Math 1560 - Notes 5

Ian Benway

15 February 2022

1 Cyclicity of Group of Units mod Odd Prime Powers

From last lecture:

Proposition. *If p is a prime, and if $d|(p-1)$, then the polynomial $x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ has exactly d roots in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

New corollary:

Corollary. *The group of units $G := (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.*

Proof. For $d|(p-1)$, write $\psi(d)$ for the number of elements of G with order d.

The proposition above implies that

$$\sum_{c|d} \psi(c) = d \qquad\qquad (\psi * i = id).$$

The Möbius Inversion give

$$\phi(d) = \sum_{c|d} \mu(c)\frac{d}{c}.$$

On the other hand, $id = \phi * id$ implies that $\phi = \mu * id$. Thus $\psi(d) = \phi(d)$ for all $d|(p-1)$; so in particular $\psi(p-1) = \phi(p-1) \geq 1$ for any prime p. □

We come to our first piece in classifying cyclicity in groups of units modulo some number, which has the longest proof of this semester:

Theorem 1. *Let $p \in \mathbb{Z}_+$ be an odd prime, and let $e \geq 1$. Then $U(p^e)$ is cyclic.*

We'll start with an overview of the proof:

1. Pick a primitive root p. Call it g.
2. Show that either g or $g + p$ is a primitive root mod p^2.
3. Show that if h is any primitive root mod p^2, then h is a primitive root mod p^e for all $e \geq 2$.

Proof. Let g be a primitive root mod p, and let d be the order of $g \mod p^2$. Since $\phi(p^2) = p(p-1)$, we have $d|p(p-1)$, by Lagrange's Theorem.

By definition of d,

$$g^d \equiv 1 \mod p^2$$
$$g^d \equiv 1 \mod p.$$

Thus $(p-1)|d$, so altogether $d = p-1$ or $p(p-1)$. If the latter, we're done with Step 2, so assume the former. Let $h = g + p$. We know that h is a primitve root mod p, so the order of $h \mod p^2$ is either $p-1$ or $p(p-1)$.

By our new hypothesis,

$$g^{p-1} \equiv 1 \mod p^2, \text{ so module } p^2 \text{ we have}$$
$$h^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2} \cdot p + \cdots + p^{p-1} \text{ by the binomial theorem}$$
$$\equiv 1 - pg^{p-2} \mod p^2.$$

But $p \nmid g$, so $pg^{p-1} \not\equiv 0 \mod p$, and hence $h^{p-1} \not\equiv 1 \mod p^2$. Thus the order of h mod p^2 is $p(p-1)$, so h generates $U(p^2)$.
So if g is a primitive root $\mod p$, then either g or $g+p$ is a primitive root mod p^2.

Let h be a primitive root mod p^e for some fixed $e \geq 2$. Let d be the order of h mod p^{e+1}. Then $d|\phi(p^{e+1}) = p^e(p-1)$ by Lagrange, and just as argued in Step 2,

$$\phi(p^e) = p^{e-1}(p-1)|d.$$

Hence, $d = p^e(p-1)$ or $p^{e-1}(p-1)$. If the former, then we are done, so assume the latter.

Our goal now is to show that

$$h^{p^{e-1}(p-1)} \neq 1 \mod p^{e+1},$$

implying that $d = p^e(p-1)$ after all.

Since h has order $\phi(p^e) = p^{e-1}(p-1)$ in $U(p^e)$, we have

$$h^{p^{e-2}(p-1)} \neq 1 \mod p^e. \tag{1}$$

However,

$$h^{p^{e-2}(p-1)} \equiv 1 \mod p^{e-1} \tag{2}$$

by Euler's Theorem.

Combining (1) and (2) yields

$$h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$$

where $p \nmid k$. Therefore

$$\begin{aligned} h^{p^{e-1}(p-1)} &= (1+kp^{e-1})^p \\ &= 1 + pkp^{e-1} + \binom{p}{2} k^2 p^{2e-2} + \dots. \end{aligned}$$

Subsequent terms are all divisible by $p^{3e-3} = (p^{e-1})^3$, and hence by p^{e+1};

$$3(e-1) \geq e+1 \quad \forall e \geq 2.$$

Thus,

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e + \frac{1}{2}k^2 p^{2e-1}(p-1) \mod p^{e+1}.$$

We have that p is odd, so $\frac{k^2 p^{2e-1}(p-1)}{2}$ is divisible by p^{e+1}, since $2e-1 \geq e+1$, $\forall e \geq 2$.
Thus,

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^2 \mod p^{e+1}.$$

Since $p \nmid k$, we get that

$$h^{p^{e-1}(p-1)} \not\equiv 1 \mod p^{e+1}.$$

This proves that $d = p^e(p-1)$, which is to say that h is a primitive root mod p^{e+1}. □

2 Non-cyclicity of Unit Group mod 2^e, $e \geq 3$

Theorem 2. *$U(2^e)$ is cyclic if and only if $e = 1$ or $e = 2$.*

Proof. Clearly $U(2)$ and $U(4)$ are cyclic. So we show that $U(2^e)$ is *not* cyclic.
Notice that it suffices to show that $U(8)$ is **not** cyclic.

$$U(8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \text{ and } \bar{1}^2 = \bar{3}^2 = \bar{5}^2 = \bar{7}^2 \mod 8.$$

□

Corollary. *$U(m)$ is cyclic if and only if $m = 1, 2, 4, p^e$, or $2p^e$ for some odd prime p.*

Proof. Recall that a product G of finite cyclic groups G_1 and G_2 is cyclic if and only if $(|G_1|, |G_2|) = 1$.

On the other hand, $\phi(m)$ is even $\forall m \geq 3$. Combined with our structure theorems above on $U(p^e)$ for primes p, this proves the corollary. □