

18.791

31 Mar 2003

Theorem:  $p$  and  $q$  distinct odd primes

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

Proof last time.

Jacobi symbol

$$\text{ex: compute } \left(\frac{-35}{97}\right)$$

$$\text{current answer: } \left(\frac{-35}{97}\right) = \left(\frac{-1}{97}\right)\left(\frac{7}{97}\right)\left(\frac{5}{97}\right)$$

Want:  $\left(\frac{P}{Q}\right)$  with  $Q$  compositeDef.  $Q$  odd and  $Q = q_1 \cdots q_s$  ← odd primes.Then define  $\left(\frac{P}{Q}\right)$  to be  $\prod_{i=1}^s \left(\frac{P}{q_i}\right)$ . (Note  $\left(\frac{P}{Q}\right) = 1 \nRightarrow P$  is a square mod  $Q$ )Thrm 1:  $Q > 0$  odd.

$$\text{i) } \left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$$

$$\text{ii) } \left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$$

Thrm 2:  $P$  and  $Q$  distinct odd positive numbers.

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$$

$$\text{ex: back to } \left(\frac{-35}{97}\right) = \left(\frac{-1}{97}\right)\left(\frac{35}{97}\right) = (-1)^{48} \cdot (-1)^{\frac{35^2-1}{8}} \left(\frac{97}{35}\right) = \left(\frac{27}{35}\right) = (-1)^{13 \cdot 12} \left(\frac{55}{27}\right) = -\left(\frac{8}{27}\right) = -\left(\frac{2}{27}\right) = -(-1)^{\frac{27^2-1}{8}} = -(-1)^{9} = 1$$

$$\frac{n^2-1}{8} \text{ is even iff } n \equiv \pm 1 \pmod{8}$$

Lemma:  $a, b$  odd.

$$1) \frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod{2}$$

$$2) \frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{(ab)^2-1}{8} \pmod{2}.$$

Proof:

$$1) \frac{ab-1}{2} = \frac{(a-1)(b-1)}{2} + \frac{a-1}{2} + \frac{b-1}{2} \Rightarrow \frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}$$

$$2) \frac{a^2b^2-1}{8} = \frac{(a^2-1)(b^2-1)}{8} + \frac{a^2-1}{8} + \frac{b^2-1}{8}$$

even  
mult. of 8

Proof of Thrm 1:i) Write  $Q = q_1 \cdots q_s$ 

$$\left(\frac{-1}{Q}\right) = \left(\frac{-1}{q_1}\right) \cdots \left(\frac{-1}{q_s}\right) = (-1)^{\frac{q_1-1}{2}} \cdots (-1)^{\frac{q_s-1}{2}} = (-1)^{\sum_{j=1}^s \frac{q_j-1}{2}}$$

$$\text{Lemma part 1 and induction } \Rightarrow \sum_{j=1}^s \frac{q_j-1}{2} \equiv \frac{q_1 \cdots q_s - 1}{2} \pmod{2}$$

$$\text{so } (-1)^{\sum_{j=1}^s \frac{q_j-1}{2}} = (-1)^{\frac{q_1 \cdots q_s - 1}{2}} = (-1)^{\frac{Q-1}{2}}$$

$$ii) \left(\frac{2}{Q}\right) = \left(\frac{2}{q_1}\right) \cdots \left(\frac{2}{q_s}\right) = (-1)^{\frac{q_1-1}{2}} \cdots (-1)^{\frac{q_s-1}{2}} = (-1)^{\sum_{j=1}^s \frac{q_j-1}{2}}$$

similarly by Lemma part 1,  $\sum_{j=1}^s \frac{q_j-1}{2} \equiv \frac{q_1 \cdots q_s - 1}{2} \pmod{2}$

so  $(-1)^{\sum_{j=1}^s \frac{q_j-1}{2}} = (-1)^{\frac{q_1 \cdots q_s - 1}{2}} = (-1)^{\frac{Q-1}{2}}$

Proof of Thrm 2:

$$P = p_1 \cdots p_n \quad Q = q_1 \cdots q_s$$

$$\left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = \prod_{i=1}^n \prod_{j=1}^s \left(\frac{p_i}{q_j}\right) \left(\frac{q_j}{p_i}\right) = \prod_i \prod_j (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} = (-1)^{\sum_i \sum_j \left(\frac{p_i-1}{2}\right) \left(\frac{q_j-1}{2}\right)}$$

$$\sum_i \sum_j \left(\frac{p_i-1}{2}\right) \left(\frac{q_j-1}{2}\right) = \sum_i \left(\frac{p_i-1}{2}\right) \sum_j \left(\frac{q_j-1}{2}\right) \equiv \sum_i \left(\frac{p_i-1}{2}\right) \left(\frac{P-1}{2}\right) \pmod{2}$$

$$\equiv \frac{P-1}{2} \sum_i \frac{p_i-1}{2} \equiv \frac{P-1}{2} \cdot \frac{P-1}{2} \pmod{2}.$$

Thus  $(-1)^{\sum_i \sum_j \left(\frac{p_i-1}{2}\right) \left(\frac{q_j-1}{2}\right)} = (-1)^{\frac{P-1}{2} \cdot \frac{P-1}{2}}$

Theorem: a nonsquare integer

Then there are infinitely many primes for which  $a$  is a quadratic nonresidue

Proof: We can assume  $a$  is square free

$$a = 2^e q_1 \cdots q_n \text{ where } e \in \{0, 1\}$$

consider case when  $n \geq 1$

say  $l_1, \dots, l_k$  are all primes for which  $\left(\frac{a}{l_i}\right) = -1$

let  $s$  be a quadratic nonresidue mod  $q_n$

let  $b$  be a solution of  $x \equiv 1 \pmod{l_i}$   $x \equiv 1 \pmod{8}$   $x \equiv 1 \pmod{q_i}$ ,  $i=1, \dots, n-1$

$$x \equiv s \pmod{q_n}$$

$$b = p_1 \cdots p_m \quad \text{note } b \equiv 1 \pmod{8} \text{ so } (-1)^{\frac{b-1}{2}} = 1, \text{ so } (-1)^{\frac{b-1}{2}} = 1.$$

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right) \left(\frac{q_1}{b}\right) \cdots \left(\frac{q_n}{b}\right) = 1 \cdot \left(\frac{b}{q_1}\right) \cdots \left(\frac{b}{q_n}\right) = \left(\frac{1}{q_1}\right) \cdots \left(\frac{1}{q_{n-1}}\right) \cdot \left(\frac{s}{q_n}\right) = -1$$

$$\left(\frac{a}{b}\right) = -1 \Rightarrow \text{at least one of } \left(\frac{a}{p_i}\right) = -1$$

which is a contradiction