

HOMEWORK 5  
 Math 104 - Dr. Evans  
 UCSD Winter 2004  
 Due Thursday, February 12

1. In class, it was shown that  $-2$  is a square modulo  $p$  when  $p \equiv 3 \pmod{8}$ , and  $-2$  is a nonsquare modulo  $p$  when  $p \equiv 7 \pmod{8}$ . Prove that  $-2$  is a square modulo  $p$  when  $p \equiv 1 \pmod{8}$ , and  $-2$  is a nonsquare modulo  $p$  when  $p \equiv 5 \pmod{8}$ .  
 (Hint: Separate out the odd factors from the even factors in  $(p-1)!$  and apply Wilson's Theorem.)

Assume that  $p \equiv 1 \pmod{4}$ , which means  $\frac{p-1}{2}$  is even. Then

$$\begin{aligned} (p-1)! &= \left(1 \cdot 3 \cdot 5 \cdot \dots \cdot (p-2)\right) \left(2 \cdot 4 \cdot 6 \cdot \dots \cdot (p-1)\right) \\ &= \left(1 \cdot 3 \cdot 5 \cdot \dots \cdot (p-2)\right) \cdot 2^{\frac{p-1}{2}} \cdot \left(1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2}\right) \end{aligned}$$

since each parenthesis has  $\frac{p-1}{2}$  numbers in it. Of the  $\frac{p-1}{2}$  odd numbers, half are less than  $\frac{p}{2}$  and half are greater than  $\frac{p}{2}$ . Furthermore, if  $k$  is an odd number between 1 and  $\frac{p}{2}$ , then  $k \equiv -(p-k) \pmod{p}$  and  $p-k$  is even greater than  $\frac{p}{2}$ . Hence,

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (p-2) \equiv (-1)^{\frac{p-1}{4}} \left(\frac{p+1}{2} \cdot \frac{p+3}{2} \cdot \dots \cdot (p-2) \cdot (p-1)\right) \pmod{p}$$

Therefore,

$$\begin{aligned} (p-1)! &= \left(1 \cdot 3 \cdot 5 \cdot \dots \cdot (p-2)\right) \cdot 2^{\frac{p-1}{2}} \cdot \left(1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2}\right) \\ &\equiv (-1)^{\frac{p-1}{4}} \left(\frac{p+1}{2} \cdot \frac{p+3}{2} \cdot \dots \cdot (p-2) \cdot (p-1)\right) \cdot 2^{\frac{p-1}{2}} \cdot \left(1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2}\right) \\ &\equiv (-1)^{\frac{p-1}{4}} \cdot 2^{\frac{p-1}{2}} \cdot (p-1)! \pmod{p} \end{aligned}$$

Note that  $2^{\frac{p-1}{2}} = (-2)^{\frac{p-1}{2}}$  since  $\frac{p-1}{2}$  is even. Canceling  $(p-1)!$  from both sides and solving for  $2^{\frac{p-1}{2}}$ , we have

$$2^{\frac{p-1}{2}} \equiv (-2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \equiv \begin{cases} 1 & \text{if } \frac{p-1}{4} \text{ is even} \\ -1 & \text{if } \frac{p-1}{4} \text{ is odd} \end{cases}$$

Now  $\frac{p-1}{4}$  is even when  $p \equiv 1 \pmod{8}$  and odd when  $p \equiv 5 \pmod{8}$ . By Euler's Criterion, we conclude that  $-2$  is a square when  $p \equiv 1 \pmod{8}$  and is a nonsquare when  $p \equiv 5 \pmod{8}$ .

2. Use the Law of Quadratic Reciprocity to prove that  $-3$  is a square modulo  $p$  if and only if  $p \equiv 1 \pmod{3}$ .

Note that if  $q = -3$ , then  $q^* = q$  since  $-3 \equiv 1 \pmod{4}$ . Hence, we can apply quadratic reciprocity directly:  $q^* = -3$  is a square modulo  $p$  if and only if  $p$  is a square modulo 3. The only nonzero square modulo 3 is 1, so  $-3$  is a square modulo  $p$  if and only if  $p \equiv 1 \pmod{3}$ .

3. Use problem 2 and the condition for  $-1$  to be a square modulo  $p$  to find a congruence relation on  $p$  that is true if and only if  $3$  is a square modulo  $p$ .

From class,  $-1$  is a square modulo  $p$  if and only if  $p \equiv 1 \pmod{4}$ . For  $3$  to be a square, either  $-1$  and  $-3$  are squares modulo  $p$ , or  $-1$  and  $-3$  are nonsquares modulo  $p$ . In the first case,  $p \equiv 1 \pmod{4}$  and  $p \equiv 1 \pmod{3}$  imply that  $p \equiv 1 \pmod{12}$  (one can show this by the process shown in class). In the second case,  $p \equiv 3 \pmod{4}$  and  $p \equiv 2 \pmod{3}$  imply  $p \equiv 11 \pmod{12}$ . So the final answer is

$$3 \text{ is a square modulo } p \iff p \equiv 1, 11 \pmod{12}$$

4. In class, it was shown that  $5$  is a square modulo  $p$  if and only if  $p \equiv \pm 1 \pmod{5}$ . Use this and the condition for  $-1$  to be a square modulo  $p$  to finish the proof that  $-5$  is a square modulo  $p$  if and only if  $p \equiv 1, 3, 7, \text{ or } 9 \pmod{20}$ .

The proof is similar to problem 3. For  $-5$  to be a square modulo  $p$ , either  $-1$  and  $5$  are squares modulo  $p$ , or  $-1$  and  $5$  are nonsquares modulo  $p$ . In the first case,  $p \equiv 1 \pmod{4}$  and  $p \equiv 1, 4 \pmod{5}$  imply that  $p \equiv 1, 9 \pmod{20}$ . In the second case,  $p \equiv 3 \pmod{4}$  and  $p \equiv 2, 3 \pmod{5}$  imply that  $p \equiv 3, 7 \pmod{20}$ . Putting them together,

$$-5 \text{ is a square modulo } p \iff p \equiv 1, 3, 7, 9 \pmod{20}$$