Math 211

Assignment 5 - Solutions

[1] 1. (a) Since $\gcd(3,17)=1$, the implication is *true* for all $x,y\in\mathbb{Z}$ by the Cancellation Law.

[1] (b) This is *false* for $x=y=5$. Indeed, $3x=15\equiv 0\equiv 45\equiv 9y \pmod{15}$, but $x=5\not\equiv 3y=15\equiv 0 \pmod{15}$.

[3] 2. (a) Suppose first that $4|x$, i.e. $x=4k$, for some $k\in\mathbb{Z}$. Then $x^2=16k^2\equiv 0 \pmod 8$. Next, suppose $x=4k\pm 1$. Then $x^2=16k^2\pm 8k+1\equiv 1 \pmod 8$. Finally, suppose $x=4k+2$. Then $x^2=16k^2+16k+4\equiv 4 \pmod 8$. Summarizing, we have

$$x^2\equiv\begin{cases} 0 \pmod 8 & \text{if } x\equiv 0 \pmod 4\\ 1 \pmod 8 & \text{if } x\equiv \pm 1 \pmod 4\\ 4 \pmod 8 & \text{if } x\equiv 2 \pmod 4\end{cases}$$

Since every integer $x\equiv 0,\pm 1$, or $2 \pmod 4$, this proves that $x^2\equiv 0,1$, or $4 \pmod 8$ for all integers x.

(b) By hypothesis, $n\equiv 7 \pmod 8$. It is therefore enough to show that $x^2+y^2+z^2\not\equiv 7 \pmod 8$, for any $x,y,z\in\mathbb{Z}$. For this, suppose (x,y,x) is such a solution and let r denote the number of odd entries. (Thus, $r=0\Leftrightarrow$ x,y,z are all even, $r=1\Leftrightarrow$ exactly one of x,y,z is even etc.). Since $r\equiv x^2+y^2+z^2\equiv 7 \pmod 2$, we see that r has to be odd. We thus have two cases:

Case 1: $r=3$. Here $x\equiv y\equiv z\equiv 1 \pmod 2$, so by part (a) $x^2+y^2+z^2\equiv 1+1+1\equiv 3\not\equiv 7 \pmod 8$.

Case 2: $r=1$. By symmetry, we may assume without loss generality that $x\equiv 1 \pmod 2$, and that hence $y,z\equiv 0 \pmod 2$. From part (a) we see that $y^2+z^2\equiv 0+0, 0+4, 4+0, 4+4 \pmod 8$, depending on whether $y\equiv 0,2 \pmod 4$ and $z\equiv 0,2 \pmod 4$. Thus $y^2+z^2\equiv 0,4 \pmod 8$, and hence $x^2+y^2+z^2\equiv 1+0, 1+4\not\equiv 7 \pmod 8$.

Thus, both cases are impossible, and hence $x^2+y^2+z^2\not\equiv 7 \pmod 8$.

Alternate proof: As in the first proof, suppose that (x,y,x) is a solution of $x^2+y^2+z^2\equiv 7 \pmod 8$, and let r denote the number of odd entries. From part (a) we see that $x^2\equiv 1 \pmod 4$ if x is odd and $x^2\equiv 0 \pmod 4$ if x is even. Thus $r\equiv x^2+y^2+z^2\equiv 7\equiv 3 \pmod 4$. Since $r\le 3$, we see that $r=3$, i.e. that x,y and z are all odd. But then by part (a) we have $x^2+y^2+z^2\equiv 1+1+1\equiv 3\not\equiv 7 \pmod 8$, so no solution can exist.

[2] 3. (a) Since $\gcd(11,57)=1$, there is a unique solution $\pmod{57}$. To find it, solve $11x+57y=1$ using the Euclidean algorithm:

$$57=5\cdot 11+2, \qquad 11=5\cdot 2+1,$$

so $1=11-5\cdot 2=11-5(57-11\cdot 5)=11\cdot 26+57(-5)$. Thus $x_0=26$ satisfies $11x_0\equiv 1 \pmod{57}$ and hence $x\equiv 23x_0\equiv 23\cdot 26\equiv 28 \pmod{57}$ is the unique solution.

[1] (b) Here $\gcd(12,63)=3$. Since $3\nmid 28$, the congruence equation has no solutions.

[2] (c) Here $\gcd(16,36)=4$, and $4|40$, so there are precisely 4 solutions $\pmod{36}$. To find these, solve $16x+36y=4$. Since $36=2\cdot 16+4$, we can take $x=-2, y=1$. Thus, the formula gives $x=\frac{40}{4}(-2)+\frac{36}{4}t=-20+9t, t\in\mathbb{Z}$, so we get $x\equiv -20,-11,-2,7 \pmod{36}$, or $x\equiv 7,16,25,34 \pmod{36}$.

[1] 4. (a) The given equation is equivalent to the congruence equation $5x\equiv 2 \pmod{13}$. Since $\gcd(5,13)=1$, Theorem 4 tells us that this congruence equation has a unique solution. Since $5(8)=40\equiv 1 \pmod{13}$, we see that $x\equiv 2\cdot 8\equiv 3 \pmod{13}$. Thus, $x=[3]$ (or just $x=3$) is the desired solution of the equation in $\mathbb{F}_{13}$.

[1] (b) Here we have to solve $16x\equiv 40 \pmod{36}$. In part (c) of the previous question we found that there are four solutions: $x\equiv 7,16,25,34 \pmod{36}$. Thus, the four solutions of $16x=40$ in $\mathbb{Z}/36\mathbb{Z}$ are: $x=[7],[16],[25],[34]$ (or $x=7,16,25,34$).

[2] 5. (a) Since $\gcd(m_1,m_2)=\gcd(27,31)=1$, we can apply the method of the Chinese Remainder Theorem. We have $m=27\cdot 31=837$, and

$$\begin{array}{rclcl} m_1' &=& \frac{27\cdot 31}{27} &=& 31, \\ m_2' &=& \frac{27\cdot 31}{31} &=& 27, \end{array} \qquad \begin{array}{rcll} m_1' &\equiv& 4 & \pmod{27} \\ m_2' &\equiv& -4 & \pmod{31}. \end{array}$$

We can find m_i^* by inspection $\left\{\begin{array}{rcll} 4m_1^* & \equiv 1 & \pmod{27} & \Rightarrow \quad m_1^* \equiv 7 \pmod{27} \\ -4m_2^* & \equiv 1 & \pmod{31} & \Rightarrow \quad m_2^* \equiv -8 \pmod{31} \end{array}\right\}$. (Indeed: $4 \cdot 7 \equiv 1 \pmod{27}$ and $(-4)(-8) \equiv 1 \pmod{31}$.) Thus, since $a_1 = 11, a_2 = 13$, we get

$$\begin{aligned} x &\equiv a_1 m_1^* m_1' + a_2 m_2^* m_2' \pmod{m} \\ &\equiv 11 \cdot 7 \cdot 31 + 13 \cdot (-8) \cdot 27 \pmod{837} \\ &\equiv 2387 - 2808 \ \equiv \ -421 \equiv 416 \pmod{837}, \end{aligned}$$

and so the solution is $x \equiv 416 \pmod{837}$. (The answer $x \equiv -421 \pmod{837}$ is also acceptable.)

[3] (b) Here we have $m_1 = 21, m_2 = 26, m_3 = 31$. Since $\gcd(21, 26) = \gcd(21, 31) = \gcd(26, 31) = 1$, we can apply the CRT formula. (Note that checking the much weaker condition $\gcd(21, 26, 31) = 1$ is insufficient here.) We have $m = 23 \cdot 27 \cdot 31 = 16926$, and

$$\begin{array}{rclcl} m_1' & = & \frac{21\cdot 26\cdot 31}{21} & = & 26 \cdot 31, \\ m_2' & = & \frac{21\cdot 26\cdot 31}{26} & = & 21 \cdot 31, \\ m_3' & = & \frac{21\cdot 26\cdot 31}{31} & = & 21 \cdot 26, \end{array} \qquad \begin{array}{rcrcrl} m_1' & \equiv & 5 \cdot 10 & \equiv & 8 & \pmod{21} \\ m_2' & \equiv & (-5)5 & \equiv & 1 & \pmod{26} \\ m_3' & \equiv & (-10)(-5) & \equiv & -12 & \pmod{31}. \end{array}$$

We now calculate the m_i^*:

$$\begin{array}{rllcrcrl} 8m_1^* & \equiv 1 & \pmod{21} & \Rightarrow & m_1^* & \equiv & 8 & \pmod{21} \\ m_2^* & \equiv 1 & \pmod{26} & \Rightarrow & m_2^* & \equiv & 1 & \pmod{26} \\ -12m_3^* & \equiv 1 & \pmod{31} & \Rightarrow & m_3^* & \equiv & -13 & \pmod{31}. \end{array}$$

These are not so easy to do by inspection, so we use the extended Euclidean algorithm. We have $21 = 2 \cdot 8 + 5$, $8 = 1 \cdot 5 + 3$, $5 = 3 + 2$, $3 = 2 + 1$, so $1 = 3 - 2 = 2 \cdot 3 - 5 = 2 \cdot 8 - 3 \cdot 5 = 8 \cdot 8 - 3 \cdot 21$. Thus, $8(8) - 3(21) = 1$, and hence $m_1^* \equiv 8 \pmod{21}$. Similarly, $31 = 2 \cdot 12 + 7$, $12 = 7 + 5$, $7 = 5 + 2$, $5 = 2 \cdot 2 + 1$, so $1 = 5 - 2(2) = 3(7) - 4(5) = 7(7) - 4(12) = 7(31) - 18(12)$. Thus, $7(31) - 18(12) = 1$, and hence $m_3^* \equiv 18 \equiv -13 \pmod{31}$.

Thus, since $a_1 = 3, a_2 = -4, a_3 = 5$, we get

$$\begin{aligned} x &\equiv a_1 m_1^* m_1' + a_2 m_2^* m_2' + a_3 m_2^* m_3' \pmod{m} \\ &\equiv 3(8)(26 \cdot 31) + 4(1)(21 \cdot 31) + 5(-13)(21 \cdot 26) \pmod{16926} \\ &\equiv 19344 + 2604 - 35490 \ \equiv \ -13542 \equiv 3384 \pmod{16926}, \end{aligned}$$

and hence the solution is $x \equiv 3384 \pmod{16926}$.

[3] 6. See the MAPLE solution on the course Web site (mast.queensu.ca/~math211).

Comments on the Submitted Solutions: 1(b) To give a counterexample means that you have to give explicit numbers x and y such that $3x \equiv 9y \pmod{15}$, but $x \not\equiv 3y \pmod{15}$.

3) – 5) The term "by inspection" means that the necessary computations can be done in your head, not just on a calculator. You need to give enough detail so that the marker can do the computations in his head.

5) The solution of a system of simultaneous congruences is a congruence mod $m_1 \cdots m_r$. But if the question asks for the smallest positive integer satisfying a given system, then the solution is an integer.