

18.791

Quadratic Reciprocity Thm:

$p, q$  distinct odd primes.  $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

ex: Is 42 a square mod 61?

$$\left(\frac{42}{61}\right) = \left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right)$$

$$\left(\frac{2}{61}\right) = -1, \text{ since } 61 \equiv -3 \pmod{8}$$

$$\left(\frac{3}{61}\right) = (-1)^{1 \cdot \left(\frac{61-1}{2}\right)} \left(\frac{61}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{7}{61}\right) = (-1)^{\left(\frac{61-1}{2}\right)\left(\frac{7-1}{2}\right)} \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = (-1)^{\left(\frac{7-1}{2}\right)\left(\frac{5-1}{2}\right)} \left(\frac{7}{5}\right) = 1 \cdot \left(\frac{2}{5}\right) = -1, \text{ since}$$

$1 \cdot 4$  are squares mod 5

$$\left(\frac{42}{61}\right) = -1 \cdot 1 \cdot -1 = 1, \text{ so } 42 \text{ is a square mod } 61$$

ex: For which primes  $p$  is 7 square mod  $p$ ?

i.e. when is  $\left(\frac{7}{p}\right)$

$$\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right)$$

case 1:  $p \equiv 1 \pmod{4}$  Want  $\left(\frac{p}{7}\right) = 1$ .

$x$	1	2	3	4	5	6	
$x^2$	1	4	2	2	4	1	

so need  $p \equiv 1, 2, 4 \pmod{7}$

$$p \equiv 1, 9, 25 \pmod{28}$$

$$p \equiv 1, 9, 25 \pmod{28}$$

case 2:  $p \equiv 3 \pmod{4}$  Want  $\left(\frac{p}{7}\right) = -1$

so need  $p \equiv 3, 5, 6 \pmod{7}$ .

$$\text{i.e. } p \equiv 3, 19, 27 \pmod{28}$$

Thus, 7 is a square mod  $p$  iff  $p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$

Proof of QR Thm: (due to Sey Yoon Kw)

$$\text{Let } m = \frac{pq-1}{2} = \frac{p-1}{2}q + \frac{q-1}{2} = \frac{q-1}{2}p + \frac{p-1}{2}$$

$$A = \{n \mid 1 \leq n \leq m \text{ and } (n, pq) = 1\}$$

$$B = \{n \mid 1 \leq n \leq m \text{ and } (n, p) = 1\}$$

$$B = A \cup \{q, 2q, \dots, \frac{p-1}{2}q\}$$

$a$  = product of elts in  $A$

$b$  = product of elts in  $B$

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

$$B = \left(\bigcup_{j=0}^{\frac{q-1}{2}} \bigcup_{i=1}^{p-1} (jp+i)\right) \cup \left(\bigcup_{i=1}^{\frac{p-1}{2}} \left(\frac{q-1}{2}p+i\right)\right)$$

$$b \equiv \left(\prod_{j=0}^{\frac{q-1}{2}} \prod_{i=1}^{p-1} i\right) \left(\prod_{i=1}^{\frac{p-1}{2}} i\right) \pmod{p}$$

$$\equiv ((p-1)!)^{\frac{q-1}{2}} \left(\frac{p-1}{2}!\right) \pmod{p}$$

$$\begin{aligned}
 \text{So } b &\equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \\
 &\equiv a \left(\frac{a}{p}\right) \left(\frac{p-1}{2}\right)! \pmod{p} \\
 \Rightarrow (-1)^{\frac{p-1}{2}} &\equiv a \left(\frac{a}{p}\right) \pmod{p} \Rightarrow a \equiv (-1)^{\frac{p-1}{2}} \left(\frac{a}{p}\right) \pmod{p} \\
 \text{By symmetry, } a &\equiv (-1)^{\frac{q-1}{2}} \left(\frac{a}{q}\right) \pmod{q}
 \end{aligned}$$

So we see that quadratic reciprocity is equivalent to a statement about the congruence class of  $a \pmod{pq}$ .

Case 1:  $p \equiv q \equiv 1 \pmod{4}$

$$\text{Q.R.: } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), \text{ which is eq. to } a \equiv \pm 1 \pmod{pq}$$

Case 2:  $p \equiv 1 \pmod{4}, q \equiv 3 \pmod{4}$

$$\text{Q.R.: } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right), \text{ so } a \equiv \pm 1 \pmod{p} \text{ and } a \equiv \mp 1 \pmod{q}$$

$$\Leftrightarrow a \not\equiv \pm 1 \pmod{pq}$$

Case 3:  $p \equiv 3 \pmod{4}, q \equiv 1 \pmod{4}$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right), \text{ so } a \equiv \pm 1 \pmod{p} \text{ and } a \equiv \mp 1 \pmod{q}$$

Case 4:  $p \equiv q \equiv 3 \pmod{4}$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), \text{ so } a \equiv \pm 1 \pmod{pq}$$

Conclusion:  $a \equiv \pm 1 \pmod{pq}$  iff  $p \equiv q \equiv 1 \pmod{4}$  implies Q.R.

Proof: There exist for every  $n \in A$  a unique number  $n' \in A$

$$\text{s.t. } n \cdot n' \equiv \pm 1 \pmod{pq}$$

We know  $\exists n_2, n_3$  s.t.

$$n n_2 \equiv 1 \pmod{pq}$$

$$n n_3 \equiv -1 \pmod{pq}$$

exercise: Exactly one of  $n_2, n_3 \in A$ .

$$a = \prod_{n \in A} n \equiv \pm \prod_{\substack{n \in A \\ n = n'}} n \pmod{pq} \equiv \pm \prod_{n^2 \equiv \pm 1 \pmod{pq}} n \pmod{pq}$$

$n^2 \equiv -1 \pmod{pq}$  has no sol'n unless  $p \equiv q \equiv 1 \pmod{4}$ ,  $\Rightarrow$

$$n^2 \equiv 1 \pmod{pq} \text{ has 4 sol'n: } \pm 1, \pm u$$

$$\text{so } \prod_{n \in A} n = \begin{cases} \pm 1 \cdot u & \text{if } p \text{ or } q \not\equiv 1 \pmod{4} \\ \pm (i \cdot i) u = \pm u^2 & \text{if } p \equiv q \equiv 1 \pmod{4} \end{cases}$$