Math 312, lecture 23, 21/6/2018

Review

Problem: Evaluate $\left(\frac{255}{419}\right)$ (fact: 419 is prime)

Method 1: Factorization of legendre symbols

$255 = 5 \cdot 51 = 3 \cdot 5 \cdot 17$

so $\left(\frac{255}{419}\right) = \left(\frac{3}{419}\right)\left(\frac{5}{419}\right)\left(\frac{17}{419}\right)$ evaluate each in turn:

$\left(\frac{3}{419}\right) = -\left(\frac{419}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$

QR: 3, 419 prime; $3 \equiv 419 \equiv 3 \pmod 4$

$419 \equiv 4+1+9 \equiv 2 \pmod 3$

2 not a square mod 3

$\left(\frac{5}{419}\right) = \left(\frac{419}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$

QR, 5, 419 prime; $5 \equiv 1 \pmod 4$

$419 \equiv 9 \equiv 4 \pmod 5$

$17 \overline{)419}$: 24, 34, 79, 68, 11

$\left(\frac{17}{419}\right) \overset{QR}{=} \left(\frac{419}{17}\right) = \left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\cdot\left(\frac{3}{11}\right)$

$6 = 2 \cdot 3$

QR, 11, 17 prime

$11 \equiv \pm 3 \pmod 8$

$17 \equiv 1 \pmod 4$

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

QR, 3, 11 prime

$11 \equiv 3 \pmod 4$

Conclusion:

$$\left(\frac{255}{419}\right) = \left(\frac{3}{419}\right)\left(\frac{5}{419}\right)\left(\frac{17}{419}\right) = 1 \cdot 1 \cdot (-1) = -1.$$

Method 2: QR for Jacobi symbols

$$\left(\frac{255}{419}\right) \overset{\text{QR}}{=} -\left(\frac{419}{255}\right) = -\left(\frac{-91}{255}\right) = -\left(\frac{-1}{255}\right)\left(\frac{91}{255}\right) =$$

QR, $255 = 256 - 1 \equiv 3 (4)$, $419 = 420 - 1 \equiv 3 (4)$

$419 - 2 \cdot 255 = 419 - 510 = -91$

$255 \equiv 3 (4)$ so $\left(\frac{-1}{255}\right) = -1$

$$= -(-1)\cdot\left(\frac{91}{255}\right) \overset{\text{QR}}{=} -\left(\frac{255}{91}\right) = -\left(\frac{-18}{91}\right) = -\left(\frac{-1}{91}\right)\left(\frac{2}{91}\right)\left(\frac{3^2}{91}\right)$$

QR, $255 \equiv 3 (4)$, $91 = 92 - 1 \equiv 3 (4)$

$255 - 3 \cdot 91 = 255 - 273 = -18$

$-18 = (-1) \cdot 2 \cdot 3^2$

$$= -(-1)\cdot(-1)\cdot 1 = -1$$

$91 \equiv 3 (4)$ so $\left(\frac{-1}{91}\right) = -1$

$91 \equiv 3 (8)$ so $\left(\frac{2}{91}\right) = -1$

$\left(\frac{3^2}{91}\right) = 1$, 3^2 is a square

OR: $-\left(\frac{-18}{91}\right) = -\left(\frac{-1}{91}\right)\left(\frac{2}{91}\right)\left(\frac{9}{11}\right) \overset{\text{same}}{=} -(-1)(-1)\left(\frac{9}{91}\right)$

$$= -\left(\frac{9}{91}\right) \overset{\text{QR}}{=} -\left(\frac{91}{9}\right) = -\left(\frac{1}{9}\right) = -1$$

QR, $9 \equiv 1 (4)$

$91 \equiv 1 (9)$

Method 3: combination

$$\left(\frac{255}{419}\right) = \left(\frac{91}{255}\right) = \left(\frac{91}{3}\right)\cdot\left(\frac{91}{5}\right)\left(\frac{91}{17}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{5}\right)\left(\frac{6}{17}\right)$$

↑ as above

↑ $255 = 3 \cdot 5 \cdot 17$ & def'n of Jacobi symbol

↑ $91 \equiv 1\ (5)$, $91 \equiv 1\ (3)$, $91 \equiv 6\ (17)$

$$= \left(\frac{2}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

↑ $17 \equiv 1\ (8)$, so $\left(\frac{2}{17}\right) = 1$

↑ QR, 3, 17 prime, $17 \equiv 1\ (4)$

↖ $17 \equiv -1\ (3)$

Facts (you know) if $m = 2, 4, p^k, 2p^k$ p odd prime $k \geq 1$
then $\exists$ primitive root mod p^k.

Pf: We already know that there exist primitive roots mod p.

Next case: mod p^2:

Let a be a primitive root mod p

Note: Suppose b is a primitive root mod p^2
Then every (invertible) class mod p^2 is a power of b

But if x is invertible mod p, $p \nmid x$, so x is invertible mod p^2
$\Rightarrow x \equiv (\text{power of } b) \pmod{p^2} \Rightarrow x \equiv (\text{power of } b) \pmod{p}$.
$\Rightarrow b$ is a primitive root mod p

(eg. if b is a primitive root mod 25, $b \equiv \pm 2 \pmod 5$, $b \not\equiv \pm 1 \pmod 5$)

Goal: Find primitive root b, $b \equiv a \pmod p$ (perhaps $b \not\equiv a \pmod{p^2}$)

Let r be order of a mod p^2. By Euler's thm, $r \mid \phi(p^2) = p(p-1)$

Conversely, $a^r \equiv 1 \pmod{p^2} \Rightarrow a^r \equiv 1 \pmod p \Rightarrow p-1 \mid r$
($p-1 = \text{ord}_p(a)$)

$= p^2(1 - \frac{1}{p})$
fraction $\frac{1}{p}$ of classes are divisible by p

See then $r \in \{p-1, p(p-1)\}$:

write $r = (p-1)\cdot \ell$ then $r \mid p(p-1) \Leftrightarrow \frac{p(p-1)}{\ell(p-1)} \in \mathbb{Z}$

$\Leftrightarrow \frac{p}{\ell} \in \mathbb{Z} \Leftrightarrow \ell \mid p \Leftrightarrow \ell \in \{1, p\}$

If $r = (p-1)p$ were done (a is primitive root mod p^2)

Otherwise, $r = p-1$

More generally, if $b \equiv a \ (p)$ then $\operatorname{ord}_{p^2}(b) \in \{p-1, p(p-1)\}$

so b is a primitive root iff $b^{p-1} \not\equiv 1 \ (p^2)$

So suppose $a^{p-1} \equiv 1 \ (p^2)$, let $b = a+p$

then $b^{p-1} = (a+p)^{p-1} = a^{p-1} + (p-1)a^{p-2}\cdot p + \sum_{k=2}^{p-1} \binom{p-1}{k} a^{p-1-k} p^k$

$\equiv 1 - a^{p-2} p \ (p^2)$: $p^k \equiv 0 \ (p^2)$ if $k \geq 2$

$\not\equiv 1 \ (p^2)$

since $p^2 \nmid a^{p-2} p \Leftrightarrow p \nmid a^{p-2}$

So b is a primitive root.

Question: (PS6, problem 3)

(a) Suppose a has order r mod m has order 1 or 2
Then product of all distinct powers of a mod m $\equiv$ mod m

Pf: Powers of a mod m are $a^0, a^1, a^2, \ldots, a^{r-1}$.

Their product is $a^0 \cdot a^1 \cdot a^2 \cdots a^{r-1} = a^{0+1+2+\cdots+(r-1)}$

$$= a^{\frac{r(r-1)}{2}}$$

$\uparrow$ PS 1

The square of this number is $\left(a^{\frac{r(r-1)}{2}}\right)^2 = a^{r(r-1)} = (a^r)^{r-1} \equiv 1^{r-1} \equiv 1 \pmod m$

So $\mathrm{ord}_m\left(a^{\frac{r(r-1)}{2}}\right) \mid 2$, i.e. the order is 1 or 2.

(b) Let $m = p^k$. Prove that the product of all invertible residues mod m is $\equiv -1 \pmod m$ (case $m=p$ is Wilson's thm)
p odd prime

Pf: Let a be a primitive root mod p^k.
Then the indicated prod is the prod over all powers of a

So we find: $\prod_{x \bmod p^k,\ p \nmid x} x \equiv a^{\frac{r(r-1)}{2}}$, $r = \mathrm{ord}_{p^k}(a) = \phi(p^k) = p^k - p^{k-1}$.

We know this squares to 1. Previous PS: $y^2 \equiv 1 \pmod{p^k}$
$\Rightarrow y \equiv \pm 1 \pmod{p^k}$

Finally, let a be a primitive root mod p^k, p odd prime

$$r = p^{k-1}(p-1) = \text{ord}_{p^k}(a)$$

We need to decide if $a^{\frac{r(r-1)}{2}} \equiv 1 \ (p^k)$

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

But $a^{\frac{r(r-1)}{2}} \equiv 1 \ (p^k)$ iff $r = \text{ord}(a) \mid \frac{r(r-1)}{2}$

this will occur iff $\frac{r-1}{2} \in \mathbb{Z}$

But $r = p^{k-1}(p-1)$ is a multiple of the even number $p-1$

so $r-1$ is odd, $\frac{r-1}{2} \notin \mathbb{Z}$

So $a^{\frac{r(r-1)}{2}} \not\equiv +1 \ (p^k)$ so $\prod_{\substack{x (p^k) \\ p \nmid x}} x \equiv a^{\frac{r(r-1)}{2}} \equiv -1 \ (p^k)$

Question: $q \mid 2^p - 1$ p odd, q prime

Show: $q \equiv 1 \ (2p)$

(1) $q \mid 2^p - 1 \Rightarrow 2^p \equiv 1 \ (q)$ so $\text{ord}_q(2) \mid p$, i.e. $\text{ord}_q(2) \in \{1, p\}$

But $\text{ord}_q(2) \neq 1$ $(2^1 \not\equiv 1 \ (q))$ so $\text{ord}_q(2) = p$

(2) Fermat's little thm: $\text{ord}_q(2) \mid q-1$ i.e. $p \mid q-1$, or $q \equiv 1 \ (p)$

Aside: q odd $\mid 2^p - 1$, $2^p - 1$ is odd, so q is odd $(q \equiv 1 \ (2))$

so by CRT $q \equiv 1 \ (2p)$

---

(3) $\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv 2^{p \cdot \frac{q-1}{2p}} \leftarrow \text{integer}$

$\equiv 1 \ (q)$ so 2 is a square mod q

so $q \equiv \pm 1 \ (8)$

either

so $q \equiv 1 \ (8p)$

or

$q \equiv 1 \ (p)$, $q \equiv -1 \ (8)$