Math 228: Solutions for Problem Set Twelve

Isaac Levy – ilevy.web.wesleyan.edu

April 13, 2007

1. **Page 133 number 6**

   (c) In mod 6, $17123 \equiv 5 \equiv -1$. So $(17123)^{50} \equiv (-1)^{50} = 1$.

   (d) In mod 7, $10 \equiv 3$. So $10^4 \equiv (3^2)^2 = 9^2 \equiv 2^2 = 4$.

   i. $10^4 \equiv 4$.
   ii. $10^8 = (10^4)^2 \equiv 4^2 = 16 \equiv 2$
   iii. $10^{12} = 10^8 \cdot 10^4 \equiv 2 \cdot 4 = 8 \equiv 1$
   iv. $10^{20} = 10^8 \cdot 10^{12} \equiv 2 \cdot 1 = 2$
   v. $10^{24} = (10^{12})^2 \equiv 1^2 = 1$

   (f) i. $4 \equiv 4 \pmod{11}$
   ii. $4^2 = 16 \equiv 5$
   iii. $4^3 = 64 \equiv 9$
   iv. $4^4 = (4^2)^2 \equiv (5)^2 = 25 \equiv 3$
   v. $4^5 = 4 \cdot 4^4 \equiv 4 \cdot 3 = 12 \equiv 1$
   vi. $4^6 = 4 \cdot 4^5 \equiv 4 \cdot 1 = 4$
   vii. $4^7 = 4^2 \cdot 4^5 \equiv 5 \cdot 1 = 5$
   viii. $4^8 = 4^3 \cdot 4^5 \equiv 9 \cdot 1 = 9$
   ix. $4^9 = 4^4 \cdot 4^5 \equiv 3 \cdot 1 = 3$
   x. $4^{10} = (4^5)^2 \equiv 1^2 = 1$

2. **Page 133 number 9**

   (b) $4 \cdot x \equiv 2 \pmod{6} \implies 2 \cdot x \equiv 1 \pmod{3}$
   $2 \cdot 2 \equiv 1 \pmod{3}$ so if we multiply by 2 on both sides:
   $2 \cdot 2 \cdot x \equiv 2 \cdot 1 \implies x \equiv 2 \pmod{3}$.
   Thus $x = \{2, 5\}$

(c) To solve this we need to find the inverse of 4 in modulo 7. Using the Euclidean Algorithm,

$$7 = 1 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$

So $1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7$. In modulo 7, $2 \cdot 4 - 7 = 1$ simplifies to $2 \cdot 4 \equiv 1$. Thus 2 is the inverse of 4 modulo 7.

$4 \cdot x \equiv 3 \implies 2 \cdot 4 \cdot x \equiv 2 \cdot 3 \implies x \equiv 6$. So $x = 6$.

(d) There are no solutions. Because $gcd(4, 6) = 2$ and $2 \nmid 3$, there cannot be values of x which are congruent to 3. Intuitively, we are looking for values of x such that $4 \cdot x - 3 = 6k$ for some k. However the left side of the equation is always odd, so it can never be a multiple of 6.

3. **Page 134 number 11**

(d) Because $gcd(2, 15) = 1$ we can multiply the equations by two without losing solutions. If we multiply the first equation by 2, and then subtract:

$$14x + 4y \equiv 6$$
$$9x + 4y \equiv 6$$
$$\Rightarrow 5x \equiv 0 \pmod{15}$$

$5 \mid 15$ so we can divide both sides by 5: $x \equiv 0 \pmod 3$. So x is a multiple of 3 and in modulo 15, $x = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$.

i. If $x \equiv 0$, then $2y \equiv 3 \equiv 18 \implies y \equiv 9 \pmod{15}$.
ii. If $x \equiv 3$, then $27 + 4y \equiv 6 \implies 4y \equiv -21 \equiv 24$. So $y \equiv 6$.
iii. If $x \equiv 6$, then $54 + 4y \equiv 6 \implies 4y \equiv -48 \equiv 12$. So then $y \equiv 3$.
iv. If $x \equiv 9$, then $81 + 4y \equiv 6 \implies 4y \equiv -75 \equiv 0$. So $y \equiv 0$.
v. Finally, if $x \equiv 12$ then $108 + 4y \equiv 6 \implies 4y \equiv 6 - 3 = 3$. Since $4 \cdot 4 \equiv 1 \pmod{15}$, $y \equiv 12$.

Thus $(x, y) = \{(0, 9), (3, 6), (6, 3), (9, 0), (12, 12)\}$.

(e) We can multiply the equations by any number relatively prime to 28. In particular, we can multiply the first equation by 5 and the second equation by 3, to get $15x + 25y \equiv 70$ and $15x + 27y \equiv 18$. So then $-2y \equiv 52 \pmod{28}$. Since $2 \mid 28$, we can divide by 2 on both sides as long as we divide the modulo number. So $y \equiv -26 \pmod{14}$. So modulo 14, $y = \overline{2}$. In modulo 28, $y = \{\overline{2}, \overline{16}\}$.

i. If $y \equiv 2$ then $3x + 10 \equiv 14 \implies 3x \equiv 4$. Using the Euclidean Algorithm, we can find that $19 \cdot 3 \equiv 1 \pmod{28}$.
So $x \equiv 19 \cdot 4 \equiv 20$.

ii. If $y \equiv 16$ then $3x + 80 \equiv 14 \implies 3x \equiv -66 \equiv 18$. We already know 19 is the inverse of 3 from part (i), so $x \equiv 18 \cdot 19 = 342$.
So $x \equiv 6$.

Thus $(x, y) = \{(20, 2), (6, 16)\}$.

4. **Page 134 number 16**
We can expand any n-digit integer x into a summation of terms:

$$x = \sum_{i=0}^{n-1} 10^i \cdot a_i$$

. We know that $10 \equiv -1 \pmod{11}$. So

$$\sum_{i=0}^{n-1} 10^i \cdot a_i \equiv \sum_{i=0}^{n-1} (-1)^i \cdot a_i$$

If i is even, then the term is multiplied by 1, otherwise it is multiplied by negative one. So in modulo 11,

$$x \equiv (a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots)$$

If $x \equiv 0 \pmod{11}$, then

$$(a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) \equiv 0 \quad \implies \quad a_0 + a_2 + \ldots \equiv a_1 + a_3 + \ldots$$

On the other hand, if $a_0 + a_2 + \ldots \equiv a_1 + a_3 + \ldots$, then
$(a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) \equiv 0$. Hence x is divisible by 11.

5. **Page 134 number 20**

(a) Using a calculator to find the solutions:

i. $x^2 \equiv 1 \pmod{2^1}$: $x = \{1\}$

ii. $x^2 \equiv 1 \pmod{2^2}$: $x = \{1, 3\}$

iii. $x^2 \equiv 1 \pmod{2^3}$: $x = \{1, 3, 5, 7\}$

iv. $x^2 \equiv 1 \pmod{2^4}$: $x = \{1, 7, 9, 15\}$

(b) $x^2 \equiv 1 \implies x^2 - 1 \equiv 0 \implies (x - 1)(x + 1) \equiv 0$.
The two factor's product must be divisible by 2^k for some $k \geq 3$. Since $k \geq 3$, one of the terms must contain at least 2 factors of 2.

i. Suppose $x-1$ contains a factor of 2^l for some $l \geq 2$. Then $x-1 = 2^l \cdot j$. So $x+1 = 2^l \cdot j + 2 = 2(2^{l-1} \cdot j + 1)$. But $l-1 \geq 1$, so $2^{l-1} \cdot j + 1$ is odd. Thus x+1 contains exactly one factor of 2. So then $x-1$ must contain $k-1$ factors of 2. Hence, $2^{k-1} \mid x-1$. So $x-1 = \{2^{k-1}, 2^k\}$. So $x = \{2^{k-1}+1, 2^k+1\} \equiv \{2^{k-1}+1, 1\}$.

ii. On the other hand, suppose $x+1$ contains a factor of 2^l for some $l \geq 2$. Then $x+1 = 2^l \cdot j$. So $x-1 = 2^l \cdot j - 2 = 2(2^{l-1} \cdot j - 1)$. But $l-1 \geq 1$, so $2^{l-1} \cdot j - 1$ is odd. Thus x-1 contains exactly one factor of 2. So then $x+1$ must contain $k-1$ factors of 2. Hence, $2^{k-1} \mid x+1$. So $x+1 = \{2^{k-1}, 2^k\}$. So $x = \{2^{k-1}-1, 2^k-1\}$.

Hence the total possible solutions are

$$x = \{2^k - 1, 2^{k-1} + 1, 2^{k-1} - 1, 1\}$$

One can (and should) verify that these are, indeed, solutions for all $k \geq 3$. For example,

$$(2^{k-1}+1)^2 = (2^{k-1})^2 + 2 \cdot 2^{k-1} + 1 = 2^{2k-2} + 2^k + 1 \equiv 1 \pmod{2^k}$$

We have already solved the problem for $k < 3$ and the solutions are also of the same form.