Recall: We were proving that "there are $\phi(d)$ units of order d modulo p when $d \mid p-1$" by induction on d.

Base case: $d = 1$ ✓

Inductive step: Assume true until some $d \mid p-1$ and prove d. We showed that there are

$$d - \sum_{\substack{d' \mid d \\ d' \neq d}} \phi(d')$$

units of order d.

It is remained to show

$$d - \sum_{\substack{d' \mid d \\ d' \neq d}} \phi(d') = \phi(d)$$

which can be rewritten as

$$d = \sum_{d' \mid d} \phi(d') .$$

Now, our proof is complete with the following lemma.

Lemma: $\displaystyle\sum_{m|n} \phi(m) = n$

$$\phi(1) + \phi(2) + \phi(3) + \phi(6)$$
$$= 1 + 1 + 2 + 2$$
$$= 6$$

Proof: "The idea of the proof"

$p \neq q$ primes, $n = pq$.

$$\Rightarrow \text{LHS} = \phi(1) + \phi(p) + \phi(q) + \phi(pq)$$

$\phi(pq)$

$\phi(p)$

$$= (\phi(1) + \phi(p)) \cdot (\phi(1) + \phi(q))$$

multiplicativity

$\phi(m) \cdot \phi(n) = \phi(mn)$

for $(m,n) = 1$.

$\phi(1)$ $\phi(q)$

This idea can be used for the sums

$\displaystyle\sum_{m|n} f(m)$ when f is multiplicative.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\begin{aligned}\sum_{m|n} \phi(m) = &\left(\phi(1) + \phi(p_1) + \phi(p_1^2) + \ldots + \phi(p_1^{\alpha_1})\right) \\ &\times \left(\phi(1) + \phi(p_2) + \phi(p_2^2) + \ldots + \phi(p_2^{\alpha_2})\right) \\ &\vdots \\ &\times \left(\phi(1) + \phi(p_k) + \phi(p_k^2) + \ldots + \phi(p_k^{\alpha_k})\right)\end{aligned}$$

$$\phi(1) + \phi(p_1) + \phi(p_1^2) + \dots + \phi(p_1^{\alpha_1})$$

$$= 1 + p_1 \cdot \frac{p_1 - 1}{p_1} + p_1^2 \cdot \frac{p_1 - 1}{p_1} + \dots + p_1^{\alpha_1} \cdot \frac{p_1 - 1}{p_1}$$

$$= 1 + (p_1 - 1) \cdot \left(1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1 - 1}\right)$$

$$= 1 + (p_1 - 1) \cdot \frac{p_1^{\alpha_1} - 1}{p_1 - 1}$$

$$= p_1^{\alpha_1}$$

So, $\sum_{m|n} \phi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n.$ ∎

Some applications

① (Wilson's Theorem) $(p-1)! \equiv -1 \pmod{p}$

g is a primitive root mod p and assume $p \neq 2$. ($p = 2$ case is obvious)

$$\{1, 2, \dots, p-1\} \equiv \{g, g^2, \dots, g^{p-1}\} \pmod{p}$$

$$\Rightarrow (p-1)! \equiv g^1 \cdot g^2 \cdot \dots \cdot g^{p-1} \pmod{p}$$

$$\equiv g^{1+2+\dots+p-1} \pmod{p}$$

$$\equiv g^{\frac{(p-1)p}{2}} \pmod{p}$$

$1 \equiv (g^{p-1})^{\frac{p-1}{2}} \cdot g^{\frac{p-1}{2}} \pmod p$

$\equiv g^{\frac{p-1}{2}} \pmod p$

Say $x \equiv g^{\frac{p-1}{2}} \pmod p$, then

- $x^2 \equiv g^{p-1} \equiv 1 \pmod p \Rightarrow x^2 - 1 \equiv 0 \pmod p$

  $\Rightarrow (x-1)\cdot(x+1) \equiv 0 \pmod p$

  $\Rightarrow x \equiv 1$ or $-1 \pmod p$

- $x \not\equiv 1 \pmod p$ because g is a primitive root.

$\Rightarrow x \equiv -1 \pmod p$.

② Finding n^{th} roots (solving $x^n \equiv a \pmod p$)

Suppose we want to solve $x^{15} \equiv 6 \pmod{101}$ and we know

- 2 is a primitive root modulo 101, and
- $6 \equiv 2^{70} \pmod{101}$

x must be a unit, so we can write

$x \equiv 2^a \pmod{101}$

$x^{15} \equiv 6 \pmod{101} \iff 2^{15a} \equiv 2^{70} \pmod{101}$

$g^k \equiv g^\ell \pmod{p} \quad \iff 15a \equiv 70 \pmod{100}$

$g^{k-\ell} \equiv 1 \pmod{p} \iff 3a \equiv 14 \pmod{20}$

$p-1 \mid k-\ell \qquad \iff 7 \cdot 3 \cdot a \equiv 7 \cdot 14 \pmod{20}$

$k \equiv \ell \pmod{p-1} \iff a \equiv 18 \pmod{20}$

So, $x \equiv 2^{18}, 2^{38}, 2^{58}, 2^{78}, 2^{98} \pmod{101}$

no need to write 2^{118} because
$2^{18} \equiv 2^{118} \pmod{101}$

(3) (Back to Carmichael numbers) n is a Carmichael number when $a^n \equiv a \pmod{n}$ for every a.

The other direction of the following theorem was left as an exercise in Lecture 13.

Theorem: If n is a Carmichael number, then

1. $n = p_1 p_2 \cdots p_k$ is a product of distinct primes and

2. $p_i - 1 \mid n-1$ for all i.

Proof: (1) This means $p^2 \nmid n$ for primes p.

Suppose $p^2 \mid n$ and n is Carmichael. Then

$$p^n \equiv p \pmod{n} \Rightarrow p^n \equiv p \pmod{p^2}$$

$$\Rightarrow 0 \equiv p \pmod{p^2}$$, contradiction.

So, $n = p_1 p_2 \cdots p_k$.

(2) $a^n \equiv a \pmod{n} \Rightarrow a^n \equiv a \pmod{p_i}$

Choose a as a primitive root mod p_i, then

$$a^n \equiv a \pmod{p_i} \Rightarrow a^{n-1} \equiv 1 \pmod{p_i}$$

$$\Rightarrow p_i - 1 \mid n - 1.$$

Next, we investigate primitive roots modulo n in general.

Definition: We say g is a primitive root modulo n if it generates all units of $\mathbb{Z}_n$, i.e.

$$\{1 \leq u \leq n : (u,n) = 1\} \equiv \{g, g^2, g^3, \ldots, g^{\phi(n)}\} \pmod{n}$$

The following results are analogous to $n=p$ case and can be proved in the same way.

Theorem: g is a primitive root modulo n if and only if $\operatorname{ord}_n(g) = \phi(n)$.

Theorem: If g is a primitive root modulo n, then

$$g^k \equiv 1 \pmod{n} \iff \phi(n) \mid k .$$

Theorem: $\operatorname{ord}_n(g^a) = \dfrac{\phi(n)}{(\phi(n), a)}$

Theorem: Suppose $\mathbb{Z}_n$ has a primitive root and d is a positive divisor of $\phi(n)$. Then, there are exactly $\phi(d)$ units of order d. In particular, there will be $\phi(\phi(n))$ primitive roots in $\mathbb{Z}_n$.

Now, the existence of a primitive root.

It doesn't always exist!

Example: $n = 8$. $\Rightarrow \phi(n) = 4$

$$\begin{array}{rcl} \text{Units in } \mathbb{Z}_8 & = & \{1, 3, 5, 7\} \\ & & \ \ \downarrow\ \ \downarrow\ \ \downarrow\ \ \downarrow \\ \text{orders :} & & \ \ 1\ \ \ 2\ \ \ 2\ \ \ 2 \end{array}$$

There is nothing of order $\phi(8) = 4$.

Which $\mathbb{Z}_n$ has primitive root?

Spoiler: exactly when

- $n = 1, 2, 4$ or $\rightarrow$ obvious. just check
- $n = p^m$ or $\rightarrow$ Step 1 (p odd prime)
- $n = 2 \cdot p^m \rightarrow$ Step 2

Step 3: otherwise, there is no primitive root.

We'll prove this step by step

Begin with Step-1 and we should first do the case $m = 2$ (we already did $m=1$)

Lemma: Let g be a primitive root mod p. Then either g or $g+p$ is a primitive root modulo p^2. So, $\mathbb{Z}_{p^2}$ has a primitive root.

Proof: Note that $\phi(p^2) = p \cdot (p-1)$

Say $\mathrm{ord}_{p^2}(g) = k$, then

- $k \mid p \cdot (p-1)$ because $g^{\phi(p^2)} \equiv 1 \pmod{p^2}$
- $g^k \equiv 1 \pmod{p^2} \Rightarrow g^k \equiv 1 \pmod{p}$
$\Rightarrow p-1 \mid k$

From $p-1 \mid k \mid (p-1)\cdot p$, we get

$$\underbrace{k = p-1}_{\text{not a primitive root}} \quad \text{or} \quad \underbrace{k = p\cdot(p-1)}_{\text{primitive root}}$$

Do the same thing for $g+p$ instead of g and we again get

$$\operatorname{ord}_{p^2}(g+p) = p-1 \quad \text{or} \quad p\cdot(p-1).$$

If $\operatorname{ord}_{p^2}(g) = k = p\cdot(p-1)$, then g is a primitive root modulo p^2 and we are done.

So, we can assume $\operatorname{ord}_{p^2}(g) = p-1$

Goal: prove $\operatorname{ord}_{p^2}(g+p) = p\cdot(p-1)$ or equivalently

$$\operatorname{ord}_{p^2}(g+p) \neq p-1$$

It is enough to show that

Binomial Theorem

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

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \overbrace{\binom{p-1}{2}g^{p-3}p^2 + \dots + \binom{p-1}{p-1}g^0 p^{p-1}}^{\text{all } 0 \pmod{p^2}}$$

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

$\text{ord}_{p^2}(g) = p-1$

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

$$\not\equiv 1 \pmod{p^2}$$

because $(p-1) \cdot p \cdot g^{p-2} \not\equiv 0 \pmod{p^2}$. ■

We'll complete Step 1 on Wednesday.