

**Lior Silberman's Math 312: Problem Set 6 (due 21/6/18)**

**Primitive roots**

1. For each  $p \in \{11, 13, 17, 19\}$  find a primitive root mod  $p$ . Justify your answers.
2. How many primitive roots are there mod 25? Find all of them.
3. (Wilson's Theorem, again)
  - (a) Let  $r = \text{ord}_m(a)$  and let  $S$  be the product of the  $r$  distinct residues which are powers of  $a$  mod  $m$ . Show that  $\text{ord}_m(S)$  is 1 if  $r$  is odd and 2 if  $r$  is even.
  - (b) Let  $p$  be an odd prime, and let  $k \geq 1$ . Show that the product of all invertible residues mod  $p^k$  is congruent to  $-1 \pmod{p^k}$ .  
*Hint:* There is a primitive root mod  $p^k$ .
4. (removed)
5. Let  $p$  be a prime. Let  $S$  be a set of representatives for all the primitive roots mod  $p$  (we showed in class this set has size  $\phi(p-1)$ ). Find  $\prod_{r \in S} r \pmod{p}$ .

**Quadratic reciprocity**

6. Evaluate the following Legendre symbols.
  - (a)  $\left(\frac{48}{103}\right)$ ,  $\left(\frac{3325}{14407}\right)$ ,  $\left(\frac{19382}{48397}\right)$ , using factorization and quadratic reciprocity.
  - (b)  $\left(\frac{799}{37}\right)$ ,  $\left(\frac{3133}{3137}\right)$ ,  $\left(\frac{39270}{49177}\right)$ , using Jacobi symbols.
7. Let  $p$  be an odd prime and let  $q|2^p - 1$ . Recall that  $q \equiv 1 \pmod{2p}$ .
  - (a) We have seen before that  $\text{ord}_q(2) = p$ . Use this and Euler's criterion to show that 2 is a square mod  $q$ . Conclude that  $q \equiv \pm 1 \pmod{8}$ .
  - (b) Show that  $M_{17} = 2^{17} - 1 < 132,000$  is prime, only trying to divide by three numbers.  
RMK Why is it not necessary to show that these numbers are prime?
8. (Math 437 Midterm, 2009)
  - (a) Let  $a \geq 3$  be odd and let  $p|a^2 - 2$  be prime. Show that  $p \equiv \pm 1 \pmod{8}$ .
  - (b) Let  $a \geq 3$  be odd. Show that *some* prime divisor of  $a^2 - 2$  is congruent to  $-1 \pmod{8}$ .  
*Hint:* What is the residue class of  $a^2 - 2 \pmod{8}$ ?
  - (c) Show that there are infinitely many primes congruent to  $-1 \pmod{8}$ .