18.781 Problem Set 6 - Fall 2008

Due Tuesday, Oct. 21 at 1:00

1. (Niven 2.8.7) If $p \geq 3$ is prime, how many solutions are there to $x^{p-1} \equiv 1 \pmod{p}$? How many solutions are there to $x^{p-1} \equiv 2 \pmod{p}$?

2. (Niven 2.8.8) Determine how many solutions there are to:

   (a) $x^{12} \equiv 16 \pmod{17}$

   (b) $x^{48} \equiv 9 \pmod{17}$

   (c) $x^{20} \equiv 13 \pmod{17}$

   (d) $x^{18} \equiv 11 \pmod{23}$.

3. (Niven 2.8.13 & 2.8.32) Show that $\{1^k, 2^k, \ldots, (p-1)^k\}$ is a reduced residue system modulo p iff $(k, p-1) = 1$.

(Bonus) Suppose that $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ is a reduced residue system modulo m. Show that $\{r_1^k, r_2^k, \ldots, r_{\phi(m)}^k\}$ is a reduced residue system if and only if $(k, \phi(m)) = 1$.

4. (Niven 2.8.14) Suppose that $e_p(a) = h$ and that $\overline{a}$ satisfies $a\,\overline{a} \equiv 1 \pmod{p}$. Show that $e_p(\overline{a}) = h$ as well. Furthermore, if $a \equiv g^i \pmod{p}$ for some primitive root g, show that $\overline{a} \equiv g^{p-1-i} \pmod{p}$.

5. (Niven 2.8.18) Show that if g and g' are both primitive roots modulo an odd prime p, then gg' is not a primitive root. (*Hint: Use the fact that $p-1$ is even.*)

6. Recall from PSet 5 that $g = 5$ is a primitive root modulo 23. Which number(s) of the form $5 + 23k$ (with $0 \leq k \leq 22$) is *not* a primitive root modulo 23^2?

7. Find a primitive root for the following moduli:

   (a) $m = 7^4$

   (b) $m = 11^3$

   (c) $m = 2 \cdot 13^2$.

8. Consider the sequence $9, 99, 999\ (= 3^3 \cdot 37), 9999\ (= 3^2 \cdot 11 \cdot 101), \ldots$. Prove that every prime $p \neq 2, 5$ appears as a factor of some term in this list.
   Hint: Note that $10^n - 1 = 99\ldots9$, with length n.

9. Consider the decimal expansions

   $1/7 = 0.\overline{142857}$
   $2/7 = 0.\overline{285714}$
   $3/7 = 0.\overline{428571}$

   $1/11 = 0.\overline{09}$
   $2/11 = 0.\overline{18}$
   $3/11 = 0.\overline{27}$

   $1/13 = 0.\overline{076923}$
   $2/13 = 0.\overline{153846}$
   $3/13 = 0.\overline{230769}$.

   Prove that for a prime $p \neq 2, 5$, the fraction a/p for $1 \leq a \leq p-1$ is repeating with period length $e_p(10)$.

10. (Niven 1.4.1 & 1.4.2) Use the binomial theorem to show that

(a) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ (b) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$

11. (Niven 2.6.3) Solve $x^3 + x + 57 \equiv 0 \pmod{5^3}$.