Homework 2

Math 124, Fall 2005

Due Wednesday, Oct 5th (In class)

Good Luck!!!

1. Find all the solutions to

$$x^3 - 9x^2 + 23x - 15 \equiv 0 \mod 143.$$

2. Generalization of the Chinese remainder theorem.

   (a) Prove that if $m_1, \ldots m_r$ are pairwise relatively prime then the set of equations

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

   has a unique solution modulo $m_1, \ldots m_r$. [Hint: If $m = m_1 \ldots m_r$, first find b_j's such that

$$b_j(m/m_j) \equiv 0 \mod m_i \qquad b_j(m/m_j) \equiv 1 \mod m_j.]$$

   (b) Find all solutions, if there are any, to the system

$$\begin{aligned} x &\equiv 13 \mod 20 \\ x &\equiv 5 \mod 12 \\ x &\equiv 17 \mod 18. \end{aligned}$$

3. Prove that there are infinitely many primes of the form $4x + 1$ as follows. Suppose $p_1, \ldots, p_n$ are all primes of the form $4x + 1$. Let

$$n = 4(p_1 p_2 \cdots p_n)^2 + 1.$$

   Suppose p is a prime divisor of n.

   (a) Prove that the equation $x^2 + 1 = 0$ has a solution in $\mathbf{Z}/p$.

   (b) Conclude that there are infinitely many primes of the form $4x+1$. [Hint : For any group G, the order of an element of G divides the number of elements in G.]

4. Recall that $\phi(n)$ is the number of integers in $1, \ldots, n$ which are prime to n.

(a) Find all values of n such that $\phi(n)$ is odd.

(b) Prove that for any integer k, there are only finitely many n such that $\phi(n) = k$.

(c) Find all n so that $\phi(n) = 24$.

5. Suppose that $f(x)$ is a polynomial with integral coefficients. Assume that

$$f(a) \equiv 0 \mod p^j.$$

This problem is interested in lifting a to a zero of f modulo p^{j+1}. Hence we are looking for an integer t modulo p such that

$$f(a + tp^j) \equiv 0 \mod p^{j+1}. \tag{1}$$

(a) Use Taylor's expansion to show that

$$f(a + tp^j) \equiv f(a) + tp^j f'(a) \mod p^{j+1}.$$

Be careful as k does not necessarily divide ka/n.

(b) Assume that

$$f'(a) \not\equiv 0 \mod p.$$

Show that a solution to (1) is equivalent to a solution of

$$tf'(a) \equiv -\frac{f(a)}{p^j} \mod p.$$

Show that there is a unique lifting of a to a zero of f modulo p^{j+1}.

(c) Assume that

$$f'(a) \equiv 0 \mod p.$$

i. Show that if

$$f(a) \equiv 0 \mod p^{j+1}$$

then there are p liftings of a to zeros of f modulo p^{j+1}.

ii. Show that if

$$f(a) \not\equiv 0 \mod p^{j+1}$$

then there are no liftings of a to zeros of f modulo p^{j+1}.

6. Using problem 5, find all solutions to

$$\begin{aligned} x^2 + x + 47 &\equiv 0 \mod 7^3 \\ x^2 + x + 7 &\equiv 0 \mod 27 \end{aligned}$$