Topics in Number Theory - 3rd exercise sheet

Alex Bartel

October 28, 2012

These questions are not for credit, but nevertheless important. Please do them!

1. Prove by induction on the degree, or otherwise, that if p is a prime and $f = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ satisfies $p \nmid a_k$, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most k solutions modulo p.

2. (a) Use Euler's theorem to compute $2^{2012} \pmod{21}$.

   (b) Compute the order of 2^{2012} in $(\mathbb{Z}/17\mathbb{Z})^\times$ without determining the congruence class of 2^{2012} modulo 17.

3. (a) Show that

   $$\frac{p + (2k+1)}{2} \equiv -\left(\frac{p - (2k+1)}{2}\right) \pmod{p}$$

   for any integer $k \geq 0$ and odd prime p.

   (b) Deduce that

   $$\left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right)\cdots(p-1) \equiv (-1)^{(p-1)/2}\left(\frac{p-1}{2}\right)! \pmod{p}$$

   for any odd prime p.

   (c) Show that an integer $p \geq 2$ is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$. (Hint: pair up elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ with their inverses.)

   (d) Deduce the value of $((\frac{p-1}{2})!)^2$ modulo p for an odd prime p. What does this tell you about the values of some Legendre symbols?

4. (a) Show that if $n = ab$ with a and b coprime and both greater than 2, then there is no primitive root modulo n.

   (b) Show (e.g. by induction) than for $k \geq 3$, there is no primitive root modulo 2^k.

5. Let $n = (6t+1)(12t+1)(18t+1)$ with $t \in \mathbb{N}$ such that $6t+1, 12t+1, 18t+1$ are all prime numbers. Prove that

   $$a^{n-1} \equiv 1 \pmod{n},$$

   whenever $(a, n) = 1$. Find a t satisfying the conditions and hence deduce that the converse of Fermat's little theorem is false, i.e. that Fermat's little theorem cannot be used as a reliable primality test.

6. Let R be a complete set of quadratic residues, and N a complete set of quadratic non-residues modulo an odd prime p.

   (a) Show that
   $$\prod_{r \in R} r \equiv -\prod_{n \in N} n \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

   (b) Show that if $p > 3$, then
   $$\sum_{r \in R} r \equiv \sum_{n \in N} n \equiv 0 \pmod{p}.$$