NUMBER-THEORY EXERCISES, VIII

DAVID PIERCE

Exercise 1. We have $(\pm 3)^2 \equiv 2 \pmod 7$. Compute the orders of 2, 3, and -3, *modulo* 7.

Exercise 2. Suppose $\operatorname{ord}_n(a) = k$, and $b^2 \equiv a \pmod n$.

(a) Show that $\operatorname{ord}_n(b) \in \{k, 2k\}$.
(b) Find an example for each possibility of $\operatorname{ord}_n(b)$.
(c) Find a condition on k such that $\operatorname{ord}_n(b) = 2k$.

Exercise 3. This is about 23:

(a) Find a primitive root of least absolute value.
(b) How many primitive roots are there?
(c) Find these primitive roots as powers of the root found in (a).
(d) Find these primitive roots as elements of $[-11, 11]$.

Exercise 4. Assuming $\operatorname{ord}_p(a) = 3$, show:

(a) $a^2 + a + 1 \equiv 0 \pmod 3$;
(b) $(a + 1)^2 \equiv a \pmod 3$;
(c) $\operatorname{ord}_p(a + 1) = 6$.

Exercise 5. Find all elements of $[-30, 30]$ having order 4 *modulo* 61.

Exercise 6. $f(x) \equiv 0 \pmod n$ may have more than $\deg(f)$ solutions:

(a) Find four solutions to $x^2 - 1 \equiv 0 \pmod{35}$.
(b) Find conditions on a such that the congruence $x^2 - a^2 \equiv 0 \pmod{35}$ has four distinct solutions, and find these solutions.
(c) If p and q are odd primes, find conditions on a such that the congruence $x^2 - a^2 \equiv 0 \pmod{pq}$ has four distinct solutions, and find these solutions.

Exercise 7. If $\operatorname{ord}_n(a) = n - 1$, then n is prime.

Exercise 8. If $a > 1$, show $n \mid \phi(a^n - 1)$.

Exercise 9. If $2 \nmid p$ and $p \mid n^2 + 1$, show $p \equiv 1 \pmod 4$.

Exercise 10.

(a) Find conditions on p such that, if r is a primitive root of p, then so is $-r$.
(b) If p does not meet these conditions, then what is $\operatorname{ord}_p(-r)$?

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: November 20, 2007.