Math 312, lecture 19, 14/6/2018

Last time: (1) Pf of existence of primitive roots mod p

(2) classification of nth power residues mod p.

Recall: r is a primitive root (mod m) if $\operatorname{ord}_m(r) = \phi(m)$

$\Leftrightarrow \{\text{invertible residues mod } m\} = \{\text{powers of } r\} = \{r^j\}_{j=0}^{\phi(m)-1}$

Then the equation $x^n \equiv a \ (m)$ is equivalent to the equation

$$ny \equiv \ell \ (\phi(m)), \quad \text{where } a \equiv r^\ell \ (m)$$

(change of vars was $x = r^y$)

Now a is an nth power (mod m) iff the equation has a solution

iff $ny \equiv \ell \ (\phi(m))$ has a solution,

iff $(n, \phi(m)) \mid \ell \quad (*)$

Example question: Is 8 a square mod 43?

Is 13 a square mod 31?

To use criterion $(*)$, need to (1) find a primitive root

(2) compute a discrete log

Different criterion:

Suppose $(n, \phi(m)) \mid \ell$. Then $\ell \cdot \dfrac{\phi(m)}{(n,\phi(m))} = \dfrac{\ell}{(n,\phi(m))} \cdot \phi(m) \equiv 0 \ (\phi(m))$

Conversely, if $\ell \cdot \dfrac{\phi(m)}{(n,\phi(m))} \equiv 0 \ (\phi(m))$ then $\dfrac{\ell}{(n,\phi(m))} = \dfrac{\ell \cdot \frac{\phi(m)}{(n,\phi(m))}}{\phi(m)} \in \mathbb{Z}$

so $(n, \phi(m)) \mid \ell$

$\Rightarrow x^n \equiv a \ (m)$ has a solution iff $\ell \cdot \dfrac{\phi(m)}{(n,\phi(m))} \equiv 0 \ (\phi(m)) \quad (**)$

Third version

note: $\ell \cdot \frac{\phi(m)}{(n,\phi(m))} \equiv 0 \ (\phi(m)) \iff r^{\ell \cdot \frac{\phi(m)}{(n,\phi(m))}} \equiv r^0 \equiv 1 \ (m)$

$\iff (r^\ell)^{\frac{\phi(m)}{(n,\phi(m))}} \equiv 1 \ (m) \iff a^{\frac{\phi(m)}{(n,\phi(m))}} \equiv 1 \ (m)$

$r^\ell \equiv$

Prop: Let $(a,m)=1$, and suppose there exist primitive roots mod m (e.g. m is prime). Then a is an nth power (mod m) iff

$$a^{\frac{\phi(m)}{(n,\phi(m))}} \equiv 1 \ (m)$$

Example: $m=p$ prime, $n=2$

⇒ **Thm:** (Euler) Let $p \nmid a$. Then a is a square mod p iff

p odd prime →

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

Def: Call a a quadratic residue mod p if a is a square

a quadratic nonresidue if not.

Examples:

$p=3$. $1^2 \equiv 1\ (3)$, $2^2 \equiv 1\ (3)$ ← equation $x^2 \equiv 1\ (3)$ has 2 solutions

quadratic residues mod 3: 1

non-residues mod 3: $2 \equiv -1$

$p=5$, $1^2 \equiv 1\ (5)$, $2^2 \equiv 4\ (5)$, $3^2 \equiv 4\ (5)$, $4^2 \equiv 1\ (5)$

quadratic residues: 1, 4 (i.e. classes of 1, 4)

non-residues: 2, 3

($6 \equiv 1^2\ (5)$ so 6 is a quadratic residue mod 5)

$p=7$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$, $6^2 \equiv 1\ (7)$

quad residues: 1, 2, 4

non-residues: 3, 5, 6

$p=11$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 5$, $5^2 \equiv 3$, $6^2 \equiv 3$, ...

$(-x)^2 \equiv x^2\ (p)$

quad residues: 1, 3, 4, 5, 9

non-residues: 2, 6, 7, 8, 10

Patterns: $(-x)^2 \equiv x^2$, every quad residue is obtained twice ($-x \not\equiv x$ since $2 \nmid p$), so get half the residues as quad residues

Conclusions: Mod p have $\frac{p-1}{2}$ quadratic residues, $\frac{p-1}{2}$ quadratic non-residues, 1 class of 0 mod p

($\frac{p-1}{2} + \frac{p-1}{2} + 1 = p$)

Return to single residue classes

Notation: $\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a quad res. mod } p \\ -1 & \text{if } a \text{ " " " non-residue} \\ 0 & \text{if } p \mid a \end{cases}$

called "Legendre symbol", p an odd prime

Examples: $\left(\frac{1}{3}\right)=1$, $\left(\frac{2}{3}\right)=-1$, $\left(\frac{6}{3}\right)=0$

$\left(\frac{16}{11}\right)=\left(\frac{5}{11}\right)=1$, $\left(\frac{8}{11}\right)=-1$, $\left(\frac{0}{11}\right)=0$

Thm (Euler): $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (p)$ for all a mod p

Pf: If $p \mid a$, $p \mid a^{\frac{p-1}{2}}$ so $a^{\frac{p-1}{2}} \equiv 0 \equiv \left(\frac{a}{p}\right)$

If $p \nmid a$, a is invertible mod p, then

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \quad \text{(by Fermat's little thm)}$$

So $a^{\frac{p-1}{2}}$ squares to 1 mod p so $a^{\frac{p-1}{2}} \equiv \pm 1 \ (p)$

We already know $a^{\frac{p-1}{2}} \equiv 1 \ (p)$ iff a is a quad residue,

so $a^{\frac{p-1}{2}} \equiv -1 \ (p)$ iff a is a non-residue ∎

Examples: $\left(\frac{5}{11}\right) \equiv 5^{\frac{11-1}{2}} \ (11) \equiv 5^5 \equiv (5^2)^2 \cdot 5 \equiv 3^2 \cdot 5 \equiv 9 \cdot 5 \equiv 1 \ (11)$ ($5^2 \equiv 3$)

$\left(\frac{8}{11}\right) \equiv 8^{\frac{11-1}{2}} \equiv 8^5 \equiv (2^3)^5 \equiv 2^5 \cdot 2^5 \cdot 2^5 \equiv (2^5)^3 \equiv (-1)^3 \equiv -1 \ (11)$ ($2^5 \equiv 32$)

Recap

Want to know if a is a square mod p

(1) can set aside case $p \mid a$

(2) can tell by computing all squares mod p

(3) can tell by $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (p)$

(can evaluate RHS by exponentiation via repeated squaring)

for more:

Lemma: let $a, a', b \in \mathbb{Z}$, p an odd prime. Then:

(1) $a \equiv a' \ (p)$ then $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ ← "replace a with its reduced residue".

(2) If $p \nmid b$ then $\left(\frac{b^2}{p}\right) = 1$ ← can ignore squares in $\mathbb{Z}$

(3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ ← reduce problem for ab to problems for a & b separately

Example: If $p \nmid 2, 3$ then $\left(\frac{12}{p}\right) = \left(\frac{3}{p}\right)\cdot\left(\frac{4}{p}\right) = \left(\frac{3}{p}\right)\cdot 1 = \left(\frac{3}{p}\right)$

Pf of lemma: (1), (2) true by defn of $\left(\frac{a}{p}\right)$

(3): $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$

(first $\equiv$: Euler; second $\equiv$: defn)

Bottom line: To compute $\left(\frac{a}{p}\right)$ can: (1) reduce a mod p

(2) factor a, check for each prime factor.

Example: $\left(\frac{51}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{17}{p}\right)$

$\left(\frac{-51}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{17}{p}\right)$

Conclusions: If we can factor, enough to be able to compute.

(1) $\left(\frac{-1}{p}\right)$, (2) $\left(\frac{2}{p}\right)$, (3) $\left(\frac{q}{p}\right)$, q odd prime

$\left(\frac{\cdot}{p}\right)$ = "Legendre symbol", "quadratic residue symbol"
"quadratic character"

Prop: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \ (4) \\ -1 & p \equiv 3 \ (4) \end{cases} = \chi_4(p) \equiv (-1)^{\frac{p-1}{2}}$

Pf: By Euler, $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \ (p)$

Both of these numbers are $+1$ or -1, so their difference is 0 or ± 2. But $p \nmid \pm 2$ so

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \frac{p-1}{2} \text{ even} \\ -1 & \frac{p-1}{2} \text{ odd} \end{cases}$$

$$= \begin{cases} 1 & \frac{p-1}{2} \equiv 0 \ (2) \\ -1 & \frac{p-1}{2} \equiv 1 \ (2) \end{cases}$$

$$= \begin{cases} 1 & p-1 \equiv 0 \ (4) \\ -1 & p-1 \equiv 2 \ (4) \end{cases} \rightsquigarrow \begin{cases} 1 & p \equiv 1 \ (4) \\ -1 & p \equiv 3 \ (4) \end{cases}$$

Pf 2: Suppose $x^2 \equiv -1 \ (p)$

Then $x^4 = (x^2)^2 \equiv (-1)^2 \equiv 1 \ (p)$ so $\text{ord}_p(x) \mid 4$. But $\text{ord}_p(x) \nmid 2$ ($-1 \not\equiv 1 \ (p)$ since p is odd), so $\text{ord}_p(x) = 4$.

(if $\left(\frac{-1}{p}\right) = 1$ then $\exists x \bmod p$ of order 4)

Conversely, if $\text{ord}_p(x) = 4$ then $(x^2)^2 \equiv 1 \ (p)$ so $x^2 \equiv \pm 1 \ (p)$ but $x^2 \not\equiv 1 \ (p)$ $(\text{ord}_p(x) \neq 2)$ so $x^2 \equiv -1 \ (p)$

(if $\exists x \bmod p$ of order 4, then $\left(\frac{-1}{p}\right) = 1$)

But theory of primitive roots showed: $\exists x \bmod p$ of order d iff $d \mid p-1$.

i.e. $\exists x$ of order 4 iff $4 \mid p-1$ iff $p \equiv 1 \ (4)$

Fact: $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \ (8) \\ -1 & p \equiv \pm 3 \ (8) \end{cases} \equiv (-1)^{\frac{p^2-1}{8}}$

Thm: (Quadratic reciprocity) (Conj. of Euler, proved by Gauss)

Let $p \neq q$ be odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \ (4) \\ 1 & \text{otherwise} \end{cases}$$

⇒ Strategy for computing $\left(\frac{a}{p}\right)$

(1) reduce a mod p (to range $[-p/2, p/2]$ is better

(2) Factor a into primes. Need to evaluate $\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right)$

(3) where q ranges over odd primes dividing p

(3) Use quadratic reciprocity to compute $\left(\frac{q}{p}\right)$ by computing $\left(\frac{p}{q}\right)$

Example: $\left(\frac{17}{43}\right)\left(\frac{51}{43}\right) = \left(\frac{3}{43}\right)\cdot\left(\frac{17}{43}\right)$

$\left(\frac{3}{43}\right) = -\left(\frac{43}{3}\right) = -\left(\frac{1}{3}\right) = -1$

QR, $3 \equiv 43 \equiv 3 \ (4)$; $43 \equiv 1 \ (3)$; $1^2 = 1$ in $\mathbb{Z}$

$17 \equiv 1 \ (8)$

$17 \equiv 1 \ (4)$

$\left(\frac{17}{43}\right) = \left(\frac{43}{17}\right) = \left(\frac{9}{17}\right) = \left(\frac{-8}{17}\right) = \left(\frac{-1}{17}\right)\cdot\left(\frac{2}{17}\right)\cdot\left(\frac{4}{17}\right) = 1\cdot 1\cdot 1 = 1$

QR, $17 \equiv 1 \ (4)$; 1 ; $9 = 3^2$; $4 = 2^2$

So $\left(\frac{51}{43}\right) = \left(\frac{3\cdot 17}{43}\right) = \left(\frac{3}{43}\right)\cdot\left(\frac{17}{43}\right) = -1\cdot 1 = \boxed{-1}$