NUMBER-THEORY EXERCISES, V

DAVID PIERCE

As usual, p and q are primes.

Exercise 1. The number 32 970 563 is the product of two primes. Find them.

Exercise 2. Factorize 1 003 207 (the product of two primes) knowing

$$1\,835^2 \equiv 598^2 \pmod{1\,003\,207}.$$

Exercise 3. Compute 16200 *modulo* 19.

Exercise 4. If $p \neq q$, and $\gcd(a, pq) = 1$, and $n = \operatorname{lcm}(p-1, q-1)$, show

$$a^n \equiv 1 \pmod{pq}.$$

Exercise 5. Show $a^{13} \equiv a \pmod{70}$.

Exercise 6. Assuming $\gcd(n, p) = 1$, and $0 \leqslant n < p$, solve the congruence

$$a^n x \equiv b \pmod{p}.$$

Exercise 7. Solve $2^{14}x \equiv 3 \pmod{23}$.

Exercise 8. Show $\displaystyle\sum_{k=1}^{p-1} k^p \equiv 0 \pmod{p}$.

Exercise 9. We can write the congruence $2^p \equiv 2 \pmod{p}$ as

$$2^p - 1 \equiv 1 \pmod{p}.$$

Show that, if $n \mid 2^p - 1$, then $n \equiv 1 \pmod{p}$. (*Suggestion:* Do this first if n is a prime q. Then $2^{q-1} \equiv 1 \pmod{q}$. If $q \not\equiv 1 \pmod{p}$, then $\gcd(p, q-1) = 1$, so $pa + (q-1)b = 1$ for some a and b. Now look at $2^{pa} \cdot 2^{(q-1)b}$ *modulo* n.)

Exercise 10. Let $F_n = 2^{2^n} + 1$. (Then $F_0, \dots, F_4$ are primes.) Show

$$2^{F_n} \equiv 2 \pmod{F_n}.$$

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: October 16, 2007.