NUMBER-THEORY EXERCISES, X

DAVID PIERCE

Exercise 1. The Law of Quadratic Reciprocity makes it easy to compute many Legendre symbols, but this law is not always needed. Compute $(n/17)$ and $(m/19)$ for as many n in $\{1, 2, \dots, 16\}$ and m in $\{1, 2, \dots, 18\}$ as you can, using only that, whenever p is an odd prime, and a and b are prime to p, then:

- $a \equiv b \pmod p \implies (a/p) = (b/p)$;
- $(1/p) = 1$;
- $(-1/p) = (-1)^{(p-1)/2}$;
- $(a^2/p) = 1$;
- $(2/p) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8; \\ -1, & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$

Exercise 2. Compute all of the Legendre symbols $(n/17)$ and $(m/19)$ by means of Gauss's Lemma.

Exercise 3. Find all primes of the form $5 \cdot 2^n + 1$ that have 2 as a primitive root.

Exercise 4. For every prime p, show that there is an integer n such that

$$p \mid (3 - n^2)(7 - n^2)(21 - n^2).$$

Exercise 5.

(a) If $a^n - 1$ is prime, show that $a = 2$ and n is prime.

(b) Primes of the form $2^p - 1$ are called **Mersenne primes.** Examples are 3, 7, and 31. Show that, if $p \equiv 3 \pmod 4$, and $2p + 1$ is a prime q, then $q \mid 2^p - 1$, and therefore $2^p - 1$ is not prime. (*Hint:* Compute $(2/q)$.)

Exercise 6. Assuming p is an odd prime, and $2p+1$ is a prime q, show that -4 is a primitive root of q. (*Hint:* Show $\operatorname{ord}_q(-4) \notin \{1, 2, p\}$.)

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 17, 2007.