Math 40520 Theory of Number
Homework 5

Due Friday 10/5, in class

Do 5 of the following problems.

1. Let m and n be two positive integers.
   (a) If $m = nq+r$ is division with remainder show that as polynomials $X^m - 1 = (X^n - 1)Q(X) + X^r - 1$ is division with remainder.
   (b) Deduce that as polynomials $(X^m - 1, X^n - 1) = X^{(m,n)} - 1$.
2. Find all solutions of the equation $x^3 - x - 1 \equiv 0 \pmod{5^k}$ for $k = 1, 2, 3$.
3. Solve $x^{11} \equiv 7 \pmod{32}$. (You have two means of solving this: either primitive roots, or Hensel's lemma.)
4. Let $p > 3$ be a prime number. Find a solution in $\mathbb{Z}_{p^6}$ to the equation
$$x^3 \equiv 1 + p^2 \pmod{p^6}$$
5. Let $p > 2$ be a prime number and $k \geq 2$. Show that there exists a unique map $\omega : \mathbb{Z}_p^\times \to \mathbb{Z}_{p^k}^\times$ such that:
   (a) $\omega(a)^{p-1} \equiv 1 \pmod{p^k}$ for all $a \in \mathbb{Z}_p^\times$,
   (b) $\omega(a) \equiv a \pmod{p}$ for all $a \in \mathbb{Z}_p^\times$, and
   (c) $\omega(ab) = \omega(a)\omega(b)$ for all $a, b \in \mathbb{Z}_p^\times$.
6. Find all solutions of the congruence $x^3 + 4x^2 + 19x + 1 \equiv 0 \pmod{147}$. [Hint: $147 = 3 \cdot 7^2$.]
7. Show that the diophantine equation $13x^2 + 12y^2 = 1$ has no integral solutions but has solutions $\bmod n$ for all positive integers n.
8. Let $p > 2$ be a prime number and $k \geq 1$. Show that there exists a primitive root mod $2p^k$.