Homework #7 Solutions

4.2.2. (a) Since $(3,7) = 1$, the congruence has a unique solution modulo 7 by Theorem 4.11. We have $7 - 2 \cdot 3 = 1$, so, reducing this equation modulo 7, we obtain $3 \cdot (-2) \equiv 1 \pmod 7$. Multiplying both sides of this congruence by 2 gives $3 \cdot (-4) \equiv 2 \pmod 7$. Therefore the unique solution to the congruence is given by $x \equiv -4 \equiv 3 \pmod 7$.
(b) Since $(6,9) = 3$ and $3 \mid 3$, the congruence has three incongruent solutions modulo 9 by Theorem 4.11. Reducing the equation $9 - 6 = 3$ modulo 9 gives $6 \cdot (-1) \equiv 3 \pmod 9$. Thus one solution to the congruence is given by $x_1 \equiv -1 \equiv 8 \pmod 9$. The remaining two incongruent solutions are given by

$$x_2 \equiv x_1 + \frac{9}{3} \equiv 8 + 3 \equiv 11 \equiv 2 \pmod 9$$

and

$$x_3 \equiv x_1 + \left(\frac{9}{3}\right) \cdot 2 \equiv 8 + 3 \cdot 2 \equiv 14 \equiv 5 \pmod 9.$$

(c) Since $(17, 21) = 1$, the congruence has a unique solution modulo 21. To find this solution, we use the Euclidean algorithm to express 1 as a linear combination of 17 and 21:

$$\begin{aligned} 21 &= 1 \cdot 17 + 4 \\ 17 &= 4 \cdot 4 + 1 \\ 1 &= 17 - 4 \cdot 4 = 17 - 4(21 - 17) = 5 \cdot 17 - 4 \cdot 21. \end{aligned}$$

Reducing the equation $5 \cdot 17 - 4 \cdot 21 = 1$ modulo 21 gives $17 \cdot 5 \equiv 1 \pmod{21}$. Multiplying this congruence by 14 gives $17 \cdot (5 \cdot 14) \equiv 14 \pmod{21}$. Therefore the unique solution to the congruence is given by

$$x \equiv 5 \cdot 14 \equiv 35 \cdot 2 \equiv 14 \cdot 2 \equiv 28 \equiv 7 \pmod{21}.$$

4.2.8. (a) We have $13 - 2 \cdot 6 = 1$, so on reducing modulo 13 we find that $2 \cdot (-6) \equiv 1 \pmod{13}$, which gives $\overline{2} \equiv -6 \equiv 7 \pmod{13}$.
(b) We have $13 - 3 \cdot 4 = 1$, so on reducing modulo 13 we find that $3 \cdot (-4) \equiv 1 \pmod{13}$, which gives $\overline{3} \equiv -4 \equiv 9 \pmod{13}$.
(c) We have $2 \cdot 13 - 5 \cdot 5 = 1$, so on reducing modulo 13 we find that $5 \cdot (-5) \equiv 1 \pmod{13}$, which gives $\overline{5} \equiv -5 \equiv 8 \pmod{13}$.
(d) We use the Euclidean algorithm to express 1 as a linear combination of 13 and 11:

$$\begin{aligned} 13 &= 1 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1 \\ 1 &= 11 - 5 \cdot 2 = 11 - 5 \cdot (13 - 11) = 6 \cdot 11 - 5 \cdot 13. \end{aligned}$$

Reducing the equation $6 \cdot 11 - 5 \cdot 13 = 1$ modulo 13 gives $11 \cdot 6 \equiv 1 \pmod{13}$, so $\overline{11} \equiv 6 \pmod{13}$.

Date: April 1, 2018.

4.2.15. Since $(\pm 1)^2 = 1$, $(\pm 1)^2 \equiv 1 \pmod{p^k}$, so ± 1 are solutions to $X^2 \equiv 1 \pmod{p^k}$. Moreover, if $1 \equiv -1 \pmod{p^k}$, then p^k divides $1-(-1) = 2$, which is impossible as p is odd. Thus ± 1 are incongruent solutions to $X^2 \equiv 1 \pmod{p^k}$. Conversely, consider an arbitrary integer x such that $x^2 \equiv 1 \pmod{p^k}$. Then p^k divides $x^2-1 = (x-1)(x+1)$. In particular, p divides $(x-1)(x+1)$, so, as p is prime, p divides $x-1$ or p divides $x+1$. Moreover, p cannot divide both $x-1$ and $x+1$, for if this were the case, then p would divide $(x+1)-(x-1) = 2$, a contradiction because p is odd. So p divides exactly one of $x \pm 1$. Assume first that p divides $x-1$. Then, since p does not divide $x+1$, $1 = (p, x+1) = (p^k, x+1)$. So, since p^k and $x+1$ are relatively prime, p^k must divide $x-1$, i.e., $x \equiv 1 \pmod{p^k}$. The case where p divides $x+1$ is similar and leads to $x \equiv -1 \pmod{p^k}$. Thus $x \equiv \pm 1 \pmod{p^k}$.

4.2.16. If $k = 1$ or $k = 2$, the assertions can be verified by direct computation, so we will assume $k > 2$. We have $(\pm 1)^2 = 1 \equiv 1 \pmod{2^k}$, while

$$(\pm(1+2^{k-1}))^2 = (1+2^{k-1})^2 = 1 + 2^k + 2^{2(k-1)},$$

and since $k > 2$, $2(k-1) > k$, so on reducing the final expression above modulo 2^k we obtain $(\pm(1+2^{k-1}))^2 \equiv 1 \pmod{2^k}$. So ± 1 and $\pm(1+2^{k-1})$ are solutions to $X^2 \equiv 1 \pmod{2^k}$. That these solutions are pairwise incongruent can be checked using that $k > 2$. For example, if $1+2^{k-1} \equiv -1 \pmod{2^k}$, then 2^k divides $2+2^{k-1}$. This is impossible because $2^k = 2^{k-1} + 2^{k-1} > 2 + 2^{k-1}$ for $k > 2$. The other cases are similar.

We have exhibited four incongruent solutions to $X^2 \equiv \pm 1 \pmod{2^k}$, and to show that these are the only solutions up to congruence modulo 2^k, we let x be any solution, so $x^2 \equiv 1 \pmod{2^k}$. This means that 2^k divides $x^2 - 1 = (x-1)(x+1)$. In particular, 2 divides $(x-1)(x+1)$, so 2 divides one of $x \pm 1$. But if one of $x \pm 1$ is even, then so is the other, and therefore 2 is a common divisor of $x \pm 1$. Moreover, since $(x+1) - (x-1) = 2$, 2 must be the greatest common divisor of $x-1$ and $x+1$. This implies that there are two possibilities: one is that 2^{k-1} divides $x-1$, and the other is that 2^{k-1} divides $x+1$. Assume that the first possibility holds. As 2^{k-1} divides $x-1$, we have $x - 1 = 2^{k-1}j$ for some integer j, hence $x = 1 + 2^{k-1}j$. If $j = 2q + r$ where q and r are integers and $0 \le r < 2$, then $x = 1 + 2^{k-1}j = 1 + 2^{k-1}(2q+r) = 1 + 2^k q + 2^{k-1} r \equiv 1 + 2^{k-1} r \pmod{2^k}$, and it follows that we need only consider $j \in \{0, 1\}$. If $j = 0$, then $x \equiv 1 \pmod{2^k}$, while if $j = 1$, then $x \equiv 1 + 2^{k-1} \pmod{2^k}$. Similarly, when 2^{k-1} divides $x+1$, we find that either $x \equiv -1 \pmod{2^k}$ or $x \equiv -1 + 2^{k-1} \pmod{2^k}$. It remains only to observe that $-1+2^{k-1} \equiv -1-2^{k-1} \pmod{2^k}$, because

$$(-1+2^{k-1}) - (-1-2^{k-1}) = 2 \cdot 2^{k-1} = 2^k \equiv 0 \pmod{2^k}.$$

We may conclude that x is congruent to one of $\pm 1, \pm(1+2^{k-1})$ modulo 2^k.

4.2.18. Suppose x is a solution to the congruence $X^2 \equiv a \pmod{p}$, so that $x^2 \equiv a \pmod{p}$. Then we have $(-x)^2 = x^2 \equiv a \pmod{p}$, so $-x$ is also a solution to the congruence. We claim that x and $-x$ are incongruent modulo p. To see this, assume the contrary, i.e., that $x \equiv -x \pmod{p}$. Then p divides $2x$, and because p is odd, $(p, 2) = 1$, so we must have $p \mid x$. But then $a \equiv x^2 \equiv 0 \pmod{p}$, contradicting the hypothesis that $p \nmid a$.

Now if y is any integer satisfying $y^2 \equiv a \pmod{p}$, then because x is also a solution to the congruence, we have $y^2 \equiv x^2 \pmod{p}$. Therefore p divides $y^2 - x^2 = (y-x)(y+x)$. As p is prime, it follows that p divides $y - x$ or p divides $y + x$, so that $y \equiv \pm x \pmod{p}$. Thus we may conclude that either the congruence $X^2 \equiv a \pmod{p}$ has no solutions, or it has exactly two incongruent solutions.

4.3.15. The integers x satisfying $x \equiv a_1 \pmod{m_1}$ are of the form $a_1 + m_1 t$, where t is a an integer. If such an x is also to satisfy the second congruence, then we must be able to choose t so that $a_1 + m_1 t \equiv a_2 \pmod{m_2}$, or equivalently, $m_1 t \equiv a_2 - a_1 \pmod{m_2}$. This is a linear congruence in t, and by Theorem 4.11, it admits a solution if and only if (m_1, m_2) divides $a_2 - a_1$ (note that this is logically equivalent to (m_1, m_2) dividing $a_1 - a_2$). Thus the system of congruences admits a simultaneous solution if and only if (m_1, m_2) divides $a_1 - a_2$.

To see that a solution to the system, when it exists, is unique modulo $[m_1, m_2]$, suppose x and x' are both solutions. Then $x \equiv a_1 \equiv x' \pmod{m_1}$, so m_1 divides $x - x'$. Similarly, m_2 divides $x - x'$. Therefore $x - x'$ is a common multiple of m_1 and m_2, and therefore must be divisible by the least common multiple $[m_1, m_2]$. So $x \equiv x' \pmod{[m_1, m_2]}$, establishing the uniqueness modulo $[m_1, m_2]$.

4.3.30. If x is congruent to any of $0, 2, 4, 6, 8, 10$ modulo 12, then $x \equiv 0 \pmod{2}$. If x is congruent to 3 or 9 modulo 12, then $x \equiv 0 \pmod{3}$. Integers x congruent to 1 or 5 modulo 12 satisfy $x \equiv 1 \pmod{4}$, and if $x \equiv 7 \pmod{12}$, then $x \equiv 7 \equiv 1 \pmod{6}$. Any integer x is congruent modulo 12 to one of the integers in the set $\{0, \ldots, 11\}$. The only integers we have not addressed are the ones congruent to 11 modulo 12, i.e., satisfying the final congruence. Thus the set of congruences is a covering set.