MODEL ANSWERS TO THE SIXTH HOMEWORK

3.3.1. a) Note that 4, 21 and 25 pairwise coprime. We have to solve three auxiliary equations

$$\begin{aligned} 21 \cdot 25 z_1 &\equiv 1 \mod 4 \\ 4 \cdot 25 z_2 &\equiv 1 \mod 21 \\ 4 \cdot 21 z_3 &\equiv 1 \mod 25. \end{aligned}$$

These reduce to

$$\begin{aligned} z_1 &\equiv 1 \mod 4 \\ 16 z_2 &\equiv 1 \mod 21 \\ 9 z_3 &\equiv 1 \mod 25. \end{aligned}$$

Note that $64 \equiv 1 \mod 21$ and $126 \equiv 1 \mod 25$. Thus we get

$$\begin{aligned} z_1 &= 1 \\ z_2 &= 4 \\ z_3 &= 14. \end{aligned}$$

It follows that

$$\begin{aligned} x &= 21 \cdot 25 \cdot 1 \cdot 3 + 4 \cdot 25 \cdot 4 \cdot 5 + 4 \cdot 21 \cdot 14 \cdot 7 \\ &= 1307 \mod 4 \cdot 21 \cdot 25. \end{aligned}$$

b) We first solve equations for y. The greatest common divisor of 3 and 12 is 3. This divides 9, so the first equation reduces to $x \equiv 3 \mod 4$. 4 and 35 are coprime. $4 \cdot 9 = 36 \equiv 1 \mod 35$. So 9 is the inverse of 4 modulo 35. The second equation reduces to $x \equiv 10 \mod 35$. 6 and 11 are coprime. $2 \cdot 6 = 12 \equiv 1 \mod 11$. Thus $x \equiv 4 \mod 11$.
So we first have to solve the three equations

$$\begin{aligned} x &\equiv 3 \mod 4 \\ x &\equiv 10 \mod 35 \\ x &\equiv 4 \mod 11. \end{aligned}$$

Note that 4, 35 and 11 pairwise coprime. We have to solve three auxiliary equations

$$\begin{aligned} 35 \cdot 11 z_1 &\equiv 1 \mod 4 \\ 4 \cdot 11 z_2 &\equiv 1 \mod 35 \\ 4 \cdot 35 z_3 &\equiv 1 \mod 11. \end{aligned}$$

These reduce to

$$\begin{aligned} z_1 &\equiv 1 \mod 4 \\ 9z_2 &\equiv 1 \mod 35 \\ 8z_3 &\equiv 1 \mod 11. \end{aligned}$$

Note that $36 \equiv 1 \mod 35$ and $56 \equiv 1 \mod 11$. Thus we get

$$\begin{aligned} z_1 &= 1 \\ z_2 &= 4 \\ z_3 &= 7. \end{aligned}$$

It follows that

$$\begin{aligned} x &= 35 \cdot 11 \cdot 1 \cdot 3 + 4 \cdot 11 \cdot 4 \cdot 10 + 4 \cdot 35 \cdot 7 \cdot 4 \\ &= 675 \mod 4 \cdot 35 \cdot 11. \end{aligned}$$

To find y, note that there are three numbers modulo $3 \cdot 4 \cdot 35 \cdot 11$ whose residue modulo $4 \cdot 35 \cdot 11$ is 675, namely:

$$675, \qquad 675 + 4 \cdot 35 \cdot 11 = 2215 \qquad \text{and} \qquad 675 + 2 \cdot 4 \cdot 35 \cdot 11 = 3755.$$

(c) Note that 12 and 21 have greatest common divisor 3. Now 3 divides $4 - 1$ so that the first two equations have a solution. 21 and 35 have greatest common divisor 7. 7 divides $18 - 4 = 14$ and so the second two equations have a solution. 12 and 35 are coprime. Thus the first and third equations have a solution.
Thus we can solve these equations. The solutions are residue classes modulo the lowest common multiple of 12, 21 and 35, that is, $3 \cdot 7 \cdot 4 \cdot 5 = 420$.
We first solve the first and second equations. We first solve

$$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 4 \mod 7. \end{aligned}$$

We need to solve

$$\begin{aligned} 7z_1 &\equiv 1 \mod 4 \\ 4z_2 &\equiv 1 \mod 7. \end{aligned}$$

We get

$$\begin{aligned} z_1 &\equiv 3 \mod 4 \\ z_2 &\equiv 2 \mod 7. \end{aligned}$$

Thus

$$\begin{aligned} x &= 7 \cdot 1 \cdot 3 + 4 \cdot 4 \cdot 2 \\ &\equiv -7 + 4 \mod 4 \cdot 7 \\ &\equiv 25 \mod 4 \cdot 7. \end{aligned}$$

In fact 25 is also the solution to the original equations. Thus 25 is the solution to the equation

$$x \equiv 25 \mod 3 \cdot 4 \cdot 7.$$

Now we need to solve the second and third equations. We first solve

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 3 \mod 5. \end{aligned}$$

We need to solve

$$\begin{aligned} 5z_1 &\equiv 1 \mod 3 \\ 3z_2 &\equiv 1 \mod 5. \end{aligned}$$

We get

$$\begin{aligned} z_1 &\equiv 2 \mod 3 \\ z_2 &\equiv 2 \mod 5. \end{aligned}$$

Thus

$$\begin{aligned} x &= 5 \cdot 1 \cdot 2 + 3 \cdot 3 \cdot 2 \\ &= 13 \mod 15. \end{aligned}$$

Now this is not a solution to the original equations. The general solution to the equation above is $y = 13 + 15t$. If this is a solution to the original equations, we want

$$13 + 15t \equiv 4 \mod 21.$$

Thus

$$15t \equiv 12 \mod 21.$$

Thus

$$5t \equiv 4 \mod 7.$$

This has solution $t = 5$. Thus $y = 13 + 15 \cdot 5 = 88$. This is a solution to the original pair of equations

$$\begin{aligned} y &\equiv 4 \mod 21 \\ y &\equiv 18 \mod 35. \end{aligned}$$

Finally we want to find a number y such that

$$y \equiv 25 \mod 3 \cdot 4 \cdot 7$$
$$y \equiv 88 \mod 3 \cdot 5 \cdot 7.$$

The general solution to the first equation is $y = 25 + 56t$. So we want

$$25 + 56t \equiv 88 \mod 3 \cdot 5 \cdot 7.$$

We get

$$56t \equiv 63 \mod 3 \cdot 5 \cdot 7.$$

Thus

$$8t \equiv 9 \mod 3 \cdot 5.$$

We get $t = 3$. Thus the solution is $25 + 56 \cdot 3 = 193$.
3.3.2. Let

$$f \colon \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_5,$$

be the function given by the Chinese Remainder theorem. Then

$$\begin{aligned}
f(0) &= (0, 0) \\
f(1) &= (1, 1) \\
f(2) &= (0, 2) \\
f(3) &= (1, 3) \\
f(4) &= (0, 4) \\
f(5) &= (1, 0) \\
f(6) &= (0, 1) \\
f(7) &= (1, 2) \\
f(8) &= (0, 3) \\
f(9) &= (1, 4).
\end{aligned}$$

3.3.5. Let $p_1, p_2, \dots, p_r$ be distinct primes, for example

$$2, 3, 5, \dots, p_r.$$

Let $m_i = p_i^2$. Then

$$m_1, m_2, \dots, m_r$$

are pairwise coprime. Let

$$c_i = m_i - i - 1,$$

so that

$$\begin{aligned} c_1 &\equiv 0 \mod m_1 \\ c_2 &\equiv -1 \mod m_2 \\ c_3 &\equiv -2 \mod m_3 \\ \vdots \quad \ddots & \qquad \vdots \\ c_r &\equiv -r+1 \mod m_r. \end{aligned}$$

Then, by the Chinese remainder theorem, we can find a natural number x congruent to c_i, modulo m_i, for every $1 \leq i \leq r$. Note that

$$x \equiv 0 \mod m_1,$$

so that $m_1 = p_1^2$ divides x. Thus x is not square-free. But

$$x + 1 \equiv 0 \mod m_2,$$

so that p_2^2 divides $x + 1$. Thus $x + 1$ is not square-free. In general

$$x + (i - 1) \equiv 0 \mod m_i,$$

so that p_i^2 divides $x + i = 1$. Thus $x + i - 1$ is not square-free.
It follows that none of the r consecutive integers

$$x, \qquad x+1, \qquad x+2, \qquad \dots \qquad x+r-1$$

is square-free.
3.3.7. (a) Let p be a prime dividing n. Suppose that p does not divide $b = 0 \cdot a + b$. In this case, we take $x = 0$. If p does divide b then p does not divide a. Then $b + a = b + 1 \cdot a$ is not divisible by p. In this case, we take $x = 1$.
Let m be the product of all primes dividing n (so that m is square-free and has the same prime factors as n). For every prime $m_i = p_i$ dividing m we have already shown that we can find c_i such that

$$ax \equiv c_i - b \neq 0 \mod m_i,$$

has a solution. By the Chinese remainder theorem, we can find x such that all of these equations have a simultaneous solution. In this case $ax + b$ is coprime to every $m_i = p_i$ so that $ax + b$ is coprime to n.
(b) We have to construct an infinite sequence of integers

$$x_1, x_2, \dots$$

whose elements are pairwise coprime. Suppose that we have constructed

$$x_1, x_2, \dots, x_i.$$

Let n be the product of

$$\prod_{j=1}^{i}(ax_i + b).$$

Then we can find x such that $(ax + b, n) = 1$. Let $x = x_{i+1}$. Then $ax_{i+1} + b$ is coprime to n so that it is coprime to $ax_j + b$ for $j \leq i$. Thus we can construct

$$x_1, x_2, \ldots, x_{i+1},$$

and so we can construct an infinite sequence.

3.3.8. We have

$$\begin{aligned} a \cdot a^{\varphi(m)-1} &= a^{\varphi(m)} \\ &\equiv 1 \mod m. \end{aligned}$$

Thus

$$x = a^{\varphi(m)-1}$$

is a solution to the equation

$$ax \equiv 1 \mod m.$$

It follows that

$$x = a^{\varphi(m)-1}b$$

is a solution to the equation

$$ax \equiv b \mod m.$$

3.4.1 If $p \leq n + 1$ then we are done by (3.1.1). So we may assume that $n + 1 < p$. Since the difference between any $n + 1$ consecutive integers is at most n, it follows that any $n + 1$ consecutive integers are pairwise different modulo p. Thus the polynomial $\bar{f}(x) \in \mathbb{Z}_p[x]$, obtained from $f(x)$ by reduction modulo p, has at least $n+1$ roots. It follows that $\bar{f}(x)$ is the zero polynomial. But then every coefficient of $f(x)$ is divisible by p, so that $p|f(a)$ for every integer a.