T-(p-1)$. These $p-1$ factors are relatively prime to each other (they're linear, with different roots), so (by a polynomial analogue of Bezout) their product is a factor:

$$T^{p-1} - 1 = (T-1)(T-2)(T-3)\cdots(T-(p-1))h(T)$$

for some polynomial $h(T)$. Comparing degrees on both sides, we see $h(T)$ has degree 0, so $h(T)$ is a constant. Now comparing leading coefficients on both sides, we must have $h(T) = 1$. □

Example 5.3. Take $p = 7$. Treating coefficients as elements of $\mathbf{Z}/7\mathbf{Z}$, the polynomial $(T-1)(T-2)(T-3)(T-4)(T-5)(T-6)$ can be rewritten as

$$\begin{aligned}(T-1)(T-2)(T-3)(T+3)(T+2)(T+1) &= (T^2-1)(T^2-4)(T^2-9)\\ &= (T^4-5T^2+4)(T^2-9)\\ &= T^6-14T^4+49T^2-36\\ &= T^6-1.\end{aligned}$$

Corollary 5.4. *If $d|(p-1)$, there are exactly d solutions to the equation $T^d = 1$ in $\mathbf{Z}/(p)$.*

Notice this strengthens Theorem 1.1, and it could be used in place of Theorem 1.1 to shorten the first two proofs that $(\mathbf{Z}/(p))^\times$ is cyclic.

Proof. Since $d|(p-1)$, the polynomial T^d-1 is a factor of $T^{p-1}-1$. Indeed, write $p-1 = dm$. Then we have a polynomial identity

$$T^m - 1 = (T-1)(T^{m-1} + T^{m-2} + \cdots + T + 1).$$

Replace T with T^d in this identity; T^m-1 becomes $T^{p-1}-1$ and $T-1$ becomes T^d-1. The other factor on the right side becomes another polynomial. We have an equation showing $T^d - 1$ is a factor of $T^{p-1} - 1$.

Over $\mathbf{Z}/(p)$, $T^{p-1} - 1$ breaks up into distinct linear factors by Theorem 5.2. Therefore, by unique factorization of polynomials over $\mathbf{Z}/(p)$, its factor $T^d - 1$ must be a product of some of those linear factors. Counting degrees, $T^d - 1$ must be a product of d of those linear factors. The linear factors all have different roots, so $T^d - 1$ has d different solutions in $\mathbf{Z}/(p)$ when $d|(p-1)$. □

Corollary 5.4 tells us $T^d = 1$ has d solutions in $\mathbf{Z}/(p)$, but it does not tell us there is an element of order d. For the case of prime power d, however, we will now derive exactly such a result.

Corollary 5.5. *If q^e is a prime power dividing $p-1$, with $e \geq 1$, then there is an element of order q^e in $(\mathbf{Z}/(p))^\times$.*

Proof. By Corollary 5.4, the polynomial $T^{q^e}-1$ has q^e different roots in $\mathbf{Z}/(p)$ and $T^{q^{e-1}}-1$ has q^{e-1} different roots (this would be nonsense if $e = 0$; we really do need $e > 0$). Since $q^e > q^{e-1}$, our count of roots shows there must be a root, say a, of $T^{q^e} - 1$ which is not a root of $T^{q^{e-1}} - 1$. That means $a^{q^e} = 1$ but $a^{q^{e-1}} \neq 1$, so a has order q^e in $(\mathbf{Z}/(p))^\times$. □

Theorem 5.6. *For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic.*

Proof. Write $p-1$ as a product of primes:

$$p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m}.$$

By Corollary 5.5, for each i from 1 to m there is an element a_i of $(\mathbf{Z}/(p))^\times$ with order $q_i^{e_i}$. These orders are relatively prime, and $(\mathbf{Z}/(p))^\times$ is abelian, so the product of the a_i's has order equal to the product of the $q_i^{e_i}$'s, which is $p-1$. Thus, the product $a_1 a_2 \cdots a_m$ is a generator of $(\mathbf{Z}/(p))^\times$. □

6. Fifth proof: the Chinese Remainder Theorem

The fifth proof that $(\mathbf{Z}/(p))^\times$ is cyclic will, like the fourth proof, focus on prime power factors of $p-1$.

Our new tool is the following theorem about finite abelian groups whose order is a prime power.

Theorem 6.1. *Let A be a finite abelian group of prime power order q^s. If A is not cyclic, then there are more than q solutions in A to the equation $x^q = 1$.*

Proof. All elements of A have q-power order. Since A is not cyclic, $s \geq 2$. Let the maximal order of an element of A be q^t, so $t < s$. Pick $g \in A$ with this order:

$$\#\langle g\rangle = q^t.$$

The element $g^{q^{t-1}}$ has order q, and its powers provide q solutions to the equation $x^q = 1$. We now aim to find an element of A outside of the subgroup $\langle g\rangle$ which also has order q. This will provide another solution to $x^q = 1$, and thus prove the theorem.

For any $h \in A$ with $h \notin \langle g\rangle$, there is some q-power h^{q^k} which lies in $\langle g\rangle$. After all, h has q-power order, so at the very least some q-power of h is the identity (which is in $\langle g\rangle$). Necessarily $k \geq 1$. It may happen that the first q-power of h which lands in $\langle g\rangle$ is not the identity. After all, a q-power of h could land inside $\langle g\rangle$ before we run through every possible power of h (hitting the identity at the last exponent).

Let ℓ be the smallest integer ≥ 1 such that some element in A outside of $\langle g\rangle$ has its q^ℓ-th power inside $\langle g\rangle$. We claim $\ell = 1$. That is, some element outside $\langle g\rangle$ has its q-th power inside $\langle g\rangle$. Indeed, suppose $\ell > 1$ and let h_0 be an element outside of $\langle g\rangle$ with $h_0^{q^\ell} \in \langle g\rangle$. Then $h_0^{q^{\ell-1}} \notin \langle g\rangle$ by minimality of ℓ, yet this element itself satisfies $(h_0^{q^{\ell-1}})^q \in \langle g\rangle$, so there is an element whose 'ℓ' is 1. Thus $\ell = 1$.

Take h_1 to be such an element outside $\langle g\rangle$ with $h_1^q \in \langle g\rangle$, say $h_1^q = g^n$. Since h_1 has (like all elements of A) order dividing q^t, the order of h_1^q is at most q^{t-1}. Then g^n has order at most q^{t-1}, so q must divide n. (Otherwise n is relatively prime to the order of g, which would imply $g^n = h_1^q$ has order q^t, and that is not correct.) Setting $n = qr$, we have

$$h_1^q = g^{qr}.$$

Then $(h_1 g^{-r})^q = 1$ and $h_1 g^{-r} \notin \langle g\rangle$ (after all, $h_1 \notin \langle g\rangle$), so $h_1 g^{-r}$ is an element of order q in A which lies outside of $\langle g\rangle$. □

Remark 6.2. In Remark 3.4, it was noted that Theorem 3.3 is true (but harder to prove) without an abelian hypothesis. What about Theorem 6.1? Is its conclusion correct if we don't make an initial abelian hypothesis? Yes if q is an odd prime, but no if $q = 2$. For instance, Q_8 is not cyclic but it has only two solutions to $x^2 = 1$. This is not a quirk about Q_8: there are infinitely many non-abelian groups of 2-power order having only two solutions to $x^2 = 1$.

Theorem 6.3. *For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic.*

Proof. Write $p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m}$, where the q_i's are different primes (and each e_i is positive). Set

$$A_i = \{a \in (\mathbf{Z}/(p))^\times : a^{q_i^{e_i}} = 1\}.$$

This is a subgroup of $(\mathbf{Z}/(p))^\times$, and all of its elements have q_i-power order, so $\#A_i$ is a power of q_i by Cauchy's theorem.

If A_i is *not* cyclic, then Theorem 6.1 says A_i has more than q_i solutions to the equation $x^{q_i} = 1$. However, we know this equation has no more than q_i solutions in $\mathbf{Z}/(p)$ by Theorem 1.1. Thus we have reached a contradiction, so A_i is cyclic. (We do not yet, however, know the order of A_i, except that it is a q_i-power. We may expect, though, that $\#A_i = q_i^{e_i}$.)

Write $A_i = \langle a_i \rangle$. We are going to show $a_1, a_2, \ldots, a_m$ together generate $(\mathbf{Z}/(p))^\times$. Then we will show the single product $a_1 a_2 \cdots a_m$ is a generator of the group.

Dividing $p-1$ by each of $q_1^{e_1}, \ldots, q_m^{e_m}$, we get the integers

$$\frac{p-1}{q_1^{e_1}}, \frac{p-1}{q_2^{e_2}}, \ldots, \frac{p-1}{q_m^{e_m}}.$$

These have no collective common prime factor, so some $\mathbf{Z}$-combination of them is equal to 1 (iterated Bezout?):

$$\sum_{i=1}^{m} c_i \frac{p-1}{q_i^{e_i}} = 1,$$

where $c_i \in \mathbf{Z}$. Then any $a \in (\mathbf{Z}/(p))^\times$ can be written as

$$a = a^1 = a^{\sum_i c_i (p-1)/q_i^{e_i}} = \prod_{i=1}^{m} a^{c_i (p-1)/q_i^{e_i}}.$$

Since the i-th factor has order dividing $q_i^{e_i}$ (raise it to the $q_i^{e_i}$-th power as a check), it lies in A_i and thus the i-th factor is a power of a_i. Therefore a is a product of powers of the a_i's, which means

$$(\mathbf{Z}/(p))^\times = \langle a_1, a_2, \ldots, a_m \rangle.$$

To end the proof, we show that any product of powers $a_1^{n_1} a_2^{n_2} \cdots a_m^{n_m}$ is equal to a single power $(a_1 a_2 \cdots a_m)^n$. Considering that each a_i has order dividing $q_i^{e_i}$, we could find such an n by trying to solve the simultaneous congruences

$$n \equiv n_1 \bmod q_1^{e_1}, n \equiv n_2 \bmod q_2^{e_2}, \ldots, n \equiv n_1 \bmod q_m^{e_m}.$$

(Then $a_i^{n_i} = a_i^n$.) Can we solve all of these congruences with a common n? Absolutely: the moduli are pairwise relatively prime, so just use the Chinese Remainder Theorem. □

Remark 6.4. The arguments in this proof really showed something quite general about finite abelian groups. If A is a finite abelian group and p is any prime, let A_p be the subgroup of elements with p-power order. Then A is cyclic if and only if A_p is cyclic for every p. (If p does not divide A, then A_p is trivial.)

7. Sixth Proof: Cyclotomic Polynomials

In our final proof that $(\mathbf{Z}/(p))^\times$ is cyclic, we will actually write down a polynomial factor of $T^{p-1} - 1$ whose roots in $\mathbf{Z}/(p)$ are (precisely) the generators of $(\mathbf{Z}/(p))^\times$! It almost sounds like a constructive proof of cyclicity. But there is a catch: while we will construct this special polynomial and show it has roots in $\mathbf{Z}/(p)$, the proof of the existence of these roots will give no recipe for finding them (and thus no recipe for finding generators). So this proof is just as non-constructive as the other proofs. Like the fourth proof, we will use unique factorization for polynomials with coefficients in $\mathbf{Z}/(p)$.

The new polynomials we now meet are the *cyclotomic polynomials*. We will define them first as polynomials with complex coefficients. Then we will prove that the coefficients of are in fact integers, so it makes sense to reduce the coefficients modulo p. Finally we will

show one of the cyclotomic polynomials, when reduced modulo p, decomposes into linear factors and its roots in $\mathbf{Z}/(p)$ are generators of $(\mathbf{Z}/(p))^\times$.

In the complex numbers, let ρ_n be the basic n-th root of unity $\cos(2\pi/n) + i\sin(2\pi/n) = e^{2\pi i/n}$. It has order n and the other roots of unity with order n are ρ_n^j where $1 \leq j \leq n$ and $(j,n) = 1$. Define the n-th cyclotomic polynomial $\Phi_n(T)$ to be the polynomial having for its roots the roots of unity in $\mathbf{C}$ with order n:

$$\Phi_n(T) := \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (T - \rho_n^j). \tag{7.1}$$

For instance, $\Phi_1(T) = T - 1$, $\Phi_2(T) = T + 1$, and $\Phi_4(T) = (T - i)(T + i) = T^2 + 1$.

Since (7.1) is a product of linear polynomials, indexed by integers from 1 to n which are relatively prime to n, $\Phi_n(T)$ has degree $\varphi(n)$ (hence the notation for the polynomial itself; Φ is a capital Greek φ). While the definition of $\Phi_n(T)$ involves complex linear factors, the polynomials themselves, after all the factors are multiplied out, actually have integer coefficients. Here is a table listing the first 12 cyclotomic polynomials.

n	$\Phi_n(T)$
1	$T - 1$
2	$T + 1$
3	$T^2 + T + 1$
4	$T^2 + 1$
5	$T^4 + T^3 + T^2 + T + 1$
6	$T^2 - T + 1$
7	$T^6 + T^5 + T^4 + T^3 + T^2 + T + 1$
8	$T^4 + 1$
9	$T^6 + T^3 + 1$
10	$T^4 - T^3 + T^2 - T + 1$
11	$T^{10} + T^9 + T^8 + T^7 + T^6 + T^5 + T^4 + T^3 + T^2 + T + 1$
12	$T^4 - T^2 + 1$

There are evidently a lot of patterns worth exploring here. For instance, Φ_8 resembles Φ_4, which resembles Φ_2, Φ_{10} is similar to Φ_5, Φ_{12} seems related to Φ_6, which is close to Φ_3. The constant term of $\Phi_n(T)$, for $n > 1$, seems to be 1. Maybe the most striking pattern, which persists for the first 100 cyclotomic polynomials, is that the coefficients are all 0, 1, or -1. We will not determine whether or not this is always true (life needs some tantalizing mysteries), but let's show at least that all the coefficients are integers. First a factorization lemma is needed.

Lemma 7.1. *For $n \geq 1$, $T^n - 1 = \prod_{d|n} \Phi_d(T)$.*

Proof. The roots of $T^n - 1$ are the n-th roots of unity, so (by the same reasoning as in Theorem 5.2) we can write

$$T^n - 1 = \prod_{\rho^n = 1} (T - \rho), \tag{7.2}$$

where the product runs over the n-th roots of unity $\rho \in \mathbf{C}$. Every n-th root of unity has some order dividing n. For each d dividing n, collect together the linear factors $T - \rho$ corresponding to roots of unity with order d. The product of these factors is $\Phi_d(T)$, by the definition of $\Phi_d(T)$. Thus, we have transformed (7.2) into the desired formula. $\square$

Example 7.2. Taking $n = 4$,

$$\prod_{d|4} \Phi_d(T) = \Phi_1(T)\Phi_2(T)\Phi_4(T) = (T-1)(T+1)(T^2+1) = T^4 - 1.$$

Example 7.3. Taking $n = p$ a prime number, $T^p - 1 = (T-1)\Phi_p(T)$. Thus, we can explicitly compute

$$\Phi_p(T) = \frac{T^p - 1}{T-1} = 1 + T + T^2 + \cdots + T^{p-1}.$$

Notice the coefficients here all equal 1.

Theorem 7.4. *For every $n \geq 1$, the coefficients of $\Phi_n(T)$ are in $\mathbf{Z}$.*

Proof. We will argue by induction on n. Since $\Phi_1(T) = T - 1$, we can take $n > 1$ and assume $\Phi_m(T)$ has integer coefficients for $m < n$. In Lemma 7.1, we can pull out the term at $d = n$:

$$T^n - 1 = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(T) \cdot \Phi_n(T). \tag{7.3}$$

Let $B_n(T) = \prod_{d|n, d\neq n} \Phi_d(T)$, so

$$T^n - 1 = B_n(T)\Phi_n(T). \tag{7.4}$$

By induction, $\Phi_d(T)$ has integer coefficients when d is a proper divisor of n, so $B_n(T)$ has integer coefficients. Each $\Phi_d(T)$ has leading coefficient 1, so $B_n(T)$ does as well. All we know about $\Phi_n(T)$ is that it has complex coefficients. We want to deduce from (7.4) that its coefficients are integers.

Let's cook up a second divisibility relation between $T^n - 1$ and $B_n(T)$ in a completely different way: the usual division of (complex) polynomials, leaving a quotient and remainder. We have

$$T^n - 1 = B_n(T)Q(T) + R(T), \tag{7.5}$$

where $R(T) = 0$ or $0 \leq \deg R < \deg B_n$. When we divide one polynomial by another and both have integer coefficients, the quotient and remainder may not have integer coefficients. For instance,

$$T^2 + 1 = (2T+1)\left(\frac{1}{2}T - \frac{1}{4}\right) + \frac{5}{4}.$$

However, if the divisor has leading coefficient 1, then everything stays integral, *e.g.*, $T^2+1 = (T+1)(T-1)+2$. Briefly, the source of all denominators in the quotient and remainder comes from the leading coefficient of the divisor, so when it is 1, no denominators are introduced. Thus, since $B_n(T)$ has integer coefficients and leading coefficient 1, $Q(T)$ and $R(T)$ have integer coefficients.

We now compare our two relations (7.4) and (7.5). Since division of polynomials (with, say, complex coefficients) has *unique* quotient and remainder, we must have $\Phi_n(T) = Q(T)$ and $0 = R(T)$. In particular, since $Q(T)$ has integer coefficients, we have proved $\Phi_n(T)$ has integer coefficients! □

Theorem 7.5. *For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic.*

Proof. Consider the factorization

$$T^{p-1} - 1 = \prod_{d|(p-1)} \Phi_d(T). \tag{7.6}$$

All polynomials appearing here have integer coefficients. Collect the $\Phi_d(T)$ with $d \neq p-1$ into a single term:

$$T^{p-1} - 1 = \Phi_{p-1}(T)H(T), \tag{7.7}$$

where $H(T)$ has integer coefficients.

Reducing the coefficients in (7.7) modulo p lets us view (7.7) as a polynomial identity over $\mathbf{Z}/(p)$. By Theorem 5.2, the left side of (7.7) breaks up into distinct linear factors over $\mathbf{Z}/(p)$. Therefore, by unique factorization for polynomials with coefficients in $\mathbf{Z}/(p)$, the two factors on the right side of (7.7) are products of linear polynomials over $\mathbf{Z}/(p)$ (as many linear polynomials as the degree of the factor). Therefore $\Phi_{p-1}(T)$ does have a root (in fact, $\varphi(p-1)$ roots) in $\mathbf{Z}/(p)$. Let $a \in \mathbf{Z}/(p)$ be a root of $\Phi_{p-1}(T)$. Certainly $a \neq 0$, since 0 is not a root of $T^{p-1} - 1$. Thus $a \in (\mathbf{Z}/(p))^\times$. We will show the order of a in $(\mathbf{Z}/(p))^\times$ is $p-1$, so it is a generator.

Let d be the order of a in $(\mathbf{Z}/(p))^\times$, so $d|p-1$. Could we have $d < p-1$? Assume so. (We will get a contradiction and then we will be done.) Since d is the order of a, $a^d - 1 = 0$ in $\mathbf{Z}/(p)$. Now consider the factorization of $T^d - 1$ given by Theorem 7.1:

$$T^d - 1 = \prod_{k|d} \Phi_k(T).$$

This identity between polynomials with integer coefficients can be viewed as an identity between polynomials with coefficients in $\mathbf{Z}/(p)$ by reducing all the coefficients modulo p. Setting $T = a$ in this formula, the left side vanishes (in $\mathbf{Z}/(p)$), so $\Phi_k(a)$ is 0 for some k dividing d. (In fact, it is $\Phi_d(a)$ which vanishes, but we don't need to know that.) Once $\Phi_k(a)$ vanishes, Lemma A.2 tells us $T-a$ is a factor of $\Phi_k(a)$. Thus, in (7.6), $T-a$ is a factor *twice*: once in $\Phi_{p-1}(T)$ (that is how we defined a) and also as a factor in $\Phi_k(T)$ for some k dividing d. But the factorization of $T^{p-1} - 1$ in Theorem 5.2 has *distinct* linear factors. We have a contradiction with unique factorization, so our assumption that $d < p-1$ was in error: $d = p-1$, so a is a generator of $(\mathbf{Z}/(p))^\times$. □

Example 7.6. Taking $p = 7$, $\Phi_{p-1}(T) = \Phi_6(T) = T^2 - T + 1$. Its roots in $\mathbf{Z}/7\mathbf{Z}$ are 3 and 5 (note $\Phi_6(3) = 7$ and $\Phi_6(5) = 21$, which both vanish modulo 7). These are the generators of $(\mathbf{Z}/7\mathbf{Z})^\times$, as you can check directly.

Appendix A. Proof of Theorem 1.1

Theorem 1.1 says that, for any integer $r \geq 1$, there are at most r solutions to the equation $x^r = 1$ in $\mathbf{Z}/(p)$. We are going to prove this as a special case of a more general result.

Theorem A.1. *Let $f(T)$ be a non-constant polynomial with coefficients in $\mathbf{Z}/(p)$, of degree d. Then $f(T)$ has at most d roots in $\mathbf{Z}/(p)$.*

Theorem 1.1 is the special case $f(T) = T^r - 1$.

To prove Theorem A.1, we will need a preliminary lemma connecting roots and linear factors. (We state the theorem with coefficients in either $\mathbf{C}$ or $\mathbf{Z}/(p)$ because both versions are needed in different proofs that $(\mathbf{Z}/(p))^\times$ is cyclic.)

Lemma A.2. *Let $f(T)$ be a non-constant polynomial with coefficients in $\mathbf{C}$ or in $\mathbf{Z}/(p)$. For a in $\mathbf{C}$ or $\mathbf{Z}/(p)$, $f(a) = 0$ if and only if $T - a$ is a factor of $f(T)$.*

Proof. If $T - a$ is a factor of $f(T)$, then $f(T) = (T - a)h(T)$ for some polynomial $h(T)$, and substituting a for T shows $f(a) = 0$.

Conversely, suppose $f(a) = 0$. Write the polynomial as

$$f(T) = c_n T^n + c_{n-1}T^{n-1} + \cdots + c_1 T + c_0, \tag{A.1}$$

where $c_j \in \mathbf{C}$ or $\mathbf{Z}/(p)$ and $c_n \neq 0$. Then

$$0 = c_n a^n + c_{n-1}r^{n-1} + \cdots + c_1 a + c_0. \tag{A.2}$$

Subtracting (A.2) from (A.1), the terms c_0 cancel and we get

$$f(T) = c_n(T^n - a^n) + c_{n-1}(T^{n-1} - a^{n-1}) + \cdots + c_1(T - a). \tag{A.3}$$

Since

$$T^j - a^j = (T - a)(T^{j-1} + aT^{j-2} + \cdots + a^i T^{j-1-i} + \cdots + a^{j-2}T + a^{j-1}),$$

each term on the right side of (A.3) has a factor of $T - a$. Factor this out of each term, and we obtain $f(T) = (T - a)g(T)$, where $g(T)$ is another polynomial with coefficients in $\mathbf{C}$ or $\mathbf{Z}/(p)$. □

Now we prove Theorem A.1.

Proof. We induct on the degree d of $f(T)$. Note $d \geq 1$.

A polynomial of degree 1 has the form $f(T) = aT + b$, where a and b are in $\mathbf{Z}/(p)$ and $a \neq 0$. This has exactly one root in $\mathbf{Z}/(p)$, namely $-b/a$, and thus *at most* one root in $\mathbf{Z}/(p)$. That settles the theorem for $d = 1$.

Now assume the theorem is true for all polynomials with coefficients in $\mathbf{Z}/(p)$ of degree d. We verify the theorem for all polynomials with coefficients in $\mathbf{Z}/(p)$ of degree $d + 1$.

A polynomial of degree $d + 1$ is

$$f(T) = c_{d+1}T^{d+1} + c_d T^d + \cdots + c_1 T + c_0, \tag{A.4}$$

where $c_j \in \mathbf{Z}/(p)$ and $c_{d+1} \neq 0$. If $f(T)$ has no roots in $\mathbf{Z}/(p)$, then we're done, since $0 \leq d + 1$. If $f(T)$ has a root in $\mathbf{Z}/(p)$, say r, then Lemma A.2 tells us $f(T) = (T - r)g(T)$, where $g(T)$ is another polynomial with coefficients in $\mathbf{Z}/(p)$, of degree d (why degree d?). We can therefore apply the inductive hypothesis to $g(T)$ and conclude that $g(T)$ has at most d roots in $\mathbf{Z}/(p)$. Since $f(a) = (a - r)g(a)$, and a product of numbers in $\mathbf{Z}/(p)$ is 0 only when one of the factors is 0 (this would be *false* if our modulus was composite rather than prime!), we see that any root of $f(T)$ in $\mathbf{Z}/(p)$ is either r or is a root of $g(T)$. Thus, $f(T)$ has at most $d + 1$ roots in $\mathbf{Z}/(p)$. As $f(T)$ was an arbitrary polynomial of degree $d + 1$ with coefficients in $\mathbf{Z}/(p)$, we are done with the inductive step. □

Remark A.3. There were two cases considered in the inductive step: when $f(T)$ has a root in $\mathbf{Z}/(p)$ and when it does not. Certainly one of those cases must occur, but in any particular example we don't know which occurs without actually searching for roots. This is why the theorem is not effective. It gives us an upper bound on the number of roots, but does not give us any tools to decide if there is even one root in $\mathbf{Z}/(p)$ for a particular polynomial.