Today: mostly exercise 3

Computations w/ Legendre symbol.

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square mod } p \\ -1 & \text{if } n \text{ is not a square mod } p \end{cases}$$

p prime, $p \nmid n$.

Main properties: · If $n \equiv m \mod p$

$$\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$$

Exercise 3.

127 is prime.

- $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

- $\left(\frac{-1}{p}\right)$ is 1 if $p \equiv 1 \mod 4$, -1 if $p \equiv 3 \mod 4$

- $\left(\frac{2}{p}\right)$ is 1 if $p \equiv 1$ or $7 \mod 8$, -1 if $p \equiv 3$ or $5 \mod 8$.

- Quadratic reciprocity: $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

In pack: $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p, q \equiv 3 \mod 4$ $\quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ otherwise

(1) Is 66 a square mod 127? NO :(

$\iff$ Is $\left(\frac{66}{127}\right) = 1$?

$66 = 2 \cdot 3 \cdot 11$

$\left(\frac{66}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{3}{127}\right)\left(\frac{11}{127}\right)$ $\quad 1 \cdot (-1) \cdot 1$ $\quad \boxed{= -1}$

$127 \equiv 7 \bmod 8$ "1" $= \left(\frac{3}{127}\right)\left(\frac{11}{127}\right)$.

Use q.r.

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

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

because $127 \equiv 1 \bmod 3$

$= -1$

$\left(\frac{11}{127}\right) = -\left(\frac{127}{11}\right)$

$= -\left(\frac{6}{11}\right)$

because $127 \equiv 1 \bmod 3$.

$= -(-1) = 1$

Note -1 rule is also useful sometimes. — e.g. $\left(\frac{12}{13}\right) = \left(\frac{-1}{13}\right)$

$\left(\frac{11}{13}\right) = \left(\frac{-2}{13}\right)$

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

7.14 For which odd primes p is 5 a square mod p?

i.e. $\left(\frac{5}{p}\right) = 1$

quadratic recip: $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$.

so 1 $\boxed{\text{if } p \equiv 1 \text{ or } 4 \pmod 5.}$

3.(5)

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \quad \text{if } p \equiv 1 \mod 4$$

need also then $p \equiv 1 \mod 3$.

$$= -\left(\frac{p}{3}\right) \quad \text{if } p \equiv 3 \mod 4.$$

need also $\left(\frac{p}{3}\right) = -1$, $p \equiv 2 \mod 3$.

Need either $p \equiv 1 \mod 4$ and $p \equiv 1 \mod 3$

or $p \equiv 3 \mod 4$ and $p \equiv 2 \mod 3$

by CRT

either $p \equiv 1 \mod 12$

$p \equiv -1 (\equiv 11) \mod 12$