

Due: March 20, 2008

## 1 Roots of -1 (20 points)

Let  $p$  be an odd prime. Show that  $-1$  is a square mod  $p$  if and only if  $p = 1 \pmod{4}$ .

## 2 Negative squares

Let  $p$  be an odd prime. Using the previous question to prove the following.

### 2.1 Case 1 (10 points)

If  $p = 1 \pmod{4}$ , then  $a$  is a square if and only if  $-a$  is a square mod  $p$ .

### 2.2 Case 2 (10 points)

If  $p = 3 \pmod{4}$ , then  $a$  is a square if and only if  $-a$  is *not* a square mod  $p$ .

## 3 Roots of roots (20 points)

Let  $p$  be a prime with  $p = 3 \pmod{4}$ . Show that every square mod  $p$  has exactly one root that is also a square. The previous problem may be helpful.

## 4 Safe primes and generators (40 points)

A prime  $p$  is called a *safe prime* if it can be written as  $2q + 1$ , where  $q$  is also prime. If  $p$  is a safe prime, then show that every non-square is a generator except  $-1$ . (Hint: You should start with Fermat's Little Theorem, combined with results from the previous homework.)