MATH342 Feedback and Solutions 4

1. If $a = 2k$ for $k \in \mathbb{Z}$ then $a^2 = 4k^2 = 0 \mod 4$. If $a = 2k+1$ then $a^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Either k or $k+1$ is even. So $k(k+1) = 2m$ for $m \in \mathbb{Z}$ – actually for $m \in \mathbb{N}$ because k and $k+1$ are either both ≥ 0 or both ≤ 0. So $a^2 = 8m + 1$ and $a^2 = 1 \mod 8$.

In this question and others: note that if $x \equiv 0 \bmod 4$ then it does not follow that $x \equiv 0 \bmod 8$. The first statement says that $4 \mod x$. The second statement says that $8 \mid x$. Of course if $x \equiv 4 \bmod 4$ we can say that $x \equiv 0 \bmod 8$ or $x \equiv 4 \bmod 8$. There are many ways of doing this question. Quite a few people considered the different choices for an odd number $\bmod 8$. These can be written as $\pm 1 \bmod 8$ and $\pm 3 \bmod 8$, for which the squares are $1 \bmod 8$ or $9 \equiv 1 \bmod 8$.

2.

a) Suppose that $n = a_1^2 + a_2^2 + a_3^2$.
If all of a_1, a_2 and a_3 are even then $a_i^2 = 0 \mod 4$ for all i and $n = 0 \mod 4$, that is, $n = 0$ or $4 \mod 8$.
If exactly one of the a_i is odd then we can assume that a_1 is odd and a_2 and a_3 are even. Then $a_1^2 = 1 \mod 8 = 1 \mod 4$ and $a_2^2 + a_3^2 = 0 \mod 4$. Hence $n = 1 \mod 4$, that is, $n = 1$ or $5 \mod 8$.
If exactly two of the a_i are odd, we can assume that a_1 and a_2 are odd and a_3 is even. Then $a_1^2 + a_2^2 = 2 \mod 8 = 2 \mod 4$ and $a_3^2 = 0 \mod 4$, and $n = 2 \mod 4$, so that $n = 2$ or $6 \mod 8$.
If all the a_i are odd then $n = a_1^2 + a_2^2 + a_3^2 = 3 \mod 8$.
So $a_1^2 + a_2^2 + a_3^2$ is never equal to $7 \mod 8$.

b) Write $b^2 = a$. then $a = 0 \mod 4$ or $1 \mod 8$. If $a = 4k$ for $k \in \mathbb{N}$ then

$$b^4 = a^2 = 16k^2 \equiv 0 \mod 16.$$

If $a = 8k + 1$ for $k \in \mathbb{N}$ then

$$b^4 = a^2 = 64k^2 + 16k + 1 \equiv 1 \mod 16.$$

It was expected that you would use question 1, to shorten the question. But it is natural to use the Binomial Theorem for b^4 in the case of b odd, which some people did. In this case $b = 2m + 1$ and

$$b^4 = 16m^4 + 32m^3 + 24m^2 + 8m + 1 = 16(m^4 + 2m^3 + m^2) + 8m(m+1) + 1$$

It is then necessary to use (as before) that $m(m+1)$ is even.

3.

$$x^2 \equiv x \mod p^k \Leftrightarrow x^2 - x \equiv 0 \mod p^k \Leftrightarrow p^k \mid x(x-1).$$

So if $x^2 \equiv x \mod p^k$, since p is prime, either $p \mid x$ or $p \mid x - 1$. Clearly it cannot divide both. So if p divides x, none of the prime factors of $x - 1$ is p, and by unique factorisation of $x(x-1)$, it must be the case that $p^k \mid x$. Similarly if $p \mid x - 1$ then $p^k \mid x - 1$. So either $x \equiv 0 \mod p^k$ or $x - 1 \equiv 0 \mod p^k$, that is, $x \equiv 1 \mod p^k$.

This works because if $p^k \mid x$ (or $p^k \mid x - 1$) then $p \mid x$ (or $p \mid (x-1)$).Then, as pointed out above, p cannot divide both.

4. The system of equations

$$\begin{cases} x \equiv 13 \mod 11 \\ 3x \equiv 12 \mod 10 \\ 2x \equiv 10 \mod 6 \end{cases}$$

is equivalent to

$$\begin{cases} x \equiv 2 \mod 11 \\ x \equiv 4 \mod 10 \\ x \equiv 2 \mod 3 \end{cases}$$

The first equation follows because $13 \equiv 2 \mod 11$. The second equation is derived by multiplying by 7, because $7 \times 3 \equiv 1 \mod 10$ and $7 \times 12 \equiv 7 \times 2 \equiv 4 \mod 10$. The third equation is obtained by dividing by 2 and then using $5 \equiv 2 \mod 3$.

Write

$$m_1 = 11, \ m_2 = 10, \ m_3 = 3.$$

Then any two of m_1, m_2 and m_3 are coprime, so we know there is a solution. We have

$$x \equiv 2 \times (30^{-1} \bmod 11) \times 30 + 4 \times (33^{-1} \bmod 10) \times 33 + 2 \times (110^{-1} \bmod 3) \times 110 \bmod 330$$

$$\equiv 2 \times (8^{-1} \bmod 11) \times 30 + 4 \times (3^{-1} \bmod 10) \times 33 + 2 \times (2^{-1} \bmod 3) \times 110$$

$$\equiv 2 \times 7 \times 30 + 4 \times 7 \times 33 + 2 \times 2 \times 110 \bmod 330$$

$$\equiv 3 \times 30 - 2 \times 33 + 110 \equiv 134 \bmod 330.$$

5. Multiplying the second equation by 5 gives $x \equiv 20 \equiv 6 \mod 14$, which implies $x \equiv 6 \bmod 7$. The first equation $x \equiv 2 \mod 7$ is inconsistent with this. So the two equations together have no solution.

The solution is not clear unless the second equation is put in the form $x \equiv a \bmod 14$. this step was often missed out.

6. We have $G_3 = \{1 \bmod 3, 2 \bmod 3\}$ and $G_4 = \{1 \bmod 4, 3 \bmod 4\}$ since 1 and 3 are the two integers ≥ 1 and ≤ 3 which are coprime to 4. Similarly we have

$$G_{12} = \{1 \bmod 12, 5 \bmod 12, 7 \bmod 12, 11 \bmod 12\}$$

since 1, 5, 7 and 11 are the four integers ≥ 1 and ≤ 11 which are coprime to 12. The isomorphism ψ between G_{12} and $G_3 \times G_4$ is given by

$$\psi(a \bmod 12) = (a \bmod 3, a \bmod 4).$$

Writing a for $a \bmod 12$ and (b, c) for $(b \bmod 3, c \bmod 4)$, we have

$$\psi(1) = (1,1), \quad \psi(5) = (2,1), \quad \psi(7) = (1,3), \quad \psi(11) = (2,3).$$

There seemed to be some confusion about this isomorphism ψ, because some people failed to write it down.

Now we check the multiplications. We write a for $a \bmod 12$ in the first table and (a, b) for $(a \bmod 3, b \bmod 4)$ in the second table

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

	$(1,1)$	$(2,1)$	$(1,3)$	$(2,3)$
$(1,1)$	$(1,1)$	$(2,1)$	$(1,3)$	$(2,3)$
$(2,1)$	$(2,1)$	$(1,1)$	$(2,3)$	$(1,3)$
$(1,3)$	$(1,3)$	$(2,3)$	$(1,1)$	$(2,1)$
$(2,3)$	$(2,3)$	$(1,3)$	$(2,1)$	$(1,1)$

Entries in the two multiplication tables do correspond, as required.