Section 9.2

Q: Which integers have primitive roots?

Partial Answer:

Yes: 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, 22, 23, 25, 26, 27, 29

No: 8, 12, 15, 16, 20, 21, 24, 28, 30

Goal: If p is prime, then p has a primitive root

Rephrase: $(\mathbb{Z}/p\mathbb{Z})^{\times} \cong \mathbb{Z}/(p-1)\mathbb{Z}$

Ask yourself: Why do we need a prime?

Thm: Let p be prime and let d be a pos. divisor of $p-1$ (i.e. $d \mid \varphi(p)$)

The the number of incongruent integers mod p of order d is equal to $\varphi(d)$.

Question: How does this imply that every prime has a primitive root?

Answer. Take $d = p-1$, so d is a divisor of $p-1$

$\rightarrow$ so there are $\varphi(p-1)$ elts. of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order $d = p-1 = \varphi(p)$

since $\varphi(p-1) \neq 0$, so some integer has order $\varphi(p)$, i.e. is a primitive root.

Q: How does this theorem fit into context we understand?

Section 9.1: If $n \in \mathbb{Z}_{>0}$ has a prim. root, then there are $\varphi(\varphi(n))$ prim. roots mod n

↳ apply to $n = p$ prime

↳ "if $(\mathbb{Z}/p\mathbb{Z})^\times$ has a prim. root, there are $\varphi(p-1)$ prim roots"

New thm: there are $\varphi(p-1)$ prim roots.

Partial pf of new thm:

Notation: p prime

$d \mid p-1$ and $d > 0$.

Define

$$S_d = \{ n \in \mathbb{Z}/p\mathbb{Z} \quad \text{ord}_p(n) = d \}$$

$$F(d) = \#\, S_d$$

The $\{S_d\}$ are pairwise disjoint and every elt. of $(\mathbb{Z}/p\mathbb{Z})^\times$ lies in some S_d.

So $(\mathbb{Z}/p\mathbb{Z})^\times = \bigcup_{d \mid p-1} S_d$ (disjoint)

$$p-1 = \#\,(\mathbb{Z}/p\mathbb{Z})^\times = \sum_{d \mid p-1} \#\, S_d = \sum_{d \mid p-1} F(d)$$

Recall: $$p-1 = \sum_{d \mid p-1} \varphi(d)$$

So $$\sum_{d \mid p-1} \varphi(d) = \sum_{d \mid p-1} F(d)$$

If we can show $F(d) \le \varphi(d)$,

then we conclude $F(d) = \varphi(d)$

Aside: $p = 7 \to p-1 = 6$

$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6)$

$= F(1) + F(2) + F(3) + F(6)$

$F(1) \leq \varphi(1)$

$F(2) \leq \varphi(2)$

$\vdots$

If $F(3) < \varphi(3)$

then $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6)$

$> F(1) + F(2) + F(3) + F(6)$

↯

New goal: $F(d) \leq \varphi(d)$

How?

What does it mean to have order d?

A: $\operatorname{ord}_p(a) = d$ iff

$a^d \equiv 1 \bmod p$ and

$a^n \not\equiv 1 \bmod p$ when $1 \le n < d$.

$a^d - 1 \equiv 0 \bmod p$

a is a root of

$x^d - 1 \bmod p$.

If we want to count elts. of order d, we want to count some roots of $x^d - 1 \mod p$.

Q: How many roots does $x^d - 1$ have mod p?

Q: How many roots does $x^{p-1} - 1$ have mod p?

A: Note $p - 1 = \varphi(p)$

Pick $a \in (\mathbb{Z}/p\mathbb{Z})^\times$

$a^{p-1} - 1 \equiv 1 - 1 \equiv 0 \mod p$

So a is a root.

So we have $p-1$ rts.

Q: How many complex roots does $x^d - 1$ have?

A: $\leq d$ roots

in general: roots $\longleftrightarrow$ linear factors

e.g. if 1 is a root of $f(x)$,
then $f(x) = (x-1)\,g(x)$

$x^d - 1$ has $\leq d$ linear factors
$\leq d$ roots.

Thm (Lagrange). Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ have $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{Z}$, $n \geq 1$. Then f has $\leq n$ distinct roots mod p when p is prime

Nonex: $x^2 - 4 \equiv 0 \mod 15$

$x^2 - 4 \equiv 0 \mod 3$ $\quad$ $x^2 - 4 \equiv 0 \mod 5$

$\approx$ 2 solns. $\quad$ $\approx$ 2 solns.

4 solns.

Extend Lagrange's Thm:

Thm: Let p be prime and $d \mid p-1$

Then $x^d - 1$ has exactly d roots mod p.

Pf: $x^d - 1$ has $\leq d$ rts. mod p.

Write $p - 1 = de$ for some $e \in \mathbb{Z}$

$$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1)$$

1

exactly

$p-1$ rts

mod p

1

at most

$d(e-1)$ rts.

mod p.

So x^d-1 has at least $p-1-d(e-1)$ rts. mod p

But $p-1-d(e-1) = p-1-de+d$

$= p-1-(p-1)+d$

$= d$

So x^d-1 has at least d rts. mod p

So x^d-1 has exactly d rts. mod p

Return to counting elts. of order d.

$F(d)$ = # of elts. of order d

If $F(d) \leq \varphi(d)$ for all $d \mid p-1$, then

$$F(d) = \varphi(d)$$

Lemma: $F(d) \leq \varphi(d)$

Pf: If $F(d) = 0$, we're done ✓

Else, $F(d) \geq 1$, so $\exists\, a \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $\operatorname{ord}_p(a) = d$.

① $a, a^2, a^3, \ldots, a^d$ are distinct mod p

- if not, then $a^i \equiv a^j \bmod p$ for some $1 \leq i < j \leq d$
- b/c (a, p), $1 \equiv a^{j-i} \bmod p$
- $d = \operatorname{ord}_p(a) \mid j - i < d$ ↯

② Each a^i is a root of $x^d - 1 \bmod p$

$$(a^i)^d - 1 \equiv (a^d)^i - 1 \equiv 1^i - 1 \equiv 0 \bmod p$$

So $a, a^2, \ldots, a^d$ are d distinct rts. of $x^d - 1$

So every rt. of $x^d - 1$ is a power of a.

Every elt. of order d is a rt. of $x^d - 1$

So every elt. of order d is a power of a.

Recall.

$$\text{ord}_p(a^j) = \frac{d}{(j, d)}$$

So $\text{ord}_p(a^j) = d$ iff $(j, d) = 1$

There are $\varphi(d)$ values of $1 \leq j \leq d$ s.t. $(j, d) = 1$

I.e. $\varphi(d)$ powers of a which have order d.

I.e. $\varphi(d)$ elts. of order d.

So $F(d) \leq \varphi(d)$

Recall: $\varphi(p-1)$ prim. rts. mod p.

---

3) $p \equiv 1 \mod 4 \rightarrow 4 \mid p-1 \rightarrow \exists\, x : \operatorname{ord}_p(x) = 4$

$\rightarrow x^2 \not\equiv 1 \mod p$

note that x^2 is a rt. of $y^2 - 1 \mod p$

b/c $(x^2)^2 - 1 \equiv x^4 - 1 \equiv 0 \mod p$

and $y^2 - 1$ has rts. $\equiv 1 \mod p$.

$x^2 \not\equiv 1 \mod p \rightarrow x^2 \equiv -1 \mod p$

$x^2 - 5 \equiv 0 \mod 13 \leftrightarrow x^2 \equiv 5 \mod 13$

$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$

$\rightarrow$ no sol'ns.