Math 243, Spring 2006, Homework #7
Solutions by Tim Callahan

§2.6 Problem 18: We want to solve

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 5). \end{aligned}$$

We have $a_1 = 2$, $a_2 = 1$ and $a_3 = 3$. The moduli $m_1 = 3$, $m_2 = 4$ and $m_3 = 5$ are pairwise relatively prime, so we can use the Chinese Remainder Theorem. We see that $a_1 = 2$, $a_2 = 1$ and $a_3 = 3$. We let

$$M_1 = m_2m_3 = 20, \qquad M_2 = m_1m_3 = 15, \qquad M_3 = m_1m_2 = 12.$$

Then we find the inverses of each M_i modulo m_i.

To find the inverse of M_1 modulo m_1 we first note that $M_1 = 20 \equiv 2 \pmod 3$. It is easy to see that the inverse of 2 is 2 itself (modulo 3). We let $y_1 = 2$.

For M_2 we have $M_2 = 15 \equiv 3 \pmod 4$, and the inverse of 3 is 3 itself (because $3 \cdot 3 = 9 \equiv 1 \pmod 4$). We let $y_2 = 3$.

For M_3 we have $M_3 = 12 \equiv 2 \pmod 5$, and the inverse of 2 is 3 (because $3 \cdot 2 \equiv 1 \pmod 5$). We let $y_3 = 3$.

Now we let

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233.$$

Of course, we can add any multiple of $m = m_1m_2m_3 = 3 \cdot 4 \cdot 5 = 60$ to this and still get a solution. In fact, we note that $233 \bmod 60 = 53$, so we might as well let $x = 53$. Actually, the problem asks for all solutions, so these would be

$$x = 60n + 53$$

for any integer n.

§2.6 Problem 19: We have $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ and $a_4 = 4$. The moduli $m_1 = 2$, $m_2 = 3$, $m_3 = 5$ and $m_4 = 11$ are pairwise relatively prime, so we use the Chinese Remainder Theorem. We get $m = m_1m_2m_3m_4 = 330$ and

$$M_1 = 165, \qquad M_2 = 110, \qquad M_3 = 66, \qquad M_4 = 30.$$

Now

$$M_1 = 165 \equiv 1 \pmod 2 \quad \Rightarrow \quad y_1 = \overline{1} = 1.$$

For M_2,

$$M_2 = 110 \equiv 2 \pmod 3 \quad \Rightarrow \quad y_2 = \overline{2} = 2.$$

For M_3,

$$M_3 = 66 \equiv 1 \pmod 5 \quad \Rightarrow \quad y_3 = \overline{1} = 1.$$

For M_4,

$$M_4 = 30 \equiv 8 \pmod{11}.$$

We need to find the inverse of 8 modulo 11, so we use the Euclidean algorithm:

$$\begin{aligned} 11 &= 1 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

so

$$\begin{aligned} 1 &= 3-2 = 3-(8-2\cdot 3) \\ &= 3\cdot 3 - 8 = 3\cdot(11-8)-8 \\ &= 3\cdot 11 - 4\cdot 8. \end{aligned}$$

Thus $(-4)\cdot 8 = 1 - 3\cdot 11 \equiv 1 \pmod{11}$, so the inverse of 8 is -4, which is $\equiv 7 \pmod{11}$. Indeed, we can now see that $7\cdot 8 = 56 \equiv 1 \pmod{11}$. Thus we let $y_4 = 7$.

Now our solution is

$x \equiv a_1M_1y_1+a_2M_2y_2+a_3M_3y_3+a_4M_4y_4 = 1\cdot 165\cdot 1+2\cdot 110\cdot 2+3\cdot 66\cdot 1+4\cdot 30\cdot 7 = 1643 \equiv 323 \pmod{330}$.

Thus all solutions are of the form

$$x = 330n + 323$$

for n any integer.

§2.6 Problem 29 (a): Because 7 is prime, we know from Fermat's Little Theorem that if $\gcd(a,7)=1$ then $a^6 \equiv 1 \pmod 7$. Any power of 5 is relatively prime to 7, so we can use this. We note that $2003 = 333\cdot 6+5$, so

$$5^{2003} = 5^{333\cdot 6+5} = 5^{333\cdot 6}\cdot 5^5 = \left(5^{333}\right)^6 \cdot 5^5 \equiv 1\cdot 5^5 \pmod 7,$$

because $\left(5^{333}\right)^6 \equiv 1 \pmod 7$. Now

$$\begin{aligned} 5^2 &= 25 \equiv 4 \pmod 7 \\ 5^4 &= \left(5^2\right)^2 \equiv 4^2 = 16 \equiv 2 \pmod 7 \\ 5^5 &\equiv 5\cdot 2 = 10 \equiv 3 \pmod 7. \end{aligned}$$

Thus $5^{2003} \bmod 7 = 3$.

For $5^{2003} \bmod 11$ we note that $a^{10} \equiv 1 \pmod{11}$ for any a such that $\gcd(a,11)=1$. Thus

$$5^{2003} = 5^{2000}\cdot 5^3 = 5^{200\cdot 10}\cdot 5^3 = \left(5^{200}\right)^{10}\cdot 5^3 \equiv 1\cdot 5^3 = 125 \equiv 4 \pmod{11}.$$

For $5^{2003} \bmod 13$ we note that $a^{12} \equiv 1 \pmod{13}$ for any a such that $\gcd(a,13)=1$. Thus

$$5^{2003} = 5^{166\cdot 12+11} = \left(5^{166}\right)^{12}\cdot 5^{11} \equiv 1\cdot 5^{11} \pmod{13}.$$

Now

$$\begin{aligned} 5^2 &= 25 = 12 \pmod{13} \\ 5^4 &\equiv 12^2 = 144 \equiv 1 \pmod{13} \\ 5^8 &\equiv 1^2 = 1 \pmod{13} \\ 5^{11} &= 5^8\cdot 5^2\cdot 5 \equiv 1\cdot 12\cdot 5 = 60 \equiv 8 \pmod{13}. \end{aligned}$$

Thus $5^{2003} \bmod 13 = 8$.

(b): 7, 11 and 13 are pairwise relatively prime and their product is 1001. We know that if $5^{2003} \bmod 1001 = x$ then

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 4 \pmod{11} \\ x &\equiv 8 \pmod{13}. \end{aligned}$$

We let $M_1 = m_2m_3 = 143$, $M_2 = m_1m_3 = 91$ and $M_3 = m_1m_2 = 77$. Then

$$M_1 = 143 \equiv 3 \pmod 7,$$

and the inverse of 3 modulo 7 is 5 (because $3\cdot 5 = 15 \equiv 1 \pmod 7$), so we let $y_1 = 5$. Then

$$M_2 = 91 \equiv 3 \pmod{11},$$

and the inverse of 3 modulo 11 is 4 (because $3\cdot 4 = 12 \equiv 1 \pmod{11}$), so we let $y_2 = 4$. Then

$$M_3 = 77 \equiv 12 \pmod{13},$$

and the inverse of 12 modulo 13 is 12 (because $12\cdot 12 = 144 \equiv 1 \pmod{13}$), so we let $y_3 = 12$. Now, working modulo 1001, we let

$$x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 3\cdot 143\cdot 5 + 4\cdot 91\cdot 4 + 8\cdot 77\cdot 12 = 10993 \equiv 983.$$

Thus $5^{2003} \bmod 1001 = 983$.

§2.7 Problem 3 (a):

$$AB = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 0 & 4 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 11 \\ 2 & 18 \end{bmatrix}.$$

(b):

$$AB = \begin{bmatrix} 1 & -1 \\ 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 3 & -2 & -1 \\ 1 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & -2 & -3 \\ 1 & 0 & 2 \\ 9 & -4 & 4 \end{bmatrix}.$$

(c):

$$AB = \begin{bmatrix} 4 & -3 \\ 3 & -1 \\ 0 & -2 \\ -1 & 5 \end{bmatrix} \begin{bmatrix} -1 & 3 & 2 & -2 \\ 0 & -1 & 4 & -3 \end{bmatrix} = \begin{bmatrix} -4 & 15 & -4 & 1 \\ -3 & 10 & 2 & -3 \\ 0 & 2 & -8 & 6 \\ 1 & -8 & 18 & -13 \end{bmatrix}.$$

§2.7 Problem 15: We have

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

so

$$A^2 = AA = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}.$$

Then

$$A^3 = A^2 A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}.$$

Then

$$A^4 = A^3 A = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}.$$

The pattern we suspect is that

$$A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

This turns out to be correct, but we need induction to prove it.

§2.7 Problem 18: To show that two matrices are inverses we just multiply them together and show that the result is the identity matrix. We have

$$\begin{bmatrix} 2 & 3 & -1 \\ 1 & 2 & 1 \\ -1 & -1 & 3 \end{bmatrix} \begin{bmatrix} 7 & -8 & 5 \\ -4 & 5 & -3 \\ 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

§2.7 Problem 29: We have

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

(a): $A \vee B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$

(b): $A \wedge B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$

(c):

$$A \odot B = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

§2.7 Problem 30:

$$A \odot B = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}.$$