18.781 Solutions to 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 $x^{p-1} \equiv 2 \pmod{p}$?

   The first equivalence is known to hold for all $a \not\equiv 0 \pmod{p}$. This is an immediate consequence of Fermat's little theorem, by multiplying by the inverse of a, which exists $\bmod p$ as long as $a \not\equiv 0$. So there are $p-1$ solutions to $x^{p-1} \equiv 1 \pmod{p}$.

   The second equivalence, on the other hand, has no solutions. This is because by the above reasoning, every integer raised to the $p-1$ is either congruent to 1, for all coprime integers, or it is congruent to 0, if the integer was itself zero. Since we are assuming that $p \geq 3$, $p \neq 2$ so 2 is neither 0 nor 1, so the equivalence has no solutions.

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

   (a) Working in the modulus 17, the nonzero residues are generated by some element, g, of order 16. So we want to find the powers of g, say g^k, such that

   $$\left(g^i\right)^{12} \equiv 16 \pmod{17}.$$

   Since $e_{17}(g) = 16$, $g^8 \equiv -1 \equiv 16 \bmod 17$. So we want to find the i with $g^{12i} \equiv g^8$, which is only true if $e_{17}(g) | 12i - 8$, or $16 | 12i - 8$. This is a solvable congruence $\bmod 16$, which is satisfied for $i \equiv 2, 6, 10, 14 \pmod{16}$, so there are 4 solutions to the congruence.

   (b) Here, we are working in the same modulus, but we notice that $48 = 3 \cdot 16$, so $x^{48} \equiv (x^{16})^3 \equiv 1 \pmod{17}$. So there are no solutions to this equivalence.

   (c) Using the notation from the first part, we note that

   $$13^2 \equiv (-4)^2 \equiv 16 \equiv -1 \equiv g^8 \pmod{17}.$$

   So this implies that either $g^4 \equiv 13$ or $g^{12} \equiv 13$. Since substituting g^{-1} for g switches these two options, we can assume without loss of generality that our original choice of g has $g^4 \equiv 13$. So we want to find the $i \pmod{16}$ with

   $$\left(g^i\right)^2 0 \equiv g^4 \pmod{17}.$$

   Since the powers of g operate additively $\bmod 16$, this is equivalent to finding the i with

   $$20i \equiv 4 \pmod{16}.$$

   We can easily solve this, we get the solutions $i \equiv 1, 5, 9, 13 \pmod{16}$. So there are 4 solutions.

(d) By taking powers of 11, we can find that $11^2 \equiv 6 \pmod{23}$ and $11^{11} \equiv -1 \pmod{23}$. Since we know the order of 11 must divide $p-1 = 22$, these congruences imply that 11 is a primitive root for 23. So we can take $g = 11$, and we want to find an i such that

$$(g^i)^{18} \equiv g \pmod{23}$$

Now, we convert this to a congruence in the exponents $\bmod 22$:

$$18i \equiv 1 \pmod{22}.$$

We can immediately see that this has no solutions, because the greatest common divisor of 18 and 22 is 2, which doesn't divide 1. So the fourth congruence has no solutions.

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 $(k, p-1) = 1$.

We can solve this problem similarly to the way the last problem was solved, by using the power of a primitive root $\bmod p$. So let g be a primitive root for p. Then we want to know for what k is the list of k^{th} powers a reduced residue system modulo p. This is just asking for what k does $x^k \equiv b$ have a solution for *every* $b \not\equiv 0$.

So let's write b as g^i, and we want to determine if we can always find some x which we can write as g^j such that $\left(g^j\right)^k \equiv g^i \pmod{p}$. Exactly as above, we can rewrite this as a congruence on the exponents $\bmod (p-1)$:

$$jk \equiv i \pmod{(p-1)}.$$

So we want to know, for what k is this congruence always solvable for j? And from our knowledge of modular arithmetic, we know that there is a solution exactly when $(k, p-1) = 1$, because then k is invertible $\bmod p$.

(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 $\overline{a} \equiv g^{p-1-i} \pmod{p}$.

The first statement comes from the following relation:

$$1 \equiv a\,\overline{a} \equiv (a\,\overline{a})^k \equiv a^k \overline{a}^k \pmod{p}.$$

Therefore $a^k \equiv 1$ *exactly* when $\overline{a}^k \equiv 1$, so they have equal orders.

Now we let $a \equiv g^i \pmod{p}$. Since we know g is a primitive root, we have that $g^j \equiv \overline{a} \pmod{p}$ for some $1 \leq j \leq p-1$. But

$$1 \equiv a\,\overline{a} \equiv g^i g^j \equiv g^{i+j} \pmod{p}.$$

Since the order of g is $p-1$, we have that $(p-1)|(i+j)$, and from the inequalities of i and j, we have that $i + j = p - 1$, or $j = p - 1 - i$, and we are done.

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.*)

   We know that $p-1$ is even, and it is the order of both g and g'. So this implies that

   $$g^{\frac{p-1}{2}} \equiv {g'}^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

   The reason this follows is we know these two powers of generators cannot be 1, by their orders, but must square to 1, so we get that they must be -1. So then we have that

   $$(gg')^{\frac{p-1}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)\left({g'}^{\frac{p-1}{2}}\right) \equiv -1 \cdot -1 \equiv 1.$$

   Therefore the order of gg' is at most $\frac{p-1}{2} < p-1$, so gg' is not a primitive root.

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?

   We are given 5 as a primitive root of 23. Then from work in class, we know numbers of the form $5 + 23k$ are primitive roots of $23^2 = 529$ unless $k \equiv \dfrac{5^{23} - 5}{23} \pmod{23}$. We calculate that $5^{23} \equiv 28 \pmod{529}$. This implies that $5 + 23k$ is not a primitive root modulo 529, for $0 \leq k \leq 22$ only when

   $$k = \frac{28 - 5}{23} = 1.$$

7. Find a primitive root for the following moduli:

   (a) $m = 7^4$
   (b) $m = 11^3$
   (c) $m = 2 \cdot 13^2$.

   (a) By inspection, 3 is a primitive root for 7. Then by the formula above, the only number of the form $3 + 7k$ that is a primitive root for $7^2 = 49$ is when $k = 4$, so in particular 3 is still a primitive root for 49. Then we move up to $7^4 = 2401$. Once you get to the third power of an odd prime modulus, any number that was a primitive root for p^2 will still be a primitive root for p^i for $i > 2$. This is because we know that the unit group has a primitive root, and then number of such roots is

   $$\begin{aligned}\phi(\phi(p^i)) &= \phi(p^{i-1}(p-1)) = \phi(p^{i-1})\phi(p-1) = p^{i-2}(p-1)\phi(p-1) \\ &= p \cdot p^{i-2}(p-1)\phi(p-1) = p \cdot \phi(\phi(p^{i-1})).\end{aligned}$$

   So the number of primitive roots is multiplied by p as we change the mod from p^{i-1} to p^i, so every primitive root must stay a primitive root. Therefore 3 is a primitive root for 7^4.

   (b) For 11, we find that 2 is a primitive root. Then moving up to $11^2 = 121$, the k for which $2 + 11k$ is not a primitive root is

   $$k \equiv \frac{2^{11} - 2}{11} \equiv 186 \equiv 10 \pmod{11}.$$

   So in particular, 2 remains a primitive root for 11^2. Then by the logic above it is also a primitive root for 11^3.

(c) For a number to be a primitive root mod $2 \cdot 13^2$, it must be a primitive root for 13^2 and also be odd. Then its order mod 13^2 is $\phi(13^2)$, so this is a lower bound for its order mod $2 \cdot 13^2$, but since $\phi(2 \cdot 13^2) = \phi(13^2)$, this implies it is a primitive root for $2 \cdot 13^2$. So we find a primitive root for 13^2.

The first step is to find a root for 13, 2 suffices upon inspection. So then we move to $13^2 = 169$. We calculate the k for which $2 + 13k$ fails to be a primitive root, it is

$$k \equiv \frac{2^{13} - 2}{13} \equiv 6 \pmod{13}.$$

So in particular, 2 is still a primitive root mod 169. But we want an odd primitive root. This is easily solved: we can just take $2 + 169 = 171$. Then this is an odd primitive root mod 169, so it is a primitive root mod $2 \cdot 169 = 338$. So 171 is our answer.

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*.*

The sequence is written in a rather awkward way, we rewrite the terms using the hint as $a_n = 10^n - 1$. So given a prime p, we want to show that for some n, $p|a_n$. Well,

$$p|a_n \Leftrightarrow p|(10^n - 1) \Leftrightarrow 10^n \equiv 1 \pmod{p}.$$

So we have reduced it to showing that some power of 10 is congruent to 1 mod p. Since p is assumed to not divide 10, 10 must have an order mod p, and this power of 10 will be congruent to 1 mod p. So we are done.

9. Consider the decimal expansions

$1/7 = 0.\overline{142857}$	$1/11 = 0.\overline{09}$	$1/13 = 0.\overline{076923}$
$2/7 = 0.\overline{285714}$	$2/11 = 0.\overline{18}$	$2/13 = 0.\overline{153846}$
$3/7 = 0.\overline{428571}$	$3/11 = 0.\overline{27}$	$3/13 = 0.\overline{230769}$.

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 $e_p(10)$.

The trick to this problem is to delve into the algorithm that generates the decimal expansions of fractions, namely, long division. We can rewrite the division that calculates the decimal expansion of $\frac{1}{7}$ in the following way:

$$\begin{aligned} 1 &= 7 \cdot 0 + 1 \\ 10 &= 7 \cdot 1 + 3 \\ 30 &= 7 \cdot 4 + 2 \\ 20 &= 7 \cdot 2 + 6 \\ 60 &= 7 \cdot 8 + 4 \\ 40 &= 7 \cdot 5 + 5 \\ 50 &= 7 \cdot 7 + 1 \\ 10 &= 7 \cdot 1 + 3 \end{aligned}$$

So we begin by performing our fraction division in the integers, and the quotient is the integer part of the decimal (in the above case, this is 0). Then, from each step, to get the next decimal place, we take the previous remainder, multiply it by 10, and then divide by our denominator, 7. The quotient is the next decimal place, and we get a new remainder.

The process repeats as soon as our original remainder is achieved a second time. But if we look at the above equations mod 7, the $7 \cdot q$ part all drops out, and we just have the next remainder in the algorithm is congruent to 10 times the previous remainder, mod 7. So, by a quick induction argument, the nth remainder is congruent to 10^n times the "zeroth" remainder. So the remainder repeats exactly when $10^n \equiv 1 \pmod 7$, so for $n = e_7(10)$. This argument is easily generalizable, so the length of the repeating part of a decimal with denominator p is always $e_p(10)$.

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

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

(a) Well, the binomial theorem states that, for integers x, y, n,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

So setting $x = y = 1$, we obtain

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

But the left hand side is obviously just 2^n.

(b) Here we can set $x = 1$, $y = -1$. We get

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

Once again, the left hand side is easily computable, this time it is 0.

11. (Niven 2.7.3) Solve $x^3 + x + 57 \equiv 0 \pmod{5^3}$.

We solve this problem by solving mod 5 and then mod 5^2. First, mod 5 we only have to seach for a solution to $x^3 + x + 2 \equiv 0 \pmod 5$ by checking the value of the equation at $0, 1, 2, 3$, and 4. We find that the only solution is 4, or -1. Then a solution mod $5^2 = 25$ must be of the form $-1 + 5k$. So once again we only have to check if $x^3 + x + 7 \equiv 0 \pmod{25}$ for five numbers, say $-6, -1, 4, 9$ and 14. It holds for 4, and none of the others. So now we only need to check $4, 29, 54, 79, 104$ for the polynomial mod 125. But in fact we immediately find that 4 again is a solution. So we can then factor the cubic mod 125:

$$x^3 + x + 57 \equiv (x-4)(x^2 + 4x + 17) \pmod{125}.$$

Then we check and find that the quadratic factor has no solutions mod 5, so the original polynomial has no solutions mod 125 other than 4.