# 115 Homework 6 Solutions

Due Friday November 12

**Question 1** (Rosen 4.2.10) Find all integers $1 \leq a \leq 14$ which have an inverse modulo 14 and compute it when it exists.

**Solution** The integers $a$ with inverses modulo 14 are exactly those that are relatively prime to 14. Therefore, 1,3,5,9,11, and 13 all have inverses modulo 14. For each of these integers $a$, relatively prime to 14, we must solve the congruence $ax \equiv 1$ (mod 14) to find each $a$'s inverse modulo 14. We have that 1 and $13 \equiv -1$ (mod 14) are both their own inverses. The solution to $3x \equiv 1$ (mod 14) is $x = 5$, so that $3^{-1} = 5$. Note then that $5^{-1} = 3$. Likewise, $-3 \equiv 11$ and $-5 \equiv 9$ (mod 14) are inverses of each other modulo 14.

**Question 2** (Rosen 4.3.4d) Solve the system of congruences $x \equiv 2$ mod 11, $x \equiv 3$ mod 12, $x \equiv 4$ mod 13, $x \equiv 5$ mod 17 and $x \equiv 6$ mod 19.

**Solution** Using the Chinese remainder theorem, we have $M = 11 \cdot 12 \cdot 13 \cdot 17 \cdot 19 = 554268, M_1 = M/11 = 50388, M_2 = M/12 = 46189, M_3 = M/13 = 42636, M_4 = M/17 = 32604, M_5 = M/19 = 29172$. To determine $y_1$ we must solve $M_1 y_1 = 50388 y_1 \equiv 1$ (mod 11), or equivalently $(50388 - 4580 \cdot 11) y_1 \equiv 8 y_1 \equiv 1$ (mod 11), which yields $y_1 = 7$. To determine $y_2$ we must solve $M_2 y_2 = 46189 y_2 \equiv 1$ (mod 12), or equivalently $(46189 - 3849 \cdot 12) y_2 \equiv y_2 \equiv 1$ (mod 12), which yields $y_2 = 1$. To determine $y_3$ we must solve $M_3 y_3 = 42636 y_3 \equiv 1$ (mod 13), or equivalently $(42636 - 3279 \cdot 13) y_3 \equiv 9 y_3 \equiv 1$ (mod 13), which yields $y_3 = 3$. To determine $y_4$ we must solve $M_4 y_4 = 32604 y_4 \equiv 1$ (mod 17), or equivalently $(32604 - 3279 \cdot 17) y_4 \equiv 15 y_4 \equiv 1$ (mod 17), which yields $y_4 = 8$. Finally, to determine $y_5$ we must solve $M_5 y_5 = 29172 y_5 \equiv 1$ (mod 19), or equivalently $(29172 - 1535 \cdot 19) y_5 \equiv 7 y_5 \equiv 1$ (mod 19), which yields $y_5 = 11$. Thus we have that

$$x = 2 \cdot M_1 \cdot 7 + 3 \cdot M_2 \cdot 1 + 4 \cdot M_3 \cdot 3 + 5 \cdot M_4 \cdot 8 + 6 \cdot M_5 \cdot 11 = 4584153 \equiv 150999$$

modulo M.

**Question 3** (Rosen 4.3.12) Ancient Indian eggs are removed from a basket, 2,3,4,5 and 6 at a time and there remains, respectively 1,2,3,4 and 5 eggs. But if the eggs are removed 7 at a time, none remain at the end. What is the smallest number of eggs that could have been in the basket?

**Solution** Let's rewrite the problem in a more mathematical way. Letting $x$ be the total number of eggs we want to solve the following system of equations: $x \equiv 1$ (mod 2), $x \equiv 2$ (mod 3), $x \equiv 3$ (mod 4), $x \equiv 4$ (mod 5), $x \equiv 5$ (mod 6), $x \equiv 0$ (mod 7), but the moduli are not pairwise relatively prime. Note that if $x \equiv 5$ (mod 6) then it satisfies the congruences $x \equiv 1$ (mod 2) and $x \equiv 2$ (mod 3) so that we can eliminate the congruence $x \equiv 5$ (mod 6) from our system. Now we are left with 5 congruences, but two of the moduli, namely 2 and 4, are still not relatively prime. Let us examine the system of congruences without the congruence modulo 2. So our system looks like: $x \equiv 2$ (mod 3), $x \equiv 3$ (mod 4), $x \equiv 4$ (mod 5), $x \equiv 0$ (mod 7), and now we can use the Chinese remainder theorem since we have a system where all the moduli are pairwise relatively prime. So we have $M = 3 \cdot 4 \cdot 5 \cdot 7 = 420, M_1 = M/3 = 140, M_2 = M/4 = 105, M_3 = M/5 = 84, M_4 = M/7 = 60$. To determine $y_1$ we must solve $M_1 y_1 = 140 y_1 \equiv 1$ (mod 3), or equivalently $2y_1 \equiv 1$ (mod 3), which yields $y_1 = 2$. To determine $y_2$ we must solve $M_2 y_2 = 105 y_2 \equiv 1$ (mod 4), or equivalently $y_2 \equiv 1$ (mod 4), which yields $y_2 = 1$. To determine $y_3$ we must solve $M_3 y_3 = 84 y_3 \equiv 1$ (mod 5), or equivalently $4y_3 \equiv 1$ (mod 5), which yields $y_3 = 4$. To determine $y_4$ we must solve $M_4 y_4 = 60 y_4 \equiv 1$ (mod 7), or equivalently $4y_4 \equiv 1$ (mod 7), which yields $y_4 = 2$. Thus we have that

$$x = 2 \cdot M_1 \cdot 2 + 3 \cdot M_2 \cdot 1 + 4 \cdot M_3 \cdot 4 + 0 \cdot M_4 \cdot 2 = 2219 \equiv 119$$

modulo M. Note now that $x = 119$ also solves the first congruence since $119 \equiv 1$ (mod 2), which concludes the problem.

**Question 4** (Rosen 6.1.2) Show $12! + 1$ is divisible by 13 by grouping pairwise inverses modulo 13 appearing in 12!.

**Solution** Note that $12! + 1 = (1)(2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11)(12) + 1 \equiv (1)(1)(1)(1)(1)(1)(-1) + 1 \equiv 0$ (mod 13). Therefore $13 | (12! + 1)$.