Number Theory Fall 2009
Homework 4
Due: Wed. Sep. 23, start of class

Instructions: For this assignment, you should **do all problems by hand.**

3.3 Inverses mod p

Exercise 3.6. *Let $G = (\mathbb{Z}/7\mathbb{Z})^\times$. We represent the elements of G by $1, 2, \ldots, 6$.*

(i) Write down the multiplication table for G.

(ii) Let $H = \{1, 6\}$. Show H is a subgroup of G. (It suffices to check H is closed under multiplication and each element of H has an inverse in H. In other words, you may use the first lemma of the next section.)

(iii) Determine the cosets of H in G.

(iv) Repeat (ii) and (iii) for the set $H = \{1, 2, 4\}$.

3.4 Fermat's little theorem

Exercise 3.7. *Check that the powers of a cyclically repeat in this example.*

(i) With the notation in the previous exercise (in $(\mathbb{Z}/7\mathbb{Z})^\times$), compute 3^k for $1 \le k \le 10$.

(ii) What is the cyclic subgroup of $(\mathbb{Z}/7\mathbb{Z})^\times$ generated by 3? What about generated by 2?

Exercise 3.8. *Use the formula $a^{-1} \equiv a^{p-2} \bmod p$ to compute the inverse of 5 mod 11.*

3.5 Congruence theorems of Wilson and Lagrange

Exercise 3.9. *Exercises 3.5.1, 3.5.2, 3.5.3. (Correction: 3.5.1 should say if $n > 5$ is not prime, show $n|(n-1)!$)*

Exercise 3.10. *Let $P(x) = x^2 + 1$. Clearly $P(x) = 0$ is not solvable in $\mathbb{Z}$. However $P(x) \equiv 0 \bmod 5$ is solvable mod 5. Determine all solutions.*

3.6 Inverses mod k

Exercise 3.11. *For $2 \le k \le 7$ and $k = 9$, do the following. Write down the elements in $(\mathbb{Z}/k\mathbb{Z})^\times$ and state the order of the group. For each $a \in (\mathbb{Z}/k\mathbb{Z})^\times$, find the smallest n such that $a^n = 1$. Determine if $(\mathbb{Z}/k\mathbb{Z})^\times$ is cyclic or not. If it is cyclic, state an element that generates the group.*

Exercise 3.12. *Show $\phi(p^j) = p^{j-1}(p-1)$ for $j \ge 1$. (Exercises 3.6.1, 3.6.2, 3.6.3.)*

Exercise 3.13. *We will show in Chapter 9 that if m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$. Check this in the special cases (i) $m = 3$ and $n = 5$ (Exercise 3.6.4), and (ii) $m = 2$ and n is an odd prime.*

Exercise 3.14. *Determine $\phi(60)$.*

Exercise 3.15. *Following the proof of Fermat's little theorem, prove Euler's theorem in the same way: For any invertible a mod k, we have $a^{\phi(k)} \equiv 1 \bmod k$. (Cf. p. 56.)*