Math 312, lecture 20, 15/6/2018

Last time: a mod p is: (p odd prime)

- a quadratic residue if $x^2 \equiv a\ (p)$ for some $x \not\equiv 0\ (p)$
- a quadratic non-residue if no such x exists (but $a \not\equiv 0\ (p)$)
- 0 otherwise

write $\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a square} \\ 0 & a \equiv 0\ (p) \\ -1 & a \text{ is a non-square} \end{cases}$

Facts: (1) Euler's criterion $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (p)$

(2) if $a \equiv a'\ (p)$ then $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ — complete multiplicativity

(3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ $\Rightarrow$ if $b \not\equiv 0\ (p)$, $\left(\frac{b^2}{p}\right) = 1$

(4) If p, q are odd primes — Law of Quadratic Reciprocity

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ie.

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

(5) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1\ (4) \\ -1 & p \equiv -1\ (4) \end{cases}$

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

Corollary: the number of roots of $ax^2+bx+c \equiv 0\ (p)$ (mod p) is $1 + \left(\frac{b^2-4ac}{p}\right)$

Example: $\left(\frac{127}{347}\right) = ?$

Verifying that 347 is prime: $347 \equiv 11 \equiv 2$ (3) (sum is divisible) $347 \equiv 1$ (2)

$347 \equiv 2$ (5)

$347 \equiv 340 \equiv 2 \cdot 5 \cdot 2 \cdot 17 \not\equiv 0$ (7)

~~$347 \equiv 3+4-7 \equiv -6 \not\equiv 0$ (11)~~

$347 \equiv 3-4+7 \equiv 6$ (11) ↑ PS2

$347 \equiv 347+13 \equiv 360 \equiv 10 \cdot 4 \cdot 9 \not\equiv 0$ (13)

$347 \equiv 7+340 \equiv 7$ (17)

$19^2 = 361 > 347$ so 347 is not divisible by any prime $\leq \sqrt{347}$ so 347 is prime

---

Factor 127: $127 \equiv 1$ (1)

$127 \equiv 1+2+7 \equiv 10 \equiv 1$ (3)

$127 \equiv 2$ (5)

$127 \equiv 120 \equiv 10 \cdot 12 \equiv 3 \cdot 5 \not\equiv 0$ (7)

$127 \equiv 1-2+7 \equiv 6$ (11)

$13^2 = 169 > 127$ so 127 is not divisible by any prime $\leq \sqrt{127}$ so 127 is prime.

By QR, $\left(\frac{127}{347}\right) = -\left(\frac{347}{127}\right)$ ($127 \equiv 7 \equiv 3$ (4), $347 \equiv 7 \equiv 3$ (4))

Continuation 1: $347 - 2 \cdot 127 = 93$ so $\left(\frac{347}{127}\right) = \left(\frac{93}{127}\right)$

Next, $93 = 3 \cdot 31$ so by multiplicativity,

$$\left(\frac{93}{127}\right) = \left(\frac{3}{127}\right)\left(\frac{31}{127}\right)$$

Next, $\left(\frac{3}{127}\right) = -\left(\frac{127}{3}\right) = -\left(\frac{1}{3}\right) = -\left(\frac{1^2}{3}\right) = -1$

QR, $3 \equiv 3 (4)$, $127 \equiv 3 (4)$; $127 = 1 + 120 + 6 \equiv 1 (3)$

$$\left(\frac{31}{127}\right) = -\left(\frac{127}{31}\right) = -\left(\frac{3}{31}\right) = \left(\frac{31}{3}\right) \equiv \left(\frac{1}{3}\right) = 1$$

QR, $31 \equiv 3 (4)$, $127 \equiv 3 (4)$; $127 - 3 \cdot 31 = 127 - 124 = 3$; QR, $31, 3 \equiv 3 (4)$

So $\left(\frac{93}{127}\right) = (-1) \cdot 1 = -1$ so $\left(\frac{347}{127}\right) = -1$

So $\boxed{\left(\frac{127}{347}\right) = -(-1) = 1}$

Continuation 2: $\left(\frac{347}{127}\right) = \left(\frac{347 - 127}{127}\right) = \left(\frac{220}{127}\right) = \left(\frac{10 \cdot 2 \cdot 11}{127}\right) =$

$$= \left(\frac{2^2 \cdot 5 \cdot 11}{124}\right) = \left(\frac{2^2}{127}\right) \cdot \left(\frac{5}{127}\right) \cdot \left(\frac{11}{127}\right)$$

and: $\left(\frac{5}{127}\right) = \left(\frac{127}{5}\right) = \left(\frac{2}{5}\right) = -1$, $\left(\frac{11}{127}\right) = -\left(\frac{127}{11}\right) = -\left(\frac{6}{11}\right)$

QR, $5 \equiv 1 (4)$; squares mod 5 are ± 1; QR, $11 \equiv 127 \equiv 3 (4)$

$$= -\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = -(-1)(1)\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

$-1 \equiv 3 (8)$; QR, $11 \equiv 3 \not\equiv 3 (4)$

So $\left(\frac{347}{127}\right) = (-1)(1) = -1$.

Method without factoring:

Continuation 3: $347 \equiv 93 \equiv 93-127 = -34 \ (127)$

So $\left(\frac{347}{127}\right) = \left(\frac{-34}{127}\right) = \left(\frac{-1}{127}\right)\left(\frac{2}{127}\right)\cdot\left(\frac{17}{127}\right)$

$-1 : 127 \equiv 3 \ (4)$ $\quad$ $1 : 127 \equiv -1 \ (8)$

Note: If q is prime, $\left(\frac{q}{p}\right)$ dependent on $\begin{cases} \text{class of } p \bmod q & q \equiv 1 \ (4) \\ \text{class of } p \bmod 4q & q \equiv -1 \ (4) \end{cases}$

Without factoring: the Jacobi Symbol

Def: Let P be an odd positive integer, $P = \prod_{i=1}^{r} p_i$

For any integer Q, the Jacobi symbol $\left(\frac{Q}{P}\right)$ is defined to be:

$$\left(\frac{Q}{P}\right) = \prod_i \left(\frac{Q}{p_i}\right)$$

In other words, $\left(\frac{Q}{\cdot}\right)$ is the completely multiplicative function s.t.

$\left(\frac{Q}{p}\right)$ = Legendre symbol if p prime

(If p is prime, $\left(\frac{Q}{p}\right)$ can mean either the Legendre or Jacobi symbol, but the value is the same)

Warning: When P not prime, $\left(\frac{Q}{P}\right)$ has **nothing** to do with eqn $X^2 \equiv Q \ (P)$

E.g. if p is a prime, $\left(\frac{Q}{p^2}\right) \overset{\text{def}}{=} \left(\frac{Q}{p}\right)^2 = \begin{cases} 0 & p \mid Q \\ 1 & p \nmid Q \end{cases}$

Warning: don't compute Jacobi symbols by def'n.

Instead: **Prop:** Let P be odd, positive. Then:

(1) $\left(\frac{-1}{P}\right) = \begin{cases} 1 & P \equiv 1 \ (4) \\ -1 & P \equiv 3 (4) \end{cases}$, $\left(\frac{2}{P}\right) = \begin{cases} 1 & P \equiv \pm 1 \ (8) \\ -1 & P \equiv \pm 3 (8) \end{cases}$

(2) $\left(\frac{Q_1 Q_2}{P}\right) = \left(\frac{Q_1}{P}\right)\left(\frac{Q_2}{P}\right)$

(3) $\left(\frac{Q}{P}\right) = 0$ iff $(P, Q) > 1$, $\left(\frac{Q}{P}\right) = \pm 1$ otherwise

(4) If $Q \equiv Q' \ (P)$ then $\left(\frac{Q}{P}\right) = \left(\frac{Q'}{P}\right)$

(5) QR If Q is odd, positive then $\left(\frac{P}{Q}\right) \cdot \left(\frac{Q}{P}\right) = \begin{cases} -1 & P \equiv Q \equiv 3 (4) \\ 1 & \text{else} \end{cases}$

⇒ Algorithm for computing Jacobi symbols (includes Legendre symbols)

Given (P, Q):

(1) reduce Q mod P

(2) Write Q as $(\pm 1) \cdot 2^s \cdot Q'$, Q' odd positive

(3) $\left(\frac{Q}{P}\right) = \left(\frac{\pm 1}{P}\right) \cdot \left(\frac{2}{P}\right)^s \cdot \left(\frac{Q'}{P}\right)$

(4) compute $\left(\frac{Q'}{P}\right) = \pm \left(\frac{P}{Q'}\right)$ by QR, return to step 1 (known)

Example:

$$\left(\frac{127}{347}\right) = -\left(\frac{347}{127}\right) = -\left(\frac{93}{127}\right) = -\left(\frac{127}{93}\right)$$

QR, $3 \equiv 127 \equiv 347 \ (4)$

$93 = 347 - 2 \cdot 127$

QR, $93 \equiv 1 \ (4)$

$127 - 93 = 34$

$$= -\left(\frac{34}{93}\right) = -\left(\frac{2}{93}\right)\left(\frac{17}{93}\right) = -(-1)\left(\frac{17}{93}\right) =$$

QR, $17 \equiv 1 \ (4)$

$93 = 96 - 3 \equiv (-3)(8)$

$$= \left(\frac{93}{17}\right) = \left(\frac{8}{17}\right) = \left(\frac{2}{17}\right)^3 = \left(\frac{2}{17}\right) = 1$$

$93 - 5 \cdot 17 = 8$

$\left(\frac{2}{17}\right)^3 \in \{\pm 1\}$

$17 \equiv 1 \ (8)$

Proof of Prop on Jacobi Symbols

$P = \prod_{i=1}^{r} p_i$, p_i odd primes

(1) $\left(\frac{-1}{p_i}\right) \equiv p_i \ (4)$ so $\left(\frac{-1}{P}\right) = \prod_i \left(\frac{-1}{p_i}\right) \equiv \prod_i p_i \equiv P \ (4)$

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

note: $3 \cdot 3 \equiv 1 \ (8)$

So $\left(\frac{2}{P}\right) = \prod_i \left(\frac{2}{p_i}\right) = \prod_{p_i \equiv \pm 3 (8)} (-1) = \begin{cases} 1 & \#\{i \mid p_i \equiv \pm 3 \ (8)\} \text{ is even} \\ -1 & \#\{i \mid p_i \equiv \pm 3 \ (8)\} \text{ is odd} \end{cases}$

mod 8, $P = \prod_i p_i \equiv (\pm 1) \cdot 3^{\#\{i \mid p_i \equiv \pm 3 (8)\}} = \begin{cases} \pm 1 & \#\{i\}\text{ even} \\ \pm 3 & \#\{i\}\text{ odd} \end{cases}$

i.e. $\left(\frac{2}{P}\right) = \begin{cases} 1 & P \equiv \pm 1 \ (8) \\ -1 & P \equiv \pm 3 \ (8) \end{cases}$

(2) $\left(\frac{Q_1Q_2}{P}\right) \overset{\text{def}}{=} \prod_i \left(\frac{Q_1Q_2}{p_i}\right) = \prod_{i=1}^{r} \left(\frac{Q_1}{p_i}\right)\cdot\left(\frac{Q_2}{p_i}\right) = \left(\prod_i \frac{Q_1}{p_i}\right)\left(\prod_i \frac{Q_2}{p_i}\right)$

↑ Legendre symbol is mult. $\overset{\text{def}}{=} \left(\frac{Q_1}{P}\right)\cdot\left(\frac{Q_2}{P}\right)$

(3) If $(P,Q)>1$ then some $p_i \mid Q$ and then $\left(\frac{Q}{p_i}\right)=0$, so $\left(\frac{Q}{P}\right)=0$

If $(P,Q)=1$ then no $p_i \mid Q$ so $\left(\frac{Q}{p_i}\right)=\pm 1 \neq 0$ for all i, so $\left(\frac{Q}{P}\right)\neq 0$

(4) If $Q \equiv Q' \ (P)$ then $p_i \mid P$ $\quad Q \equiv Q' \ (p_i)$ for each i.

so $\left(\frac{Q}{p_i}\right) = \left(\frac{Q'}{p_i}\right)$, multiplying over i gives $\left(\frac{Q}{P}\right) = \left(\frac{Q'}{P}\right)$

(5): Say $Q = \prod_{j=1}^{s} q_j$, q_j odd primes.

Then $\left(\frac{P}{Q}\right) \overset{\text{def}}{=} \prod_i \left(\frac{P}{p_i}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right)$

↑ mult of $\left(\frac{\bullet}{p_i}\right)$

then $\left(\frac{P}{Q}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)$

so $\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\#\{(i,j) \mid p_i \equiv q_j \equiv 3 (4)\}}$

$= (-1)^{(\#\{i \mid p_i \equiv 3(4)\})(\#\{j \mid q_j \equiv 3(4)\})}$

But $P \equiv (-1)^{\#\{i \mid p_i \equiv 3(4)\}}$ (4)

Same for Q so $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \begin{cases} -1 & P \equiv Q \equiv 3(4) \\ 1 & \text{else} \end{cases}$