MATH 498/812: Assignment 3

Due: 12 November 2012

---

1. Let p be a prime number. Show that $(\mathbb{Z}/p^a\mathbb{Z})^*$ has order $p^{a-1}(p-1)$.

2. Let p be an odd prime and g a generator of the group $(\mathbb{Z}/p\mathbb{Z})^*$. Show that g or $g+p$ is a generator of $(\mathbb{Z}/p^2\mathbb{Z})^*$.

3. Let p be an odd prime. Show by induction on a that $(\mathbb{Z}/p^a\mathbb{Z})^*$ is cyclic. [You may assume the result for $a = 1$, which was proved in class.]

4. Prove by induction that for $a \geq 3$,

$$5^{2^{a-3}} \equiv 1 + 2^{a-1} (\mathrm{mod}\, 2^a).$$

   Deduce that $5 \pmod{2^a}$ has order 2^{a-2} for $a \geq 3$.

5. Let $a \geq 3$. Let H be the multiplicative subgroup of $(\mathbb{Z}/2^a\mathbb{Z})^*$ generated by 5 (mod 2^a). Show that $-1 \notin H$. Deduce that every residue class (mod 2^a) can be written as $\pm 5^r$ for some r.

6. For each odd prime p, show that the congruence

$$x^2 \equiv 1 (\mathrm{mod}\, p^a)$$

   has precisely two solutions.

7. Show that the congruence

$$x^2 \equiv 1 (\mathrm{mod}\, 2^a)$$

   has precisely one solution if $a = 1$, two solutions if $a = 2$ and four solutions if $a \geq 3$.

8. Let q be a natural number and write $q = 2^r q_0$ with q_0 odd. Show that the congruence

$$x^2 \equiv 1 (\mathrm{mod}\, q)$$

   has exactly 2^{s+t} solutions where s is the number of distinct prime factors of q_0 and $t = 0, 1, 2$ according as $r \leq 1$, $r = 2$ or $r \geq 3$.

9. Let $d(n)$ be the number of divisors of n. Prove that $d(n)$ is a multiplicative function of n and show that for any natural number $r \geq 1$, the series

$$\sum_{n=1}^{\infty} \frac{d(n)^r}{n^s}$$

converges absolutely for $s > 1$. Deduce that for any $\epsilon > 0$, $d(n) = O(n^{\epsilon})$.

10. Let $f(x)$ be a polynomial of degree $k \geq 2$, with integer coefficients. Define

$$S_f(q, a) := \sum_{r=1}^{q} e(af(r)/q), \qquad e(t) = e^{2\pi i t}.$$

If $(q, r) = 1$, show that

$$S_f(qr, ar + bq) = S_f(q, a)S_f(r, b).$$