18.781 Problem Set 3: Due Wednesday, March 8.

1.(a) Find out whether 7 is a quadratic residue modulo 23, using (i) Euler's criterion; (ii) Gauss's criterion; (iii) quadratic reciprocity.

(b) Compute $\left(\frac{361}{11}\right)$, $\left(\frac{-1111}{691}\right)$, $\left(\frac{1000}{97}\right)$.

(c) What is the discriminant of the quadratic polynomial

$$f(x) = 6x^2 + 23x + 7?$$

Use quadratic reciprocity to decide whether $f(x) \equiv 0 \pmod{11}$ has a solution. If you discover that there is one, find one explicitly.

2. Let m be square-free (that is, m is not divisible by any square integer greater than 1), and consider $\left(\frac{m}{p}\right)$ as a function of the odd prime p. Show that it depends only on

$p \pmod{m}$ if $m \equiv 1 \pmod{4}$;

$p \pmod{4m}$ if $m \equiv 2$ or $3 \pmod{4}$.

Thus for example determine $\left(\frac{-5}{p}\right)$ and $\left(\frac{5}{p}\right)$ for all primes p, in terms of the congruence class of p modulo 20 (respectively, 5).

3. Suppose that the Fermat number $F_m = 2^{2^m} + 1$ is prime, and that $m > 0$. Show that 3 is a primitive root mod F_m.

4. Suppose p is a prime greater than 5, and that $q = \frac{p-1}{2}$ is also prime.

(a) Show that $p \equiv 3$ or $7 \pmod{8}$.

(b) Show that 2 is a primitive root mod p if $p \equiv 3 \pmod{8}$, but that 2 has order q in $\mathbb{Z}_p^*$ if $p \equiv 7 \pmod{8}$.

Thus 2 is a primitive root modulo the primes $11, 59, 83, 107, \ldots$, but not modulo $7, 23, 47, 167, \ldots$. So the numbers $1, 2, 4, 8, \ldots, 2^{105}$, have distinct residues mod 107; whereas $2^{83} \equiv 1 \pmod{167}$. Unfortunately it is not known whether or not there are infinitely many primes p such that $\frac{p-1}{2}$ is also prime (much less subject to the additional condition that $p \equiv 3 \pmod{8}$).

5. Even with the use of the law of quadratic reciprocity, the Legendre symbol is in principle "incomputable," because before you can use quadratic reciprocity you have to factor the "numerator" into a product of primes. The *Jacobi symbol* overcomes this computational defect. It is defined for any two integers k, n, with n odd and positive, by

$$\left(\tfrac{k}{n}\right) = \prod_i \left(\tfrac{k}{p_i}\right)$$

where $n = \prod p_i$ is the prime factorization of n. (Remember, the Legendre symbol $\left(\frac{k}{p}\right)$ is extended to allow k divisible by declaring it to be 0 in that case.) **(a)** through **(c)** below are obvious. Check **(d)** through **(g)**.

(a) If $k \equiv l \pmod{n}$ then $\left(\frac{k}{n}\right) = \left(\frac{l}{n}\right)$.

(b) $\left(\frac{kl}{n}\right) = \left(\frac{k}{n}\right)\left(\frac{l}{n}\right)$.

(c) If also m is odd and positive then $\left(\frac{k}{mn}\right) = \left(\frac{k}{m}\right)\left(\frac{k}{n}\right)$.

(d) Compute $\left(\frac{-1}{n}\right)$.

(e) Compute $\left(\frac{2}{n}\right)$.

(f) Prove the following extended version of quadratic reciprocity: if m and n are positive odd numbers then

$$\left(\tfrac{m}{n}\right)\left(\tfrac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

(You'll want check that if $m = p_1 \cdots p_s$ and $n = q_1 \cdots q_t$ are prime factorizations then

$$\sum_{i,j} \tfrac{p_i-1}{2}\tfrac{q_j-1}{2} \equiv \tfrac{m-1}{2}\tfrac{n-1}{2} \pmod{2}$$

first.)

(g) Check that if m is a quadratic residue mod n, then $\left(\frac{m}{n}\right) = 1$. But the converse assertion is false, since for example $\left(\frac{2}{9}\right) = 1$ but 2 is not a quadratic residue mod 9.

Challenge Problem (G. Rousseau, *The Mathematical Intelligencer*, Vol. 14, No. 3, p. 64 (1992)) The "$pq-1$ puzzle" is like the famous "15 puzzle" or "jeu de taquin" of Sam Loyd, except that the frame has p rows and q columns instead of 4 rows and 4 columns. The movable tiles are numbered $1, 2, \ldots, pq-1$, with the blank square labelled 0. Say the pieces are in *row order* if the first row is $0, 1, \ldots, q-1$, the second is $q, q+1, \ldots, 2q-1$, and so on. They are in *column order* if the first column (reading down) is $0, 1, \ldots, p-1$, the second is $p, p+1, \ldots, 2p-1$, and so on. They are in *diagonal order* if they start with 0 at the upper left corner, and increase one by one along the main diagonal; whenever an edge is reached the sequence is continued one row down or one column to the right on the opposite edge. (For this to make sense, p and q must be relatively prime.)

Assume that p and q are distinct odd primes, and show:

(a) It is possible to pass from row to column order except when p and q are both congruent to 3 mod 4.

(b) It is possible to pass from row order to diagonal order if and only if q is a quadratic residue modulo p; and it is possible to pass from column order to diagonal order if and only if p is a quadratic residue modulo q.

$$\begin{aligned}\cos(2\pi/17) &= \frac{1}{16}\Big(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\Big)\\ &\quad +\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34}-2\sqrt{17}-2\sqrt{34+2\sqrt{17}}}\end{aligned}$$

–C. F. Gauss, *Disquisitiones Arithmeticae* §365.