NUMBER-THEORY EXERCISES, XI

DAVID PIERCE

Exercise 1. Compute the Legendre symbols $(91/167)$ and $(111/941)$.

Exercise 2. Find $(5/p)$ in terms of the class of p *modulo* 5.

Exercise 3. Find $(7/p)$ in terms of the class of p *modulo* 28.

Exercise 4. The nth **Fermat number,** or F_n, is $2^{2^n}+1$. A **Fermat prime** is a Fermat number that is prime.

(a) Show that every prime number of the form 2^m+1 is a Fermat prime.
(b) Show $4^k \equiv 4 \pmod{12}$ for all positive k.
(c) If p is a Fermat prime, show $(3/p) = -1$.
(d) Show that 3 is a primitive root of every Fermat prime.
(e) Find a prime p less than 100 such that $(3/p) = -1$, but 3 is not a primitive root of p.

Exercise 5. Solve the congruence $x^2 \equiv 11 \pmod{35}$.

Exercise 6. We have so far defined the Legendre symbol (a/p) only when $p \nmid a$; but if $p \mid a$, then we can define $(a/p) = 0$. We can now define (a/n) for arbitrary a and n: the result is the **Jacobi symbol,** and the definition is

$$\left(\frac{a}{n}\right) = \prod_p \left(\frac{a}{p}\right)^{k(p)}, \qquad \text{where} \qquad n = \prod_p p^{k(p)}.$$

(a) Prove that the function $x \mapsto (x/n)$ on $\mathbb{Z}$ is **completely multiplicative** in the sense that $(ab/n) = (a/n) \cdot (b/n)$ for all a and b (not necessarily co-prime).
(b) If $\gcd(a,n) = 1$, and the congruence $x^2 \equiv a \pmod{n}$ is soluble, show $(a/n) = 1$.
(c) Find an example where $(a/n) = 1$, and $\gcd(a,n) = 1$, but $x^2 \equiv a \pmod{n}$ is insoluble.
(d) If m and n are co-prime, show

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^k, \qquad \text{where} \qquad k = \frac{m-1}{2} \cdot \frac{n-1}{2}.$$

MATHEMATICS DEPT, MIDDLE EAST TECH. UNIV., ANKARA 06531, TURKEY
E-mail address: dpierce@metu.edu.tr
URL: http://www.math.metu.edu.tr/~dpierce/

Date: December 18, 2007.