Course 311, Part I: Number Theory Problems Michaelmas Term 2005

1. Let x be an integer, and let p be a prime number. Suppose that $x^3 \equiv 1 \pmod{p}$. Prove that either $x \equiv 1 \pmod{p}$ or else $x^2 + x \equiv -1 \pmod{p}$.

2. Let x be a rational number. Suppose that x^n is an integer for some positive integer n. Explain why x must itself be an integer.

3. Find a function $f\colon \mathbb{Z}^3 \to \mathbb{Z}$ with the property that $f(x, y, z) \equiv x \pmod{3}$, $f(x, y, z) \equiv y \pmod{5}$ and $f(x, y, z) \equiv z \pmod{7}$ for all integers x, y, z.

4. Is 273 a quadratic residue or quadratic non-residue of 137?

5. Let p be a prime number. Prove that there exist integers x and y coprime to p satisfying $x^2 + y^2 \equiv 0 \pmod{p}$ if and only if $p \equiv 1 \pmod{4}$.

6. Let p be a odd prime number, and let g be a primitive root of p.

   (a) Let h is an integer satisfying $h \equiv g \pmod{p}$. Explain why the order of the congruence class of h modulo p^2 is either $p - 1$ or $p(p - 1)$. Hence or otherwise prove that h is a primitive root of p^2 if and only if $h^{p-1} \not\equiv 1 \pmod{p^2}$.

   (b) Use the result of (a) to prove that there exists a primitive root of p^2. (This primitive root will be of the form $g + kp$ for some integer k.)

   (c) Let x be an integer, and let m be a positive integer. Use the binomial theorem to prove that if $x \equiv 1 \pmod{p^m}$ and $x \not\equiv 1 \pmod{p^{m+1}}$ then $x^p \equiv 1 \pmod{p^{m+1}}$ and $x \not\equiv 1 \pmod{p^{m+2}}$

   (d) Use the results of previous parts of this question to show that any primitive root of p^2 is a primitive root of p^m for all $m \geq 2$. What does this tell you about the group of congruence classes modulo p^m of integers coprime to p?

   (e) Do the above results hold when $p = 2$ (i.e., when the prime number p is no longer required to be odd)?