Math 312, lecture 18, 13/6/2018

Last time: (1) A primitive root mod m is a residue r s.t. $\mathrm{ord}_m(r) = \phi(m)$ (largest possible) $(r,m)=1$.

Then $U(m) = \{a \bmod m \mid (a,m)=1\} = \{r^j\}_{j=0}^{\phi(m)-1}$.

(2) Primitive roots exist iff $m \in \{2, 4, p^k, 2p^k\}$ p odd prime $k \geq 1$
(Pf today)

(3) Discrete log: if $r^j = b$, given r, b find j.

(has the usual properties of logarithms, since $r^i r^j = r^{i+j}$ $(r^i)^j = r^{ij}$

so also $r^i r^j \equiv r^{i+j}$ (m)

$(r^i)^j \equiv r^{ij}$ (m) where $i+j, ij$ are mod $\phi(m)$)

(4) Use this to solve equations: if $r^j = b$ ~~then~~ $(b,m)=1$ then equation $x^n \equiv b\,(m)$ is equivalent to $ny \equiv j\ (\phi(m))$ by change of variable $x = r^y$.

Today: (1) proof of existence of primitive roots mod p

(2) Diffie-Hellman key exchange

(3) nth power residues mod p.

Thm: Let p be prime. Then there exist primitive root mod p (actually $\phi(p-1)$ of them)

Pf: Idea: count how many classes mod p have each order dividing $p-1$.

Ingredients: (1) every non-zero residue mod p is invertible

$\Rightarrow$ (2) a polynomial of degree d has at most d roots mod p

(sketch: if $f(x)$ has root a then $x-a \mid f$: $f(x) \equiv (x-a)g(x)$ (p) then every root of f other than a must be a root of g)

(3) $n = \sum_{d \mid n} \phi(d)$

Pf of thm: Let $n = p-1$ so the order of each a mod p divides n. Goal: for each $d \mid n$, exactly $\phi(d)$ classes of order d

For this, let a have order d mod p, where $d \mid n = p-1$

(Fermat's little thm: $\mathrm{ord}_p(a) \mid p-1$ for all $a \not\equiv 0$ (p))

If a has order d, a is a root of the polynomial $x^d - 1$.

Note: $b^d \equiv 1$ (p) iff $\mathrm{ord}_p(b) \mid d$ so $\{\text{roots of } x^d - 1\} = \{\text{classes of order} \mid d\}$

$\Rightarrow$ at most d classes of order dividing d

On the other hand, the d distinct classes $\{a^j\}_{j=0}^{d-1}$ have order dividing d: $(a^j)^d = a^{jd} = a^{dj} = (a^d)^j \equiv 1^j \equiv 1$ (p)

$\Rightarrow$ If a has order d mod p, $\{a^j\}_{j=0}^{d-1}$ are exactly the classes having order dividing d

<u>Next step</u>: count classes of order d exactly.

<u>Example</u>: say $2|d$. Then a^2 has order $d/2$: $(a^2)^{d/2} = a^d \equiv 1\ (p)$

but if $f < d/2$, $(a^2)^f = a^{2f} \not\equiv 1\ (p)$ since $2f < d$

what about a^4, or a^6?

if $4|d$, $\mathrm{ord}_p(a^4) = d/4$. what if $2|d$, but $4 \nmid d$?

then a^2 has order $d/2$, <u>odd</u>, 2 is invertible mod $d/2$

Let $\bar{2}$ be an inverse. Then $a^4 \equiv (a^2)^2$ but $a^2 \equiv (a^4)^{\bar{2}} = (a^2)^{2\cdot\bar{2}} \equiv a^2$

$2\cdot\bar{2} \equiv 1\ (\mathrm{ord}(a^2))$

~~thus~~ if a, b are powers of each other, have same order: if b power of a then $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.

if reverse also true then $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

$\Rightarrow$ if $2|d$, $4\nmid d$, $\mathrm{ord}_p(a^4) = d/2$

if $2|d$, $6|d$, $\mathrm{ord}_p(a^6) = d/6$

if $2|d$, $3 \nmid d$, $\mathrm{ord}_p(a^6) = \mathrm{ord}(a^2) = d/2$ since 3 invertible mod $d/2$

<u>See</u>: If j is invertible mod $\mathrm{ord}_m(a)$ then $\mathrm{ord}_m(a^j) = \mathrm{ord}_m(a)$

(Pf: if $\bar{j}$ is an inverse, $a = (a^j)^{\bar{j}}$)

$\Rightarrow$ <u>at least</u> $\phi(d)$ powers of a of order d

In general, $\mathrm{ord}_m(a^j) = \dfrac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a), j)}$

Pf of claim: $d = \mathrm{ord}_m(a)$, $e = \gcd(j, d)$

a^e has order $\frac{d}{e}$ mod m

and $\frac{j}{e}$ is invertible mod $\frac{d}{e}$ $\left(\gcd\left(\frac{j}{e}, \frac{d}{e}\right) = 1\right)$

so $\mathrm{ord}_m\left((a^e)^{j/e}\right) = \mathrm{ord}_m(a^e) = \frac{d}{e}$

---

so $\mathrm{ord}_m(a^j) = d = \mathrm{ord}_m(a)$ iff j ~~invertible~~ prime to d

$\Rightarrow$ exactly $\phi(d)$ classes of order d

Recap: p prime, $n = p-1$, $d \mid p-1$, a mod p has order d

$\Rightarrow$ exactly $\phi(d)$ classes of order d

If no element has order d then have 0 such classes

Endgame: let $f(d) = \#$ classes of order d

Fermat: every class has order $\mid n = p-1$

so
$$\sum_{d \mid n} f(d) = n = p-1$$

and
$$\sum_{d \mid n} \phi(d) = n$$

each summand on top is either equal to corresponding summand on bottom or zero. But sums are equal, so no zeroes: $f(d) = \phi(d)$ for all d, in particular

$f(p-1) = \phi(p-1) \geq 1 > 0.$