

MATH 361: NUMBER THEORY — SEVENTH LECTURE

1. THE UNIT GROUP OF $\mathbf{Z}/n\mathbf{Z}$

Consider a nonunit positive integer,

$$n = \prod p^{e_p} > 1.$$

The Sun Ze Theorem gives a ring isomorphism,

$$\mathbf{Z}/n\mathbf{Z} \cong \prod \mathbf{Z}/p^{e_p}\mathbf{Z}.$$

The right side is the cartesian product of the rings $\mathbf{Z}/p^{e_p}\mathbf{Z}$, meaning that addition and multiplication are carried out componentwise. It follows that the corresponding unit group is

$$(\mathbf{Z}/n\mathbf{Z})^\times \cong \prod (\mathbf{Z}/p^{e_p}\mathbf{Z})^\times.$$

Thus to study the unit group $(\mathbf{Z}/n\mathbf{Z})^\times$ it suffices to consider $(\mathbf{Z}/p^e\mathbf{Z})^\times$ where p is prime and $e > 0$. Recall that in general,

$$|(\mathbf{Z}/n\mathbf{Z})^\times| = \phi(n),$$

so that for prime powers,

$$|(\mathbf{Z}/p^e\mathbf{Z})^\times| = \phi(p^e) = p^{e-1}(p-1),$$

and especially for primes.

$$|(\mathbf{Z}/p\mathbf{Z})^\times| = p-1.$$

Here are some examples of unit groups modulo prime powers.

$$\begin{aligned} (\mathbf{Z}/2\mathbf{Z})^\times &= (\{1\}, \cdot) = (\{2^0\}, \cdot) \cong (\{0\}, +) = \mathbf{Z}/\mathbf{Z}, \\ (\mathbf{Z}/3\mathbf{Z})^\times &= (\{1, 2\}, \cdot) = (\{2^0, 2^1\}, \cdot) \cong (\{0, 1\}, +) = \mathbf{Z}/2\mathbf{Z}, \\ (\mathbf{Z}/4\mathbf{Z})^\times &= (\{1, 3\}, \cdot) = (\{3^0, 3^1\}, \cdot) \cong (\{0, 1\}, +) = \mathbf{Z}/2\mathbf{Z}, \\ (\mathbf{Z}/5\mathbf{Z})^\times &= (\{1, 2, 3, 4\}, \cdot) = (\{2^0, 2^1, 2^2, 2^3\}, \cdot) \\ &\cong (\{0, 1, 2, 3\}, +) = \mathbf{Z}/4\mathbf{Z}, \\ (\mathbf{Z}/7\mathbf{Z})^\times &= (\{1, 2, 3, 4, 5, 6\}, \cdot) = (\{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\}, \cdot) \\ &\cong (\{0, 1, 2, 3, 4, 5\}, +) = \mathbf{Z}/6\mathbf{Z}, \\ (\mathbf{Z}/8\mathbf{Z})^\times &= (\{1, 3, 5, 7\}, \cdot) = (\{3^0 5^0, 3^1 5^0, 3^0 5^1, 3^1 5^1\}, \cdot) \\ &\cong (\{0, 1\} \times \{0, 1\}, +) = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \\ (\mathbf{Z}/9\mathbf{Z})^\times &= (\{1, 2, 4, 5, 7, 8\}, \cdot) = (\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\}, \cdot) \\ &\cong (\{0, 1, 2, 3, 4, 5\}, +) = \mathbf{Z}/6\mathbf{Z}. \end{aligned}$$

2. THE UNIT GROUP STRUCTURE FOR PRIMES

Proposition 2.1. *Let k be a field. Let the polynomial $f \in k[X]$ have degree $d \geq 1$. Then f has at most d roots in k .*

Naturally, the field that we have in mind here is $k = \mathbf{Z}/p\mathbf{Z}$.

The proposition does require that k be a field, not merely a ring. For example, the polynomial $X^2 - 1$ over the ring $\mathbf{Z}/24\mathbf{Z}$ has for its roots

$$\{1, 5, 7, 11, 13, 17, 19, 23\} = (\mathbf{Z}/24\mathbf{Z})^\times.$$

Proof. If f has no roots then we are done. Otherwise let $a \in k$ be a root. Write

$$f(X) = q(X)(X - a) + r(X), \quad \deg(r) < 1 \text{ or } r = 0.$$

Thus $r(X)$ is a constant. Substitute a for X to see that in fact $r = 0$, and so $f(X) = q(X)(X - a)$. By induction, q has at most $d - 1$ roots in k and we are done. \square

Since $(\mathbf{Z}/p\mathbf{Z})^\times$ is a finite subgroup of the unit group of a field, the general structure theorem for finitely generated abelian groups quickly shows that it must be cyclic. Briefly, for $p > 2$ we have

$$(\mathbf{Z}/p\mathbf{Z})^\times \cong \mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z} \times \cdots \times \mathbf{Z}/d_k\mathbf{Z}, \quad k \geq 1, 1 < d_1 \mid d_2 \cdots \mid d_k.$$

By the proposition, the polynomial $X^{d_k} - 1$ has $d_1 d_2 \cdots d_k$ roots in $\mathbf{Z}/p\mathbf{Z}$, forcing $k = 1$ and thus making $(\mathbf{Z}/p\mathbf{Z})^\times$ cyclic.

However, we proceed by more elementary methods.

The proposition says that a polynomial can not have more roots than its degree. On the other hand, Fermat's Little Theorem ($a^{p-1} = 1$ for all $a \in (\mathbf{Z}/p\mathbf{Z})^\times$) says that the polynomial

$$f(X) = X^{p-1} - 1$$

has a full contingent of $p - 1$ roots in the field $k = \mathbf{Z}/p\mathbf{Z}$.

For any divisor d of $p - 1$, consider the factorization (in consequence of the finite geometric sum formula)

$$f(X) = X^{p-1} - 1 = (X^d - 1) \sum_{i=0}^{\frac{p-1}{d}-1} X^{id} \stackrel{\text{call}}{=} g(X)h(X).$$

We know that

- f has $p - 1$ roots in $\mathbf{Z}/p\mathbf{Z}$,
- g has at most d roots in $\mathbf{Z}/p\mathbf{Z}$,
- h has at most $p - 1 - d$ roots in $\mathbf{Z}/p\mathbf{Z}$.

It follows that $g(X) = X^d - 1$ where $d \mid p - 1$ has d roots in $\mathbf{Z}/p\mathbf{Z}$.

Now factor $p - 1$,

$$p - 1 = \prod q^{e_q}.$$

For each factor q^e of $p - 1$,

$$\begin{aligned} X^{q^e} - 1 & \text{ has } q^e \text{ roots in } \mathbf{Z}/p\mathbf{Z}, \\ X^{q^{e-1}} - 1 & \text{ has } q^{e-1} \text{ roots in } \mathbf{Z}/p\mathbf{Z}, \end{aligned}$$

and so $(\mathbf{Z}/p\mathbf{Z})^\times$ contains $q^e - q^{e-1} = \phi(q^e)$ elements x_q of order q^e . (The order of an element is the smallest positive number of times that the element is multiplied by itself to give 1.) Plausibly,

$$\text{any product } \prod_q x_q \text{ has order } \prod_q q^{e_q} = p - 1,$$

and certainly there are $\phi(p - 1)$ such products. In sum, we have done most of the work of showing

Proposition 2.2. *Let p be prime. Then $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic, with $\phi(p-1)$ generators.*

The loose end is as follows.

Lemma 2.3. *In a multiplicative group, consider two elements whose orders are coprime. Then the order of their product is the product of their orders.*

Proof. We have $a^e = b^f = 1$, and so

$$(ab)^{ef} = (a^e)^f (b^f)^e = 1^f 1^e = 1.$$

Also we have $(e, f) = 1$. So for any positive integer d ,

$$(ab)^d = 1 \implies 1 = ((ab)^d)^e = (a^e b^e)^d = b^{ed} \implies f \mid ed \implies f \mid d,$$

and symmetrically $e \mid d$. Thus $ef \mid d$ □

3. THE UNIT GROUP STRUCTURE FOR ODD PRIME POWERS

Proposition 3.1. *Let p be an odd prime, and let e be any positive integer. Then the multiplicative group modulo p^e is cyclic,*

$$(\mathbf{Z}/p^e\mathbf{Z})^\times \cong \mathbf{Z}/\phi(p^e)\mathbf{Z}.$$

That is, there is a generator $g \pmod{p^e}$ such that

$$(\mathbf{Z}/p^e\mathbf{Z})^\times \cong \{1, g, g^2, \dots, g^{\phi(p^e)-1}\} \cong \{0, 1, 2, \dots, \phi(p^e) - 1\}.$$

Proof. Let g generate $(\mathbf{Z}/p\mathbf{Z})^\times$. Since

$$(g + p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p \pmod{p^2} \neq g^{p-1} \pmod{p^2},$$

it follows that

$$g^{p-1} \not\equiv 1 \pmod{p^2} \quad \text{or} \quad (g + p)^{p-1} \not\equiv 1 \pmod{p^2}.$$

So after replacing g with $g + p$ if necessary, we may assume that $g^{p-1} \not\equiv 1 \pmod{p^2}$. Thus we know that

$$g^{p-1} = 1 + k_1 p, \quad p \nmid k_1.$$

By the Binomial Theorem,

$$\begin{aligned} g^{p(p-1)} &= (1 + k_1 p)^p = 1 + pk_1 p + \sum_{j=2}^{p-1} \binom{p}{j} k_1^j p^j + k_1^p p^p \\ &= 1 + k_2 p^2, \quad p \nmid k_2. \end{aligned}$$

The last equality holds because the terms in the sum and the term $k_1^p p^p$ are multiples of p^3 . (Here it is relevant that $p > 2$. The assertion fails for $p = 2, g = 3$ because of

the last term. That is, $3^{2-1} = 1 + 1 \cdot 2$ so that $k_1 = 1$ is not divisible by $p = 2$, but then $3^{2(2-1)} = 9 = 1 + 2 \cdot 2^2$ so that $k_2 = 2$ is.) Again by the Binomial Theorem,

$$\begin{aligned} g^{p^2(p-1)} &= (1 + k_2 p^2)^p = 1 + p k_2 p^2 + \sum_{j=2}^p \binom{p}{j} k_2^j p^{2j} \\ &= 1 + k_3 p^3, \quad p \nmid k_3, \end{aligned}$$

because the terms in the sum are multiples of p^4 . Similarly

$$g^{p^3(p-1)} = 1 + k_4 p^4, \quad p \nmid k_4,$$

and so on, up to

$$g^{p^{e-2}(p-1)} = 1 + k_{e-1} p^{e-1}, \quad p \nmid k_{e-1}.$$

That is,

$$g^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}.$$

The order of g in $(\mathbf{Z}/p^e\mathbf{Z})^\times$ must divide $\phi(p^e) = p^{e-1}(p-1)$. If the order takes the form $p^\varepsilon d$ where $\varepsilon \leq e-1$ and d is a *proper* divisor of $p-1$ then Fermat's Little Theorem ($g^p = g \pmod{p}$) shows that the relation

$$g^{p^\varepsilon d} = 1 \pmod{p^e}$$

reduces modulo p to

$$g^d = 1 \pmod{p}.$$

But this contradicts the fact that g is a generator modulo p . Thus the order of g in $(\mathbf{Z}/p^e\mathbf{Z})^\times$ takes the form $p^\varepsilon(p-1)$ where $\varepsilon \leq e-1$. The calculation above has shown that $\varepsilon = e-1$, and the proof is complete. \square

For example, 2 generates $(\mathbf{Z}/5\mathbf{Z})^\times$, and $2^{5-1} = 16 \not\equiv 1 \pmod{5^2}$, so in fact 2 generates $(\mathbf{Z}/5^e\mathbf{Z})^\times$ for all $e \geq 1$.

A small consequence of the proposition is that since $(\mathbf{Z}/p^e\mathbf{Z})^\times$ is cyclic for odd p , and since $\phi(p^e) = p^{e-1}(p-1)$ is even, the equation

$$x^2 = 1 \pmod{p^e}$$

has two solutions: 1 and $g^{\phi(p^e)/2}$.

4. THE UNIT GROUP STRUCTURE FOR POWERS OF 2

Proposition 4.1. *The structure of the unit group $(\mathbf{Z}/2^e\mathbf{Z})^\times$ is*

$$(\mathbf{Z}/2^e\mathbf{Z})^\times \cong \begin{cases} \mathbf{Z}/\mathbf{Z} & \text{if } e = 1, \\ \mathbf{Z}/2\mathbf{Z} & \text{if } e = 2, \\ (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2^{e-2}\mathbf{Z}) & \text{if } e \geq 3. \end{cases}$$

Specifically, $(\mathbf{Z}/2\mathbf{Z})^\times = \{1\}$, $(\mathbf{Z}/4\mathbf{Z})^\times = \{1, 3\}$, and for $e \geq 3$,

$$(\mathbf{Z}/2^e\mathbf{Z})^\times \cong \{\pm 1\} \times \{1, 5, 5^2, \dots, 5^{2^{e-2}-1}\}.$$

Proof. The results for $(\mathbf{Z}/2\mathbf{Z})^\times$ and for $(\mathbf{Z}/4\mathbf{Z})^\times$ are readily observable, and so we take $e \geq 3$.

Since $|(\mathbf{Z}/2^e\mathbf{Z})^\times| = \phi(2^e) = 2^{e-1}$, we need to show that

$$5^{2^{e-3}} \not\equiv 1 \pmod{2^e}, \quad 5^{2^{e-2}} \equiv 1 \pmod{2^e},$$

Similarly, to the previous argument, start from

$$5^{2^0} = 5 = 1 + k_2 2^2, \quad 2 \nmid k_2,$$

and thus

$$5^{2^1} = 5^2 = 1 + 2k_2 2^2 + k_2^2 2^4 = 1 + k_3 2^3, \quad 2 \nmid k_3,$$

and then

$$5^{2^2} = 5^4 = 1 + 2k_3 2^3 + k_3^2 2^6 = 1 + k_4 2^4, \quad 2 \nmid k_4,$$

and so on up to

$$5^{2^{e-3}} = 1 + k_{e-1} 2^{e-1}, \quad 2 \nmid k_{e-1},$$

and finally

$$5^{2^{e-2}} = 1 + k_e 2^e, \quad 2 \nmid k_e.$$

The last two displays show that

$$5^{2^{e-3}} \not\equiv 1 \pmod{2^e}, \quad 5^{2^{e-2}} \equiv 1 \pmod{2^e}.$$

That is, 5 generates half of $(\mathbf{Z}/2^e\mathbf{Z})^\times$. To show that the full group is

$$(\mathbf{Z}/2^e\mathbf{Z})^\times \cong \{\pm 1\} \times \{1, 5, 5^2, \dots, 5^{2^{e-2}-1}\},$$

suppose that

$$(-1)^a 5^b = (-1)^c 5^d \pmod{2^e}, \quad a, c \in \{0, 1\}, \quad b, d \in \{0, \dots, 2^{e-2} - 1\}.$$

Inspect modulo 4 to see that $c = a$. So now $5^b = 5^d \pmod{2^e}$, and the restrictions on b and d show that $d = b$ as well. \square

The group $(\mathbf{Z}/2^e\mathbf{Z})^\times$ is not cyclic for $e \geq 3$ because all of its elements have order dividing 2^{e-2} .

The equation

$$x^2 = 1 \pmod{2^e}$$

has one solution if $e = 1$, two solutions if $e = 2$, and four solutions if $e \geq 3$,

$$(1, 1), \quad (-1, 1), \quad (1, 5^{2^{e-3}}), \quad (-1, 5^{2^{e-3}}).$$

With this information in hand, the Sun Ze Theorem shows that the number of solutions of the equation

$$x^2 = 1 \pmod{n}, \quad (\text{where } n = 2^e \prod_{i=1}^g p_i^{e_i})$$

is

$$\begin{cases} 2^g & \text{if } e = 0, 1, \\ 2 \cdot 2^g & \text{if } e = 2, \\ 4 \cdot 2^g & \text{if } e \geq 3. \end{cases}$$

For example, if $n = 120 = 2^3 \cdot 3 \cdot 5$ then the number of solutions is 16.

And in general, if n is odd then the number of solutions is 2 if and only if n is a prime power. This is the idea behind the Miller–Rabin primality test.

5. CYCLIC UNIT GROUPS $(\mathbf{Z}/n\mathbf{Z})^\times$

Consider a positive nonunit integer

$$n = \prod_i p_i^{e_i}.$$

Recall the multiplicative component of the Sun Ze Theorem,

$$(\mathbf{Z}/n\mathbf{Z})^\times \xrightarrow{\sim} \prod (\mathbf{Z}/p^{e_p}\mathbf{Z})^\times, \quad a \bmod n \longmapsto (a \bmod p_1^{e_1}, \dots, a \bmod p_k^{e_k}).$$

Consequently, the order of a divides the least common multiple of the orders of the multiplicand-groups,

$$\text{lcm}\{\phi(p_1^{e_1}), \dots, \phi(p_k^{e_k})\},$$

and thus a can not conceivably have order $\phi(n)$ unless all of the $\phi(p_i^{e_i})$ are coprime.

For each odd p , the totient $\phi(p^e)$ is even for all $e \geq 1$. So for $(\mathbf{Z}/n\mathbf{Z})^\times$ to be cyclic, n can have at most one odd prime divisor. Also, $2 \mid \phi(2^e)$ for all $e \geq 2$. So the possible unit groups $(\mathbf{Z}/n\mathbf{Z})^\times$ that could be cyclic are

$$(\mathbf{Z}/2\mathbf{Z})^\times, \quad (\mathbf{Z}/4\mathbf{Z})^\times, \quad (\mathbf{Z}/p^e\mathbf{Z})^\times, \quad (\mathbf{Z}/2p^e\mathbf{Z})^\times.$$

We know that the first three groups in fact are cyclic. For $n = 2p^e$, the Sun Ze Theorem gives

$$(\mathbf{Z}/2p^e\mathbf{Z})^\times \cong (\mathbf{Z}/2\mathbf{Z})^\times \times (\mathbf{Z}/p^e\mathbf{Z})^\times \cong (\mathbf{Z}/p^e\mathbf{Z})^\times,$$

showing that the fourth group is cyclic as well. If g generates $(\mathbf{Z}/p^e\mathbf{Z})^\times$ then whichever of g and $g + p^e$ is odd generates $(\mathbf{Z}/2p^e\mathbf{Z})^\times$.