Math 25: Solutions to Homework # 4

(4.3 # 10) Find an integer that leaves a remainder of 9 when it is divided by either 10 or 11, but that is divisible by 13.

We use the Chinese Remainder Theorem to solve the system of congruences

$$\begin{aligned} x &\equiv 9 \pmod{10} \\ x &\equiv 9 \pmod{11} \\ x &\equiv 0 \pmod{13}. \end{aligned}$$

There is a unique solution modulo $10 \cdot 11 \cdot 13 = 1430$. Let $M_1 = 11 \cdot 13 = 143$, $M_2 = 10 \cdot 13 = 130$, and $M_3 = 10 \cdot 11 = 110$. Then the solution is

$$x \equiv 9M_1y_1 + 9M_2y_2 + 0M_3, y_3 \pmod{1430}$$

where

$$\begin{aligned} 143y_1 &\equiv 1 \pmod{10} \\ 130y_2 &\equiv 1 \pmod{11} \\ 110y_3 &\equiv 1 \pmod{13}. \end{aligned}$$

Then $3y_1 \equiv 1 \pmod{10}$, so $y_1 \equiv 7 \pmod{10}$, and $9y_2 \equiv 1 \pmod{11}$, so $y_2 \equiv 5 \pmod{11}$. We don't need to find y_3 since the third term in the sum is zero. Then

$$x \equiv 9 \cdot 143 \cdot 7 + 9 \cdot 130 \cdot 5 \equiv 559 \pmod{1430}$$

so 559 is a particular solution.

(4.6 # 2(b)) Use the Pollard rho method to factor the integer 1387, with $x_0 = 3$ and $f(x) = x^2 + 1$.

Iterating the formula $x_{j+1} \equiv x_j^2 + 1 \pmod{1387}$, we have the sequence $x_0 = 3$, $x_1 = 10$, $x_2 = 101$, $x_3 = 493$, $x_4 = 325$, $x_5 = 214$, $x_6 = 26$, $x_7 = 677$, $x_8 = 620$, $x_9 = 202$, $x_{10} = 582$, $x_{11} = 297$, $x_{12} = 829$. Then

$$\begin{aligned} (x_2 - x_1, 1387) &= (91, 1387) = 1 \\ (x_4 - x_4, 1387) &= (224, 1387) = 1 \\ (x_6 - x_3, 1387) &= (467, 1387) = 1 \\ (x_8 - x_4, 1387) &= (295, 1387) = 1 \\ (x_{10} - x_5, 1387) &= (368, 1387) = 1 \\ (x_{12} - x_6, 1387) &= (803, 1387) = 73. \end{aligned}$$

Therefore $1387 = 73 \cdot 19$.

(5.1 # 22) An old receipt has faded. It reads 88 chickens at a total cost of \$$x4.2y$, where x and y are unreadable digits. How much did each chicken cost?

The total cost was $x42y$ cents. If 88 divides this number, then both 8 and 11 must divide it. We know that $8 \mid x42y$ if $8 \mid 42y$. Thus we must have $y = 4$ since 424 is the only number of this form divisible by 8. Now $11 \mid x424$ only if 11 divides $x - 4 + 2 - 4 = x - 6$. Thus $x = 6$, so the total cost was 64.24, and each chicken cost 73 cents.

(5.1 # 24(a)) Check the multiplication $875,961 \cdot 2753 = 2,410,520,633$ by casting out nines.

Checking the product mod 9, we see that $875961 \equiv 8+7+5+9+6+1 \equiv 0 \pmod 9$ and $2753 \equiv 2+7+5+3 \equiv 8 \pmod 9$, but $2,410,520,633 \equiv 2+4+1+5+2+6+3+3 \equiv 8 \pmod 9$. Since $0 \cdot 8 \not\equiv 8 \pmod 9$, the multiplication does not hold.

(5.2 # 6) Show that days with the same calendar date in two different years of the same century, 28, 56 and 84 years apart, fall on the identical day of the week.

Let Y be defined as in the perpetual calendar. Then

$$Y + 28 + \left[\frac{Y+28}{4}\right] = Y + 28 + \left[\frac{Y}{4}\right] + 7 \equiv Y + \left[\frac{Y}{4}\right] \pmod 7.$$

The same holds when 28 is replaced by 56 or 84, since each of these numbers is divisible by both 4 and 7. Therefore changing the year to another year in the same century 28, 56 or 84 years apart does not change the day of the week.

(5.5 # 8) The bank identification number consists of digits $x_1x_2\cdots x_9$ where $x_9 \equiv 7x_1 + 3x_2 + 9x_3 + 7x_4 + 3x_5 + 9x_6 + 7x_7 + 3x_7 \pmod{10}$.

(a) What is the check digit following the eight-digit identification number 00185403?

$$7 \cdot 0 + 3 \cdot 0 + 9 \cdot 1 + 7 \cdot 8 + 3 \cdot 5 + 9 \cdot 4 + 7 \cdot 0 + 3 \cdot 3 \equiv 5 \pmod{10}$$

so $x_9 = 5$.

(b) What single errors does this check digit detect?

If x_j is replaced by $x_j + a$ where $a \not\equiv 0 \pmod{10}$ then the sum will differ by ka where k is 3, 7 or 9. Then $ka \not\equiv 0 \pmod{10}$, so the error will be detected. Therefore every single error is detected.

(c) Which transposition of two digits does this scheme detect?

The scheme does not detect the transposition of any two digits that have the same weight in the sum. Also, a transposition is not detected if the two digits differ by 5, but the scheme will detect all other transposition errors. To see this, note that a transposition of the digits a and b ($a \neq b$) will not be detected if $7a + 3b \equiv 3a + 7b \pmod{10}$. Then $4a \equiv 4b \pmod{10}$, so $10 \mid 4(a-b)$. Since $a \neq b$, this implies that $5 \mid a - b$. Similarly if $7a + 9b \equiv 9a + 7b \pmod{10}$ or if $3a + 9b \equiv 9a + 3b \pmod{10}$, then a and b differ by 5.

(5.5 # 12(a)) Suppose that one digit in the ISBN $0-19-8?3804-9$ has been smudged. What should the missing digit be?

$$1\cdot 0+2\cdot 1+3\cdot 9+4\cdot 8+5x+6\cdot 3+7\cdot 8+8\cdot 0+9\cdot 4+10\cdot 9\equiv 5x+8 \pmod{11}$$

so solving $5x+8\equiv 0 \pmod{11}$, we have $5x\equiv 3 \pmod{11}$ so $x=5$.

(6.1 # 12) Using Fermat's Little Theorem, find the least positive residue of $2^{1000000}$ modulo 17.

By Fermat's Little Theorem, $2^{16}\equiv 1 \pmod{17}$, and $16\cdot 62500 = 1000000$, so $2^{1000000} = (2^{16})^{62500}\equiv 1 \pmod{17}$.

(6.1 # 18) Show that if n is odd and $3\nmid n$, then $n^2\equiv 1 \pmod{24}$.

By Fermat's Little Theorem, since $3\nmid n$, $n^2\equiv 1 \pmod{3}$. Since n is odd, n is 1, 3, 5, or 7 modulo 8. The square of each of these numbers modulo 8 is 1, so $n^2\equiv 1 \pmod{8}$. Then since $(8,3)=1$, and $8\cdot 3=24$, $n^2\equiv 1 \pmod{24}$.

(6.1 # 24) Show that $1^p+2^p+3^p+\cdots+(p-1)^p\equiv 0 \pmod{p}$ whenever p is an odd prime.

By the corollary to Fermat's Little Theorem, $a^p\equiv a \pmod{p}$ for every integer a. Then

$$1^p+2^p+3^p+\cdots+(p-1)^p\equiv 1+2+3+\cdots+(p-1)\equiv \frac{p(p-1)}{2}\equiv 0 \pmod{p},$$

since $2\mid p-1$.

(6.1 # 26) Use the Pollard $p-1$ method to find a divisor of 689.

Using the formula $r_k\equiv r_{k-1}^k \pmod{689}$, and checking $(r_k-1, 689)$, we have $r_1=2$, $r_2=4$, $r_3=64$, and $r_4=66$, with $(65,689)=13$. Hence $689=13\cdot 53$.