

MA357, Spring 2008 — Problem Set 7

All about quadratic reciprocity and related topics. This is due **Friday, May 2**.

1. (We will do this in class next week; try to beat me to it!)

Let p be an odd prime number, and let a and b be integers.

a. Show that if $p \equiv 3 \pmod{4}$ and $p|(a^2 + b^2)$, then $p|a$ and $p|b$.

b. Show that if $p \equiv 1 \pmod{4}$ then there exist integers a and b such that $p \nmid a$, $p \nmid b$, and $p|(a^2 + b^2)$.

2. Silverman, Exercise 25.1.

3. Silverman, Exercise 25.2.

4. Silverman, Exercise 25.4.

5. Show that our result about when 2 is a square modulo a prime p can be expressed by the formula

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

6. Which of the following congruences have solutions? How many solutions?

a. $x^2 \equiv 125 \pmod{1016}$

b. $x^2 \equiv 129 \pmod{1016}$

c. $x^2 \equiv 41 \pmod{79}$

d. $41x^2 \equiv 43 \pmod{79}$

e. $43x^2 \equiv 47 \pmod{79}$

f. $x^2 \equiv 151 \pmod{840}$

(It's helpful to remember that if m and n are relatively prime, then $a \equiv b \pmod{mn}$ if and only if we have both $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. So you can factor the modulus, then use the Chinese Remainder Theorem.)

7. Show that for any n the prime divisors of $n^2 - n + 1$ have to be congruent to 1 modulo 6. (Hint: complete the square.)

For fun only: This problem gives a fancy proof of the quadratic reciprocity law, based on the identity

$$\frac{\sin(mx)}{\sin(x)} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin^2(x) - \sin^2(2\pi j/m) \right),$$

which we'll take for granted (at least for the moment).

Let p and q be odd primes.

- a. Let s run through the set $S = \{1, 2, \dots, \frac{p-1}{2}\}$. Define $m_q(s) = \pm 1$ by the condition

$$qs \equiv m_q(s)s_q \pmod{p}, \quad \text{where } 1 \leq s_q \leq \frac{p-1}{2}.$$

Explain why Gauss's Lemma, which we discussed in class, boils down to the equation

$$\left(\frac{q}{p}\right) = \prod_{s=1}^{\frac{p-1}{2}} m_q(s).$$

- b. From here on we will use brackets around fractions to avoid confusion; $\left(\frac{a}{b}\right)$ always means the Legendre symbol. Show that

$$\sin \left[\frac{2\pi qs}{p} \right] = m_q(s) \sin \left[\frac{2\pi s_q}{p} \right],$$

then multiply all these equations to show that

$$\left(\frac{q}{p}\right) = \prod_{s=1}^{\frac{p-1}{2}} \frac{\sin \left[\frac{2\pi qs}{p} \right]}{\sin \left[\frac{2\pi s}{p} \right]}.$$

- c. Now apply the identity with $m = q$, $x = 2\pi s/p$, to get a formula for the Legendre symbol $\left(\frac{q}{p}\right)$.
- d. Swap p and q in the formula you just got to get a formula for $\left(\frac{p}{q}\right)$.
- e. Compare the two formulas to conclude that

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

- f. Finally: can you prove the trigonometric identity that fueled this proof?