115 Homework 5

Due Friday November 5

Question 1 (Rosen 4.1.3) For which $m \in \mathbb{N}$ are the following true

(a) $27 \equiv 5 \text{ mod } m$

(b) $1000 \equiv 1 \text{ mod } m$

(c) $1331 \equiv 0 \text{ mod } m$

Why?

Solution (a) Since the positive divisors of $27-5=22$ are 1,2,11, and 22 it follows that $27 \equiv 5 \pmod{m}$ iff $m=1, m=2, m=11$, or $m=22$.

(b) Since the positive divisors of $1000-1=999$ are 1,3,9,27,37,111,333, and 999 it follows that $1000 \equiv 1 \pmod{m}$ iff $m=1, m=3, m=9, m=27, m=37, m=111, m=333$, or $m=999$.

(c) Since the positive divisors of $1331-0=1331$ are 1,11,121, and 1331 it follows that $1331 \equiv 0 \pmod{m}$ iff $m=1, m=11, m=121$, or $m=1331$.

Question 2 Compute 5^{127} mod 7. Express your answer as the least positive residue and show your working.

Solution First note that $127 = 128-1 = 2^7-1 = 2^0+2^1+2^2+2^3+2^4+2^5+2^6$ so that we can write $5^{127} = 5^{2^0+2^1+2^2+2^3+2^4+2^5+2^6} = 5^{2^0}5^{2^1}5^{2^2}5^{2^3}5^{2^4}5^{2^5}5^{2^6}$. Secondly, note that $5^{2^i} = 5^{2\cdot 2^{i-1}} = (5^{2^{i-1}})^2$. Now we will calculate all the residues of 5^{2^i} (mod 7) for $i = 0, 1, \ldots, 6$:
$5^{2^0} \equiv 5$ (mod 7)
$5^{2^1} \equiv 4$ (mod 7)
$5^{2^2} \equiv (5^{2^1})^2 \equiv 4^2 \equiv 2$ (mod 7)
$5^{2^3} \equiv (5^{2^2})^2 \equiv 2^2 \equiv 4$ (mod 7)
$5^{2^4} \equiv (5^{2^3})^2 \equiv 4^2 \equiv 2$ (mod 7)
$5^{2^5} \equiv (5^{2^4})^2 \equiv 2^2 \equiv 4$ (mod 7)
$5^{2^6} \equiv (5^{2^5})^2 \equiv 4^2 \equiv 2$ (mod 7)
So now we can write $5^{2^0}5^{2^1}5^{2^2}5^{2^3}5^{2^4}5^{2^5}5^{2^6} \equiv 5 \cdot 4 \cdot 2 \cdot 4 \cdot 2 \cdot 4 \cdot 2 \cdot \equiv 5 \cdot 1^3 \equiv 5$ (mod 7). Thus $5^{127} \equiv 5$ (mod 7).

Question 3 (Rosen 4.1.22) Use induction to show $4^n \equiv 1+3n \pmod 9$ for $n \in \mathbb{N}$.

Solution When $n = 1$ we have $4^1 = 4 = 1 + 3 \cdot 1$ so the basis step holds. Now suppose that $4^n \equiv 1 + 3n \pmod 9$. Then $4^{n+1} = 4 \cdot 4^n \equiv 4(1 + 3n) \equiv 4 + 12n \equiv 4 + 3n \equiv 1 + 3(n + 1) \pmod 9$. This completes the proof by mathematical induction.

Question 4 (Rosen 4.1.38) Coconuts! 5 shipwrecked men and 1 monkey collect a big pile of coconuts which they plan to divide equally the next morning. However, during the night, each man in turn wakes up, divides the pile in 5 equal parts with one leftover coconut which he gives to the monkey and then steals one of the 5 parts. In the morning, the 5 sleepy men divide the remaining coconuts into 5 equal piles and again 1 coconut remains for the monkey. What is the minimum possible number of coconuts in the original pile?

Solution Let N be the number of coconuts. From the dvision of the coconuts by the first man, gving one to the monkey, we see that $N \equiv 1 \pmod 5$, so that $N = 5k_0 + 1$ for some positive integer k_0.
The division of the coconuts by the second man, giving one to the monkey, we see that $N_1 = (4/5)(N-1) = 4k_0 \equiv 1 \pmod 5$, so that $k_0 \equiv 4 \pmod 5$, $k_0 = 5k_1+4$, or equivalently, that $N = 5(5k_1 + 4) + 1 = 25k_1 + 21$, and $N_1 = 20k_1 + 16$, for some positive integer k_1.
The division of the coconuts by the third man, giving one to the monkey, shows that $N_2 = (4/5)(N_1 - 1) = (4/5)(20k_1 + 15) = 16k_1 + 12 \equiv 1 \pmod 5$, so that $k_1 \equiv 4 \pmod 5$, $k_1 = 5k_2 + 4$, or equivalently, that $N = 25(5k_2 + 4) + 21 = 125k_2 + 121$, and $N_2 = (4/5)(100k_2 + 95) = 80k_2 + 76$ for some positive integer k_2.
The division of the coconuts by the fourth man, giving one to the monkey, shows that $N_3 = (4/5)(N_2 - 1) = (4/5)(80k_2 + 75) = 64k_2 + 60 \equiv 1 \pmod 5$, so that $k_2 \equiv 4 \pmod 5$, $k_2 = 5k_3 + 4$, or equivalently, that $N = 125(5k_3 + 4) + 121 = 625k_3 + 621$, and $N_3 = 64(5k_3 + 4) + 60 = 320k_3 + 316$ for some positive integer k_3.
The division of the coconuts by the fifth man, giving one to the monkey, shows that $N_4 = (4/5)(N_3 - 1) = (4/5)(320k_3 + 315) = 256k_3 + 252 \equiv 1 \pmod 5$, so that $k_3 \equiv 4 \pmod 5$, $k_3 = 5k_4+4$, or equivalently, that $N = 625(5k_4+4)+621 = 3125k_4 + 3121$, and $N_4 = 256(5k_4 + 4) + 252 = 1280k_4 + 1276$ for some positive integer k_4.
The last division of the coconuts into five equal piles, giving the left ofer one

to the monkey, shows that $N_5 = (4/5)(N_4 - 1) = (4/5)(1280k_4 + 1275) = 1024k_4 + 1020 \equiv 1$ (mod 5), so that $k_4 \equiv 4$ (mod 5), $k_4 = 5k_5 + 4$, or equivalently, that $N = 3125(5k_5 + 4) + 3121 = 15625k_5 + 15621, for some integer k_5$. The least number of coconuts is given by the smallest positive integer of the form $15625k_5 + 15621$, which is 15621 with $k_5 = 0$.

Question 5 (Rosen 4.2.2abc) Find all solutions to the linear congruences

(a) $3x \equiv 2$ mod 7

(b) $6x \equiv 3$ mod 9

(c) $17x \equiv 14$ mod 21

Solution (a) Suppose that $3x \equiv 2$ (mod 7). Since $(3, 2) = 1$, by Theorem 4.10 there is a unique solution modulo 7 to this congruence. To solve $3x \equiv 2$ (mod 7) first translate this to the equation $3x - 7y = 2, y \in \mathbb{Z}$. Using the Euclidean algorithm we find that $-2 \cdot 3 + 1 \cdot 7 = 1$. Multiplying both sides by 2 gives $-4 \cdot 3 + 2 \cdot 7 = 2$. This implies that $x \equiv -4 \equiv 3$ (mod 7).

(b) Suppose that $6x \equiv 3$ (mod 9). Since $(6, 3) = 3$, by Theorem 4.10 there are exactly 3 incongruent solutions modulo 9. To find these solutions, we first translate this congruence into the linear diophantine equation $6x - 9y = 3, y \in \mathbb{Z}$. Using the Euclidean algorithm we find that $-1 \cdot 6 + 1 \cdot 9 = 3$. Hence all solutions of $6x - 9y = 3$ are given by $x = -1 + (9/3)t - -1 + 3t, y = -1 - (6/3)t = -1 - 2t$. We obtain three incongruent solutions modulo 9 by taking the values of x for $t = 0, 1, 2$. We obtain $x = -1 \equiv 8$ (mod 9), $x = -4 \equiv 5$ (mod 9), and $x = -7 \equiv 2$ (mod 9).

(c) Suppose that $17x \equiv 14$ (mod 21). Since $(17, 14) = 1$, by Theorem 4.10 there is a unique solution modulo 21 to this congruence. To solve $17x \equiv 14$ (mod 21) first translate this to the linear diophantine equation $17x - 21y = 14, y \in \mathbb{Z}$. Using the Euclidean algorithm we find that $5 \cdot 17 - 4 \cdot 21 = 1$. Multiplying both sides by 14 gives $70 \cdot 17 - 56 \cdot 21 = 14$. Hence $x = 70, y = 56$ is a soltion. This implies that the unique solution modulo 21 is $x = 70 \equiv 7$ (mod 21).

Question 6 (Rosen 4.2.12) Show that if a' and b' are inverses of a and b modulo m, respectively, then $a'b'$ is an inverse of ab modulo m.

Solution Suppose that a' and b' are inverses of a and b modulo m, respectively. Then $a \cdot a' \equiv 1 \pmod{m}$ We see that $(a \cdot b)(a' \cdot b') = (aa')(bb') \equiv 1 \cdot 1 \equiv 1 \pmod{m}$. It follows that $a'b'$ is an inverse of ab modulo m.