Primitive Roots

Number Theory Handout
12 Feb 2022

1 Prelude: Multiplicative Groups

Given a set that is closed under multiplication, such as any field, or the set of mod n integers $\mathbb{Z}/n\mathbb{Z}$, we can look at the subset of all invertible elements. This subset allows us to do multiplication and division freely without any concerns, it is called the **multiplicative group** $S^\times$ of the original set S.

- The multiplicative group of any field F is $F^\times = F \setminus \{0_F\}$. (Why?)
- The multiplicative group of $\mathbb{Z}/n\mathbb{Z}$ consists of those coprime to n. (Why?)

2 Orders

In this handout, we will focus on multiplicative groups that are commutative $ab = ba$. Don't worry, the examples given in section 1 are all commutative.

Definition. The **order** O_x of x is the smallest positive integer n such that $x^n = 1$, if it exists.

Note. The definition above applies to elements x in any *multiplicative group*. For example, if $x \neq 1$ is a real number, then there is no order. Or if $x \in \mathbb{F}_p^\times$, then there is always an order. If x is complex, there is sometimes an order (when?). We will see other multiplicative groups afterwards. In fact, the 1 in the definition above should be specified as the identity element 1_G of the multiplicative group G, but we will abuse a little bit of notation – I will not draw bars above elements in $\mathbb{F}_p$ either.

Exercise. Prove that if $x^n = 1$ then $O_x \mid n$.

Exercise. Prove that if $x \in \mathbb{F}_p^\times$ then $O_x \mid p - 1$.

Proposition 1. If O_x and O_y are coprime, then $O_{xy} = O_x O_y$.

Proof. Since $(xy)^{O_x O_y} = (x^{O_x})^{O_y} \cdot (y^{O_y})^{O_x} = 1$, we know $O_{xy} \mid O_x O_y$. On the other hand,

$$\begin{aligned} x^{O_{xy}} &= y^{-O_{xy}} \\ x^{O_y O_{xy}} &= y^{-O_y O_{xy}} \\ x^{O_y O_{xy}} &= 1 \end{aligned}$$

and thus $O_x \mid O_y O_{xy}$. But $(O_x, O_y) = 1$, so $O_x \mid O_{xy}$. Similarly $O_y \mid O_{xy}$. $\square$

Proposition 2. If $n \mid O_x$, there exist another element y such that $O_y = n$.

Proof. Write $O_x = mn$. We claim that $O_{x^m} = n$. That $O_{x^m} \mid n$ is obvious. Conversely,

$$1 = (x^m)^{O_{x^m}} = x^{mO_{x^m}} \quad \Rightarrow \quad mn \mid mO_{x^m} \quad \Rightarrow \quad n \mid O_{x^m}$$

and thus $O_{x^m} = n$. $\square$

Proposition 3. Let O_x, O_y be some orders, there exist another order $O_z = \operatorname{lcm}\left(O_x, O_y\right)$.

Proof. Write $O_x = \prod_i p_i^{\alpha_i}$ and $O_y = \prod_i p_i^{\beta_i}$. By proposition 2 there exist orders

$$O_{x'} = \prod_{i:\ \alpha_i \geq \beta_i} p_i^{\alpha_i} \qquad \text{and} \qquad O_{y'} = \prod_{i:\ \alpha_i < \beta_i} p_i^{\beta_i}$$

since they divide O_x and O_y respectively. But they're coprime and multiply to $\operatorname{lcm}\left(O_x, O_y\right)$ (verify!), so by proposition 1 we just pick $z = x'y'$. $\square$

By taking successive lcm, we can deduce the following:

Proposition 4. If we work in a finite multiplicative group, there exists an order that is equal to the lcm of all orders. This is called the *universal order*.

Exercise. Why does the universal order of $\mathbb{F}_p^\times$ divide $p-1$?

Theorem 1. The universal order of $\mathbb{F}_p^\times$ is, in fact, $p-1$.

Proof. The above exercise shows the universal order O divides $p-1$. Conversely, note that $x^O = 1$ for all $x \in \mathbb{F}_p^\times$ because O is a multiple of all orders. Therefore, the polynomial $x^O - 1$ has $p-1$ roots in the field $\mathbb{F}_p$. By comparing degrees, $O \geq p-1$. $\square$

3 Primitive Roots

Theorem 1 is the culmination of this handout. It asserts that, **there is an element with order $p-1$ mod p.** We call such an element g a **primitive root** mod p and write $\langle g \rangle = \mathbb{F}_p^\times$.

Exercise. g is a primitive root mod p if and only if $\{1, g, g^2, \cdots, g^{p-2}\} = \mathbb{F}_p^\times$.

Example. 3 is a primitive root mod 5 because $(1, 3, 3^2, 3^3) = (1, 3, 4, 2)$ in $\mathbb{F}_5$.

Exercise. Find all primitive roots mod 13.

You can safely quote the existence of primitive roots without proof. Primitive roots are extremely useful when we are studying multiplicative properties of mod p numbers. For example, given a mod p integer written in the form g^k, we can see whether or not it has an n-th root mod p by seeing whether $k + (p-1)m$ is a multiple of n for some m (Why?).

4 Another Perspective: Cyclotomic Polynomials

Denote $e^{2\pi ik/n} = \zeta_n^k$.

Consider factoring polynomials in the form $X^n - 1$ in $\mathbb{Z}[x]$:

$$\begin{aligned}
X - 1 &= X - 1 \\
X^2 - 1 &= (X-1)(X+1) \\
X^3 - 1 &= (X-1)(X^2+X+1) \\
X^4 - 1 &= (X-1)(X+1)(X^2+1) \\
X^5 - 1 &= (X-1)(X^4+X^3+X^2+X+1) \\
X^6 - 1 &= (X-1)(X+1)(X^2+X+1)(X^2-X-1)
\end{aligned}$$

The pattern may not look exactly obvious, but if we decompose these irreducible factors in $\mathbb{C}[x]$ there seems to be some pattern:

$$\begin{aligned}
X + 1 &= X - \zeta_2^1 \\
X^2 + X + 1 &= (X - \zeta_3^1)(X - \zeta_3^2) \\
X^2 + 1 &= (X - \zeta_4^1)(X - \zeta_4^3) \\
X^4 + X^3 + X^2 + X + 1 &= (X - \zeta_5^1)(X - \zeta_5^2)(X - \zeta_5^3)(X - \zeta_5^4) \\
X^2 - X - 1 &= (X - \zeta_6^1)(X - \zeta_6^5)
\end{aligned}$$

Hmm... 2 with $\{1\}$, 3 with $\{1,2\}$, 4 with $\{1,3\}$, 5 with $\{1,2,3,4\}$, 6 with $\{1,5\}$... They are the numbers coprime to it! We give the polynomials above a special name:

Definition. The polynomial

$$\Phi_n(X) = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} (X - \zeta_n^k)$$

is called the *n-th cyclotomic polynomial.*

It might not be entirely obvious that $\Phi_n(x) \in \mathbb{Z}[x]$ yet, but something you can show is

Exercise. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Exercise. Use the above exercise to prove that $\Phi_n(x) \in \mathbb{Z}[x]$.

Proposition 5. $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Let $\Phi_n(X) = f(X)g(X)$ and f is irreducible. We prove that for all primes $p \nmid n$ we have that $f(z) = 0 \Rightarrow f(z^p) = 0$ (Why does this imply the result?). Suppose the contrary that $f(z) = 0, f(z^p) \neq 0$, then $g(z^p) = 0$, so z is a root of $g(X^p)$. But f is the minimal polynomial of z, so $f(X) \mid g(X^p)$. Note that a simple generalisation of $(a+b)^p \equiv a^p + b^p \pmod{p}$ gives $g(X^p) \equiv g(X)^p \pmod{p}$. Therefore, reducing mod p, $\overline{f}(X) \mid \overline{g}(X)^p$. This means $\overline{f}$ and $\overline{g}$ has a nontrivial common factor, but $\overline{\Phi_n}(X)$ does not have double roots as $\overline{\Phi_n}'(X) = nX^{n-1} \not\equiv 0 \pmod{p}$! $\square$

Exercise. Let $a \in \mathbb{Z}$. If $\Phi_n(a) \equiv 0 \pmod{p}$, then $a^n \equiv 1 \pmod{p}$. (i.e. are you awake?)

The following result is why all of these matter in number theory:

Theorem 2. Let $a \in \mathbb{Z}$ and $p \nmid n$. If $\Phi_n(a) \equiv 0 \pmod{p}$, then not only $a^n \equiv 1 \pmod{p}$, but also n is the order of a mod p.

Proof. Suppose the contrary that the order of a mod p is m (strictly divides n). Then $p \mid a^m - 1$ and hence $\Phi_d(a) \equiv 0 \pmod{p}$ for some $d \mid m \mid n$. Therefore

$$\Phi_n(x) = \prod_{k|n} \Phi_k(x)$$

has a double root a under mod p (one in $\Phi_d(x)$, one in $\Phi_n(x)$), but

$$\Phi_n'(x) = nx^{n-1}$$

has no common roots with $\Phi_n(x)$ as $p \nmid n$. $\square$

Corollary 2.1. If $a^2 \equiv -1 \pmod{p}$ then $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof. $\Phi_4(a) \equiv 0 \pmod{p}$. By Theorem 2, either $p \mid 4$, or 4 is the order of a mod p, i.e. $4 \mid p - 1$. $\square$

Corollary 2.2. There exists a primitive root mod p.

Proof. Consider $\Phi_{p-1}(x)$. It divides $x^{p-1} - 1$ which splits completely into $(x-1)(x-2)\cdots(x-p+1)$ mod p, therefore there must exist some $\Phi_{p-1}(a) \equiv 0 \pmod{p}$. $\square$

5 General Primitive Roots

We found that there is a primitive root for $\mathbb{F}_p^\times$. How about for other moduli? For which n is there a primitive root for $(\mathbb{Z}/n\mathbb{Z})^\times$? Turns out it is:

Theorem 3. $(\mathbb{Z}/n\mathbb{Z})^\times$ has a primitive root $\Leftrightarrow n = 2, 4, p^k$ or $2p^k$ where p is an odd prime.

Proof. Fun exercise. Remember to use the trick $(g + mp)^k \equiv g^k + kmpg^{k-1} \pmod{p^2}$ etc.

Note. $\mathbb{F}_{p^k}$ and $\mathbb{Z}/p^k\mathbb{Z}$ are different sets! They are only isomorphic when $k = 1$. Otherwise, the former is a field while the latter is not. The field $\mathbb{F}_{p^k}$ is something complicated that I will not talk about, but a sneak peek is that $\mathbb{F}_{p^2} \cong \mathbb{F}_p[\delta]$ where δ is a square root.

6 Problems.

1. Notice that the decimal expansions of $k/7$ are cyclic shifts. Why?

   - $1/7 = 0.\overline{142857}$
   - $2/7 = 0.\overline{285714}$
   - $3/7 = 0.\overline{428571}$
   - $4/7 = 0.\overline{571428}$
   - $5/7 = 0.\overline{714285}$
   - $6/7 = 0.\overline{857142}$

2. How many primitive roots are there in $\mathbb{F}_p^\times$?

3. Find the remainder of

$$1^k + 2^k + \cdots + (p-1)^k$$

   when divided by p.

4. Find all positive integers n such that $n \mid 2^n - 1$.

5. (IMOSL1997) Show that if an infinite arithmetic progression of positive integers contains a square and a cube, it must contain a sixth power.

6. (IMOSL2006) Prove that

$$\frac{x^7-1}{x-1} = y^5 - 1$$

   has no integer solutions.

7. (USATST2008) Prove that $x^7 + 7$ cannot be a perfect square for all positive integers n.

References

[1] *Olympiad Number Theory: An Abstract Perspective* by Thomas J. Mildorf

[2] *Orders Modulo A Prime* by Evan Chen