NUMBER-THEORY EXERCISES, IX

DAVID PIERCE

Exercise 1. For $(\mathbb{Z}/(17))^\times$:

(a) construct a table of logarithms using 5 as the base;
(b) using this (or some other table, with a different base), solve:
  (i) $x^{15} \equiv 14 \pmod{17}$;
  (ii) $x^{4095} \equiv 14 \pmod{17}$;
  (iii) $x^4 \equiv 4 \pmod{17}$;
  (iv) $11x^4 \equiv 7 \pmod{17}$.

Exercise 2. If n has primitive roots r and s, and $\gcd(a, n) = 1$, prove

$$\log_s a \equiv \frac{\log_r a}{\log_r s} \pmod{\phi(n)}.$$

Exercise 3. In $(\mathbb{Z}/(337))^\times$, for any base, show

$$\log(-a) \equiv \log a + 168 \pmod{336}.$$

Exercise 4. Solve $4^x \equiv 13 \pmod{17}$.

Exercise 5. How many primitive roots has 22? Find them.

Exercise 6. Find a primitive root of 1250.

Exercise 7. Define the function λ by the rules

$$\lambda(2^k) = \begin{cases} \phi(2^k), & \text{if } 0 < k < 3; \\ \phi(2^k)/2, & \text{if } k \geqslant 3; \end{cases}$$

$$\lambda(2^k \cdot {p_1}^{\ell(1)} \cdots {p_m}^{\ell(m)}) = \operatorname{lcm}(\phi(2^k), \phi({p_1}^{\ell(1)}), \dots, \phi({p_m}^{\ell(m)})).$$

where the p_i are distinct odd primes.

(a) Prove that, if $\gcd(a, n) = 1$, then $a^{\lambda(n)} \equiv 1 \pmod{n}$.
(b) Using this, show that, if n is not 2 or 4 or an odd prime power or twice an odd prime power, then n has no primitive root.

Exercise 8. Solve the following quadratic congruences.

(a) $8x^2 + 3x + 12 \equiv 0 \pmod{17}$;
(b) $14x^2 + x - 7 \equiv 0 \pmod{29}$;
(c) $x^2 - x - 17 \equiv 0 \pmod{23}$;
(d) $x^2 - x + 17 \equiv 0 \pmod{23}$.

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 6, 2007.