$\therefore\ (m+1)^{k+1} = (m+1)^k(m+1)$
$\equiv (1+mk)(m+1) \pmod{m^2}$
$\equiv m + m^2k + 1 + mk \pmod{m^2}$
$\equiv m + 0 + 1 + mk \pmod{m^2}$
$\equiv 1 + m(k+1) \pmod{m^2}$

Thus $P_1$ is true and $P_{k+1}$ is true whenever $P_k$ is true.
$\Rightarrow$ $P_n$ is true. {Principle of mathematical induction}

21 $2^{11} - 1 = (2^4)^2 \times 2^3 - 1$
$= 16^2 \times 8 - 1$
$\equiv (-7)^2 \times 8 - 1 \pmod{23}$
$\equiv 49 \times 8 - 1 \pmod{23}$
$\equiv 3 \times 8 - 1 \pmod{23}$
$\equiv 0 \pmod{23}$ $\quad\therefore\ 2^{11} - 1$ is divisible by 23.

## EXERCISE 1F.2

1 a $2x \equiv 3 \pmod 7$ has $\gcd(2, 7) = 1$
$\therefore$ we have a unique solution.
By inspection, $x \equiv 5 \pmod 7$
{as $2 \times 5 = 10 \equiv 3 \pmod 7$}

b $8x \equiv 5 \pmod{25}$ has $\gcd(8, 25) = 1$
$\therefore$ we have a unique solution.
By inspection, $x \equiv 10 \pmod{25}$
{as $8 \times 10 = 80 \equiv 5 \pmod{25}$}

c $3x \equiv 6 \pmod{12}$ has $\gcd(3, 12) = 3$ where $3 \mid 6$
$\therefore$ there are exactly 3 incongruent solutions.
Cancelling by 3 gives $x \equiv 2 \pmod 4$
$\therefore$ the solutions are $x = 2 + 4t$ where $t = 0, 1, 2$
$\therefore$ $x \equiv 2, 6,$ or $10 \pmod{12}$

d $9x \equiv 144 \pmod{99}$ has $\gcd(9, 99) = 9$
where $9 \mid 144$ $\quad\{144 = 9 \times 16\}$
$\therefore$ there are exactly 9 incongruent solutions.
Cancelling by 9 gives $x \equiv 16 \pmod{11}$
$\therefore\ x \equiv 5 \pmod{11}$
$\therefore$ the solutions are $x = 5 + 11t$
where $t = 0, 1, 2, 3, 4, 5, 6, 7, 8$
$\therefore$ $x \equiv 5, 16, 27, 38, 49, 60, 71, 82,$ or $93 \pmod{99}$

e $18x \equiv 30 \pmod{40}$ has $\gcd(18, 40) = 2$ where $2 \mid 30$
$\therefore$ there are exactly 2 incongruent solutions.
Cancelling by 2 gives $9x \equiv 15 \pmod{20}$.
By inspection, $x \equiv 15$ is a solution.
$\therefore$ the solutions are $x = 15 + 20t$ where $t = 0, 1$
$\therefore$ $x \equiv 15$ or $35 \pmod{40}$

f $3x \equiv 2 \pmod 7$ has $\gcd(3, 7) = 1$
$\therefore$ we have a unique solution.
By inspection, $x \equiv 3 \pmod 7$
{as $3 \times 3 = 9 \equiv 2 \pmod 7$}

g $15x \equiv 9 \pmod{27}$ has $\gcd(15, 27) = 3$ where $3 \mid 9$
$\therefore$ there are exactly 3 incongruent solutions.
Cancelling by 3 gives $5x \equiv 3 \pmod 9$.
By inspection, $x \equiv 6$ is a solution.
$\therefore$ the solutions are $x = 6 + 9t$ where $t = 0, 1, 2$
$\therefore$ $x \equiv 6, 15,$ or $24 \pmod{27}$

h $56x \equiv 14 \pmod{21}$ has $\gcd(56, 21) = 7$ where $7 \mid 14$
$\therefore$ there are exactly 7 incongruent solutions.
Cancelling by 7 gives $8x \equiv 2 \pmod 3$
By inspection, $x \equiv 1$ is a solution.
$\therefore$ the solutions are $x = 1 + 3t$ where
$t = 0, 1, 2, 3, 4, 5, 6$
$\therefore$ $x \equiv 1, 4, 7, 10, 13, 16,$ or $19 \pmod{21}$

2 a $x \equiv 4 \pmod 7$ has $\gcd(1, 7) = 1$
$\therefore$ a unique solution exists
$\therefore$ $x = 4$
and $\gcd(x, 7)$
$= \gcd(4, 7)$
$= 1$
$\therefore$ the statement is **true**.

b $12x \equiv 15 \pmod{35}$ has $\gcd(12, 35) = 1$
$\therefore$ a unique solution exists.
By inspection, $x = 10$
and $4(10) = 40 \equiv 5 \pmod 7$
$\therefore\ 4x \equiv 5 \pmod 7$
$\therefore$ the statement is **true**.

c $12x \equiv 15 \pmod{39}$ has $\gcd(12, 39) = 3$
$\therefore$ 3 solutions exist
and $4x \equiv 5 \pmod{(\frac{39}{3})}$
$\therefore\ 4x \equiv 5 \pmod{13}$
$\therefore$ the statement is **true**.

d $x \equiv 7 \pmod{14}$
$\Rightarrow$ $x = 7 + 14k,\ k \in \mathbb{Z}$
$\Rightarrow$ $\gcd(x, 14)$
$= \gcd(7 + 14k, 14)$
$= \gcd(7(1+2k), 2 \times 7)$
$= 7$
$\therefore$ the statement is **true**.

e $5x \equiv 5y \pmod{19}$ has $\gcd(5, 19) = 1$
$\Rightarrow$ $x \equiv y \pmod{19}$
$\therefore$ the statement is **true**.

f $3x \equiv y \pmod 8$
$\Rightarrow$ $5(3x) \equiv 5(y) \pmod 8$ $\quad$ {congruence law}
$\Rightarrow$ $15x - 5y = 8t,\ t \in \mathbb{Z}$
$\Rightarrow$ $5(3x - y) = 8t$
$\Rightarrow$ $5 \mid t$ $\quad$ {as $5 \nmid 8$}
$\Rightarrow$ $40 \mid 8t$
$\Rightarrow$ $15x - 5y \equiv 0 \pmod{40}$
$\Rightarrow$ $15x \equiv 5y \pmod{40}$
$\therefore$ the statement is **true**.

g $10x \equiv 10y \pmod{14}$ has $\gcd(10, 14) = 2$
$\Rightarrow$ $x \equiv y \pmod{(\frac{14}{2})}$
$\Rightarrow$ $x \equiv y \pmod 7$
$\therefore$ the statement is **true**.

h $x \equiv 41 \pmod{37}$
$\Rightarrow$ $x = 41 + 37k,\ k \in \mathbb{Z}$
$\Rightarrow$ $x \pmod{41} \equiv 37k \pmod{41}$
$\equiv 74 \pmod{41}$ when $k = 1$
$\equiv 33$
$\therefore$ the statement is **false**.

i $x \equiv 37 \pmod{40}$ and $0 \leqslant x < 40$
$\Rightarrow$ $x = 37 + 40k,\ k \in \mathbb{Z}$ and $0 \leqslant x < 40$
$\Rightarrow$ $0 \leqslant 37 + 40k < 40$
$\Rightarrow$ $40k \geqslant -37$ and $40k < 3$
$\Rightarrow$ $k \geqslant -\frac{37}{40}$ and $k < \frac{3}{40}$
$\Rightarrow$ $k = 0$
$\Rightarrow$ $x = 37$
$\therefore$ the statement is **true**.

j $15x \equiv 11 \pmod{33}$ has $\gcd(15, 33) = 3$ and $3 \nmid 11$
$\therefore$ no solutions exist for $x \in \mathbb{Z}$
$\therefore$ the statement is **true**.



## EXERCISE 1G

1 a $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod 7$
11 and 7 are relatively prime
and $M = 11 \times 7 = 77$
$\therefore$ $M_1 = \frac{77}{11} = 7$ and $M_2 = \frac{77}{7} = 11$
Now $7x_1 \equiv 1 \pmod{11} \Rightarrow x_1 = 8$ $\quad$ {inspection}
and $11x_2 \equiv 1 \pmod 7 \Rightarrow x_2 = 2$ $\quad$ {inspection}
Now $x \equiv a_1M_1x_1 + a_2M_2x_2 \pmod{77}$
$\therefore$ $x \equiv (4)(7)(8) + (3)(11)(2) \pmod{77}$
$\therefore$ $x \equiv 290 \pmod{77}$
$\therefore$ $x \equiv 59 \pmod{77}$

b $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, $x \equiv 3 \pmod 7$
where 5, 6, 7 are relatively prime and $M = 5 \times 6 \times 7 = 210$
$\therefore$ $M_1 = \frac{210}{5} = 42$, $M_2 = \frac{210}{6} = 35$, $M_3 = \frac{210}{7} = 30$
Now $42x_1 \equiv 1 \pmod 5 \Rightarrow x_1 = 3$
$35x_2 \equiv 1 \pmod 6 \Rightarrow x_2 = 5$
$30x_3 \equiv 1 \pmod 7 \Rightarrow x_3 = 4$
Now
$x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{210}$
$\therefore$ $x \equiv (1)(42)(3) + (2)(35)(5) + (3)(30)(4) \pmod{210}$
$\therefore$ $x \equiv 836 \pmod{210}$
$\therefore$ $x \equiv 206 \pmod{210}$

2 $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$
3, 5, and 7 are relatively prime and $M = 3 \times 5 \times 7 = 105$
$\therefore$ $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$
Now $35x_1 \equiv 1 \pmod 3 \Rightarrow x_1 = 2$
$21x_2 \equiv 1 \pmod 5 \Rightarrow x_2 = 1$
$15x_3 \equiv 1 \pmod 7 \Rightarrow x_3 = 1$
Now $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{105}$
$\therefore$ $x \equiv (2)(35)(2) + (3)(21)(1) + (2)(15)(1) \pmod{105}$
$\therefore$ $x \equiv 233 \pmod{105}$
$\therefore$ $x \equiv 23 \pmod{105}$
$\therefore$ $x = 23, 128, 233, 338,$ and so on.

Thus 23 is the smallest solution, and all other solutions have the form $23 + 105k$, $k \in \mathbb{N}$.

3 a $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$
2, 3, 5 are relatively prime and $M = 30$
$\therefore$ $M_1 = 15$, $M_2 = 10$, $M_3 = 6$
Now $15x_1 \equiv 1 \pmod 2 \Rightarrow x_1 = 1$
$10x_2 \equiv 1 \pmod 3 \Rightarrow x_2 = 1$
$6x_3 \equiv 1 \pmod 5 \Rightarrow x_3 = 1$
Now $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{30}$
$\therefore$ $x \equiv (1)(15)(1) + (2)(10)(1) + (3)(6)(1) \pmod{30}$
$\therefore$ $x \equiv 53 \pmod{30}$
$\therefore$ $x \equiv 23 \pmod{30}$

b $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 5$,
$x \equiv 6 \pmod 7$
2, 3, 5, and 7 are relatively prime and
$M = 2 \times 3 \times 5 \times 7 = 210$
$\therefore$ $M_1 = 105$, $M_2 = 70$, $M_3 = 42$, $M_4 = 30$
Now $105x_1 \equiv 1 \pmod 2 \Rightarrow x_1 = 1$
$70x_2 \equiv 1 \pmod 3 \Rightarrow x_2 = 1$
$42x_3 \equiv 1 \pmod 5 \Rightarrow x_3 = 3$
$30x_4 \equiv 1 \pmod 7 \Rightarrow x_4 = 4$
$\therefore$ $x \equiv (0)(105)(1) + (0)(70)(1) + (1)(42)(3)$
$+ (6)(30)(4) \pmod{210}$
$\therefore$ $x \equiv 846 \pmod{210}$
$\therefore$ $x \equiv 6 \pmod{210}$

4 a $x \equiv 4 \pmod{11}$
$\therefore$ $x = 4 + 11t,\ t \in \mathbb{Z}$
and as $x \equiv 3 \pmod 7$
then $4 + 11t \equiv 3 \pmod 7$
$\therefore$ $11t \equiv -1 \pmod 7$
$\therefore$ $11t \equiv 6 \pmod 7$
$\therefore$ $t \equiv 5 \pmod 7$
$\therefore$ $t = 5 + 7s,\ s \in \mathbb{Z}$
Thus $x = 4 + 11t$
$= 4 + 11(5 + 7s),\ s \in \mathbb{Z}$
$= 59 + 77s,\ s \in \mathbb{Z}$
$\therefore$ $x \equiv 59 \pmod{77}$
(This agrees with 1 a.)

b $x \equiv 1 \pmod 5$
$\therefore$ $x = 1 + 5r,\ r \in \mathbb{Z}$
Substituting into the 2nd congruence $x \equiv 2 \pmod 6$,
$1 + 5r \equiv 2 \pmod 6$
$\therefore$ $5r \equiv 1 \pmod 6$
$\therefore$ $r \equiv 5 \pmod 6$
$\therefore$ $r = 5 + 6s,\ s \in \mathbb{Z}$
Substituting into the 3rd congruence $x \equiv 3 \pmod 7$,
$1 + 5(5 + 6s) \equiv 3 \pmod 7$
$\therefore$ $26 + 30s \equiv 3 \pmod 7$
$\therefore$ $30s \equiv -23 \pmod 7$
$\therefore$ $2s \equiv 5 \pmod 7$
$\therefore$ $s \equiv 6 \pmod 7$
$\therefore$ $s = 6 + 7t,\ t \in \mathbb{Z}$
$\therefore$ $x = 26 + 30s$
$x = 26 + 30(6 + 7t)$
$x = 206 + 210t$
$\therefore$ $x \equiv 206 \pmod{210}$
(This agrees with 1 b.)

c $x \equiv 0 \pmod 2$
$\therefore$ $x = 0 + 2q,\ q \in \mathbb{Z}$
Substituting into the 2nd congruence $x \equiv 0 \pmod 3$,
$2q \equiv 0 \pmod 3$
$\therefore$ $q \equiv 0 \pmod 3$
$\therefore$ $q = 3r,\ r \in \mathbb{Z}$
Substituting into the 3rd congruence $x \equiv 1 \pmod 5$,
$2(3r) \equiv 1 \pmod 5$
$\therefore$ $6r \equiv 1 \pmod 5$
$\therefore$ $r \equiv 1 \pmod 5$
$\therefore$ $r = 1 + 5s,\ s \in \mathbb{Z}$
Substituting into the 4th congruence $x \equiv 6 \pmod 7$,
$6(1 + 5s) \equiv 6 \pmod 7$
$6 + 30s \equiv 6 \pmod 7$
$\therefore$ $30s \equiv 0 \pmod 7$
$\therefore$ $s \equiv 0 \pmod 7$
$\therefore$ $s = 7t$
$\therefore$ $x = 6 + 210t$
$\therefore$ $x \equiv 6 \pmod{210}$
(This agrees with 3 b.)

5 $17x \equiv 3 \pmod{210}$

As $210 = 2\times3\times5\times7$ where these factors are relatively prime, an equivalent problem is to solve simultaneously

$17x \equiv 3 \pmod 2$, $17x \equiv 3 \pmod 3$, $17x \equiv 3 \pmod 5$, and $17x \equiv 3 \pmod 7$.

$\therefore$ $x \equiv 1 \pmod 2$, $2x \equiv 0 \pmod 3$, $2x \equiv 3 \pmod 5$, and $3x \equiv 3 \pmod 7$

$\therefore$ $x \equiv 1 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 4 \pmod 5$, and $x \equiv 1 \pmod 7$.

As 2, 3, 5, and 7 are relatively prime, and $M = 210$, then $M_1 = 105$, $M_2 = 70$, $M_3 = 42$, $M_4 = 30$.

Now $105x_1 \equiv 1 \pmod 2 \Rightarrow x_1 = 1$
$70x_2 \equiv 1 \pmod 3 \Rightarrow x_2 = 1$
$42x_3 \equiv 1 \pmod 5 \Rightarrow x_3 = 3$
$30x_4 \equiv 1 \pmod 7 \Rightarrow x_4 = 4$

Thus
$x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 + a_4M_4x_4 \pmod{210}$
$\therefore$ $x \equiv (1)(105)(1) + 0 + (4)(42)(3) + (1)(30)(4) \pmod{210}$
$\therefore$ $x \equiv 729 \pmod{210}$
$\therefore$ $x \equiv 99 \pmod{210}$

6 We need to find $x$ for $x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 4$

3, 4 are relatively prime and $M = 12$

$\therefore$ $M_1 = 4$, $M_2 = 3$.

Now $4x_1 \equiv 1 \pmod 3 \Rightarrow x_1 = 1$
$3x_2 \equiv 1 \pmod 4 \Rightarrow x_2 = 3$

Now $x \equiv a_1M_1x_1 + a_2M_2x_2 \pmod{12}$
$\therefore$ $x \equiv (2)(4)(1) + (2)(3)(3) \pmod{12}$
$\therefore$ $x \equiv 26 \pmod{12}$
$\therefore$ $x \equiv 2 \pmod{12}$
$\therefore$ $x = 2 + 12k$, $k \in \mathbb{Z}$.

Thus, all integers with this property have form $2 + 12k$, $k \in \mathbb{Z}$.

7 We need to find $x$ for
$x \equiv 2 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 0 \pmod 3$

5, 7, and 3 are relatively prime and $M = 105$

$\therefore$ $M_1 = 21$, $M_2 = 15$, $M_3 = 35$.

Now $21x_1 \equiv 1 \pmod 5 \Rightarrow x_1 = 1$
$15x_2 \equiv 1 \pmod 7 \Rightarrow x_2 = 1$
$35x_3 \equiv 1 \pmod 3 \Rightarrow x_3 = 2$

$\therefore$ $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{105}$
$\therefore$ $x \equiv (2)(21)(1) + (2)(15)(1) + 0 \pmod{105}$
$\therefore$ $x \equiv 72 \pmod{105}$
$\therefore$ $x = 72 + 105k$, $k \in \mathbb{Z}$.

Thus, all integers with this property have form $72+105k$, $k \in \mathbb{Z}$.

8 We need to find $x$ for
$x \equiv 1 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 0 \pmod 4$

where 3, 5, and 4 are relatively prime and $M = 3\times5\times4 = 60$

$\therefore$ $M_1 = 20$, $M_2 = 12$, $M_3 = 15$.

Now $20x_1 \equiv 1 \pmod 3 \Rightarrow x_1 = 2$
$12x_2 \equiv 1 \pmod 5 \Rightarrow x_2 = 3$
$15x_3 \equiv 1 \pmod 4 \Rightarrow x_3 = 3$

$\therefore$ $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{60}$
$\therefore$ $x \equiv (1)(20)(2) + (3)(12)(3) + 0 \pmod{60}$
$\therefore$ $x \equiv 148 \pmod{60}$
$\therefore$ $x \equiv 28 \pmod{60}$
$\therefore$ $x = 28 + 60k$, $k \in \mathbb{Z}$.

Thus, all integers with this property are of the form $28 + 60k$, $k \in \mathbb{Z}$.

9 Let the total number of sweets be $x$.

$\therefore$ $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$,
$x \equiv 4 \pmod 5$, $x \equiv 5 \pmod 6$, $x \equiv 0 \pmod 7$.

We cannot use the Chinese Remainder Theorem here as 2, 3, 4, 5, 6, and 7 are not relatively prime. For example, $\gcd(4, 6) = 2$.

We notice that $x + 1$ is divisible by 2, 3, 4, 5, and 6

$\therefore$ $x + 1$ is divisible by 60 $\{60 = \mathrm{lcm}(2, 3, 4, 5, 6)\}$
$\therefore$ $x = -1 + 60s$, $s \in \mathbb{Z}$
$\therefore$ $x = 59, 119, 179, 239, \ldots$

We test these in order for divisibility by 7

$\therefore$ 119 is the smallest possible number of sweets.

10 Let $x$ be the number of gold coins.

Then, $x \equiv 3 \pmod{17}$, $x \equiv 10 \pmod{16}$, $x \equiv 0 \pmod{15}$

where 17, 16, and 15 are relatively prime

and $M = 17 \times 16 \times 15 = 4080$

with $M_1 = 240$, $M_2 = 255$, $M_3 = 272$.

Now $240x_1 \equiv 1 \pmod{17} \Rightarrow x_1 = 9$
$255x_2 \equiv 1 \pmod{16} \Rightarrow x_2 = 15$
$272x_3 \equiv 1 \pmod{15} \Rightarrow x_3 = 8$

Now $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{4080}$
$\therefore$ $x \equiv (3)(240)(9) + (10)(255)(15) + 0 \pmod{4080}$
$\therefore$ $x \equiv 44\,730 \pmod{4080}$
$\therefore$ $x \equiv 3930 \pmod{4080}$
$\therefore$ the smallest number of coins is 3930.

11 a $4x + 7y = 5$ .... (1)

| | |
|---|---|
| $\therefore$ $4x = 5 - 7y$ | and $7y = 5 - 4x$ |
| $\therefore$ $4x \equiv 5 \pmod 7$ | $\therefore$ $7y \equiv 5 \pmod 4$ |
| $\therefore$ $x \equiv 3 \pmod 7$ | $\therefore$ $3y \equiv 1 \pmod 4$ |
| $\therefore$ $x = 3 + 7t$, $t \in \mathbb{Z}$ | $\therefore$ $y \equiv 3 \pmod 4$ |
| | $\therefore$ $y = 3 + 4s$, $s \in \mathbb{Z}$ |

and so in (1), $4(3 + 7t) + 7(3 + 4s) = 5$
$\therefore$ $12 + 28t + 21 + 28s = 5$
$\therefore$ $28(s + t) = 5 - 33$
$\therefore$ $28(s + t) = -28$
$\therefore$ $s + t = -1$

Thus $y = 3 + 4(-1 - t)$
$\therefore$ $y = -1 - 4t$
$\therefore$ $x = 3 + 7t$, $y = -1 - 4t$, $t \in \mathbb{Z}$.

b i $11x + 8y = 31$ and $8y = 31 - 11x$

| | |
|---|---|
| $\therefore$ $11x = 31 - 8y$ | $\therefore$ $8y \equiv 31 \pmod{11}$ |
| $\therefore$ $11x \equiv 31 \pmod 8$ | $\therefore$ $8y \equiv 9 \pmod{11}$ |
| $\therefore$ $3x \equiv 7 \pmod 8$ | $\therefore$ $y \equiv 8 \pmod{11}$ |
| $\therefore$ $x \equiv 5 \pmod 8$ | $\therefore$ $y = 8 + 11s$, $s \in \mathbb{Z}$ |
| $\therefore$ $x = 5 + 8t$, $t \in \mathbb{Z}$ | |

But $11x + 8y = 31$
$\therefore$ $55 + 88t + 64 + 88s = 31$
$\therefore$ $88(s + t) = -88$
$\therefore$ $s + t = -1$
$\therefore$ $s = -1 - t$
$\therefore$ $y = 8 + 11(-1 - t)$
$\therefore$ $y = -3 - 11t$
$\therefore$ $x = 5 + 8t$, $y = -3 - 11t$, $t \in \mathbb{Z}$.



ii $7x + 5y = 13$

| | |
|---|---|
| $\therefore$ $7x = 13 - 5y$ | and $5y = 13 - 7x$ |
| $\therefore$ $7x \equiv 13 \pmod 5$ | $\therefore$ $5y \equiv 13 \pmod 7$ |
| $\therefore$ $2x \equiv 3 \pmod 5$ | $\therefore$ $5y \equiv 6 \pmod 7$ |
| $\therefore$ $x \equiv 4 \pmod 5$ | $\therefore$ $y \equiv 4 \pmod 7$ |
| $\therefore$ $x = 4 + 5t$, $t \in \mathbb{Z}$ | $\therefore$ $y = 4 + 7s$, $s \in \mathbb{Z}$ |

But $7x + 5y = 13$
$\therefore$ $28 + 35t + 20 + 35s = 13$
$\therefore$ $35(s + t) = -35$
$\therefore$ $s + t = -1$
$\therefore$ $s = -1 - t$
$\therefore$ $y = 4 + 7(-1 - t)$
$\therefore$ $y = -3 - 7t$
$\therefore$ $x = 4 + 5t$, $y = -3 - 7t$, $t \in \mathbb{Z}$.

12 $2 \mid a$, $3 \mid (a + 1)$, $4 \mid (a + 2)$, $5 \mid (a + 3)$, $6 \mid (a + 4)$

$\therefore$ $a \equiv 0 \pmod 2$, $a + 1 \equiv 0 \pmod 3$, $a + 2 \equiv 0 \pmod 4$, $a + 3 \equiv 0 \pmod 5$, $a + 4 \equiv 0 \pmod 6$

$\therefore$ $a$ is even and $a \equiv 2$ (mod 3, 4, 5, or 6)
$\therefore$ $a$ is even and $a = 2 + 60t$, $t \in \mathbb{Z}$ $\{60 = \mathrm{lcm}(3, 4, 5, 6)\}$
$\therefore$ $a = 62, 122, 182, \ldots$
$\therefore$ the smallest $a$ is 62.

**Note:** As the divisors 2, 3, 4, 5, and 6 are not relatively prime the Chinese Remainder Theorem may not be appropriate.

13 $2x \equiv 1 \pmod 5$, $3x \equiv 9 \pmod 6$, $4x \equiv 1 \pmod 7$, and $5x \equiv 9 \pmod{11}$

$\therefore$ $x \equiv 3 \pmod 5$, $\underset{\substack{\uparrow \\ \text{on cancellation}}}{x \equiv 3 \pmod 2}$, $x \equiv 2 \pmod 7$,

$x \equiv 4 \pmod{11}$ where 5, 2, 7, and 11 are relatively prime.

$M = 770$

$\therefore$ $M_1 = 154$, $M_2 = 385$, $M_3 = 110$, $M_4 = 70$

Now $154x_1 \equiv 1 \pmod 5$
$\therefore$ $4x_1 \equiv 1 \pmod 5$
$\therefore$ $x_1 = 4$
$385x_2 \equiv 1 \pmod 2$
$\therefore$ $x_2 \equiv 1 \pmod 2$
$\therefore$ $x_2 = 1$
$110x_3 \equiv 1 \pmod 7$
$\therefore$ $5x_3 \equiv 1 \pmod 7$
$\therefore$ $x_3 = 3$
$70x_4 \equiv 1 \pmod{11}$
$\therefore$ $4x_4 \equiv 1 \pmod{11}$
$\therefore$ $x_4 = 3$

Thus $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 + a_4M_4x_4 \pmod{770}$
$\therefore$ $x \equiv (3)(154)(4) + (3)(385)(1) + (2)(110)(3) + (4)(70)(3) \pmod{770}$
$\therefore$ $x \equiv 4503 \pmod{770}$
$\therefore$ $x \equiv 653 \pmod{770}$.

## EXERCISE 1H

1 $A \pmod 2 = 1 \longleftarrow$ remainder
$A \pmod 3 = 1 \longleftarrow$ remainder
{The digit sum is $52 \equiv 1 \pmod 3$}

$A \pmod 5 = 2$ {it ends in 7}
$A \pmod 9 = 7 \longleftarrow$ remainders
{The digit sum is $52 \equiv 7 \pmod 9$}
$A \pmod{11} = 0$
$\therefore$ $A$ is divisible by 11
{sum of digits in odd positions − sum of digits in even positions
$= 26 - 26$
$= 0$ which is a multiple of 11}

2 a i $a_i10^i \equiv 0 \pmod{10}$ for $i \geqslant 1$
$\therefore$ $A \pmod{10} = 0 + 0 + \ldots + 0 + a_0$
$= a_0$

ii $a_i10^i \equiv 0 \pmod{100}$ for $i \geqslant 2$
$\therefore$ $A \pmod{100} = 0 + 0 + \ldots + 0 + a_110 + a_0$
$= 10a_1 + a_0$

iii $a_i10^i \equiv 0 \pmod{1000}$ for $i \geqslant 3$
$\therefore$ $A \pmod{1000}$
$= 0 + 0 + \ldots + 0 + a_210^2 + a_110 + a_0$
$= 100a_2 + 10a_1 + a_0$

b $A$ is divisible by 10 if it ends in 0
$A$ is divisible by 100 if it ends in 00
$A$ is divisible by 1000 if it ends in 000.

3 $A = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \ldots + a_210^2 + a_110 + a_0$

a $4 \mid A \Leftrightarrow 4 \mid 10a_1 + a_0$
$\Leftrightarrow 4 \mid 2a_1 + a_0$
$\{10^k$ for $k \geqslant 2$ are all divisible by 4$\}$

$8 \mid A \Leftrightarrow 8 \mid 4a_2 + 2a_1 + a_0$

**Proof:**
$a_i10^i \equiv 0 \pmod 8$ for $i \geqslant 3$
$\therefore$ $A \pmod 8 = 100a_2 + 10a_1 + a_0$
$= 4a_2 + 2a_1 + a_0$
$\therefore$ $8 \mid A \Leftrightarrow 8 \mid (4a_2 + 2a_1 + a_0)$

b $A$ is divisible by 16 $\Leftrightarrow 16 \mid (8a_3 + 4a_2 + 2a_1 + a_0)$

c i $2^8$ ii $2^3$ iii $2^{10}$ iv $2^1$ v $2^4$ vi $2^4$

4 a $n \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \pmod{10}$
$\therefore$ $n^2 \equiv 0, 1, 4, 9, 6, 5, 6, 9, 4, 1 \pmod{10}$
$\Rightarrow$ $n^2 \equiv 0, 1, 4, 5, 6$, or $9 \pmod{10}$

b From a, an integer can be a perfect square if it ends in 0, 1, 4, 5, 6, or 9.
Thus none of the given integers can be a perfect square.

5 $\sum_{r=1}^{4} r! = 1! + 2! + 3! + 4!$
$= 33$ which is not a square

$\sum_{r=1}^{5} r! = 33 + 5!$
$= 33 + 120$
$= 153$ which is not a square

Since $n!$ ends in 0 for all $n \geqslant 5$, $\sum_{r=1}^{n} n!$ ends in 3 for all $n \geqslant 5$.

From a, any such number cannot be square, so Claudia is correct.

6 $R_k = \underbrace{111\,111\,11\ldots1}_{k \text{ 1s}}$

a $R_k$ is divisible by 3 if $k = 3n$, $n \in \mathbb{Z}^+$.
For example, $R_6 = 111\,111$ and the sum of its digits is 6 and $3 \mid 6$.

b $R_k$ is divisible by 9 if $k = 9n,\ n \in \mathbb{Z}^+$.

c $R_k$ is divisible by 11 if $k = 2n,\ n \in \mathbb{Z}^+$.
For example, $111\,111 = 11 \times 10\,101$.

7 a $7 \mid 6994 \Leftrightarrow 7 \mid 699 - 2(4)$
$\Leftrightarrow 7 \mid 691$
$\Leftrightarrow 7 \mid 69 - 2(1)$
$\Leftrightarrow 7 \mid 67$
which is not true.
So, $7 \nmid 6994$.
$7 \mid 6993 \Leftrightarrow 7 \mid 699 - 2(3)$
$\Leftrightarrow 7 \mid 693$
$\Leftrightarrow 7 \mid 69 - 2(3)$
$\Leftrightarrow 7 \mid 63$
which is true.
So, $7 \mid 6993$.

b $13 \mid 6994 \Leftrightarrow 13 \mid 699 - 9(4)$
$\Leftrightarrow 13 \mid 663$
$\Leftrightarrow 13 \mid 66 - 9(3)$
$\Leftrightarrow 13 \mid 39$
which is true.
So, $13 \mid 6994$.
$13 \mid 6993 \Leftrightarrow 13 \mid 699 - 9(3)$
$\Leftrightarrow 13 \mid 672$
$\Leftrightarrow 13 \mid 67 - 9(2)$
$\Leftrightarrow 13 \mid 49$
which is not true.
So, $13 \nmid 6993$.

8 Let $c = (a_{n-1}a_{n-2}....a_3a_2a_1)$
$\therefore\ A = 10c + a_0$
$\therefore\ -9A = -90c - 9a_0$
$\therefore\ -9A \equiv c - 9a_0 \pmod{13}$
Thus $13 \mid A \Leftrightarrow 13 \mid -9A$
$\Leftrightarrow 13 \mid c - 9a_0$
$\Leftrightarrow 13 \mid ((a_{n-1}a_{n-2}....a_2a_1) - 9a_0)$

9 a i An integer is divisible by 25 if $(a_1a_0)$ is divisible by 25.
ii An integer is divisible by 125 if $(a_2a_1a_0)$ is divisible by 125.

b i $5^3$ ii $5^1$ iii $5^9$

10 a An integer is divisible by 6 if it is divisible by both 2 and 3.
b An integer is divisible by 12 if it is divisible by both 4 and 3.
c An integer is divisible by 14 if it is divisible by both 2 and 7.
d An integer is divisible by 15 if it is divisible by both 3 and 5.

11 a $(1+7+3+3)-(0+6+7+2)$
$= 14 - 15$
$= -1$ which is not divisible by 11
$\therefore$ the number is not divisible by 11.

b $(8+2+3+0+6+5+8)-(9+4+4+1+0+4+3)$
$= 32 - 21$
$= 11$ which is divisible by 11
$\therefore$ the number is divisible by 11.

c $(1+8+3+6+1)-(0+6+2+7+5)$
$= 19 - 20$
$= -1$ which is not a multiple of 11
$\therefore$ the number is not divisible by 11.

12 a $A = 201\,984$
- sum of digits $= 2+0+1+9+8+4$
$= 24$ where $3 \mid 24$
$\therefore\ A$ is divisible by 3.
- sum of digits $= 24$ and $9 \nmid 24$
$\therefore\ A$ is not divisible by 9.
- $(2+1+8)-(0+9+4)$
$= 11 - 13$
$= -2$ which is not a multiple of 11
$\therefore\ A$ is not divisible by 11

b $A = 101\,582\,283$
- sum of digits $= 1+0+1+5+8+2+2+8+3$
$= 30$ and $3 \mid 30$
$\therefore\ A$ is divisible by 3.
- sum of digits $= 30$ and $9 \nmid 30$
$\therefore\ A$ is not divisible by 9.
- $(1+1+8+2+3)-(0+5+2+8)$
$= 15 - 15$
$= 0$ which is a multiple of 11
$\therefore\ A$ is divisible by 11.

c $A = 41\,578\,912\,245$
- sum of digits $= 48$ and $3 \mid 48$ and $9 \nmid 48$
$\therefore\ A$ is divisible by 3 but not by 9.
- $(4+5+8+1+2+5)-(1+7+9+2+4)$
$= 25 - 23$
$= 2$ which is not a multiple of 11
$\therefore\ A$ is not divisible by 11.

d $A = 10\,415\,486\,358$
- sum of digits $= 45$ and $3 \mid 45$ and $9 \mid 45$
$\therefore\ A$ is divisible by 3 and 9.
- $(1+4+5+8+3+8)-(0+1+4+6+5)$
$= 29 - 16$
$= 13$ and $11 \nmid 13$
$\therefore\ A$ is not divisible by 11.

13 $n \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \pmod{10}$
$\therefore\ n(n-1) \equiv 0, 0, 2, 6, 2, 0, 0, 2, 6, 2 \pmod{10}$
$\therefore\ n^2 - n \equiv 0, 2, 6 \pmod{10}$
$\therefore\ n^2 - n + 7 \equiv 7, 9, 3 \pmod{10}$
$\therefore\ n^2 - n + 7$ has a last digit of 3, 7, or 9.

14 a i $A = 101\,110\,101\,001$
$= 2^{11} + 2^9 + 2^8 + 2^7 + 2^5 + 2^3 + 1$
which is odd $\therefore$ highest power of 2 is $2^0$.

ii **Note:**

| $2^{2n}$ | $2^{2n+1}$ |
|---|---|
| $= 4^n$ | $= 4^n \times 2$ |
| $\equiv 1^n \pmod 3$ | $\equiv 1 \times 2 \pmod 3$ |
| $\equiv 1 \pmod 3$ | $\equiv 2 \pmod 3$ |

$\therefore\ A \equiv 2+2+1+2+2+2+1 \pmod 3$
$\therefore\ A \equiv 12 \pmod 3$
$\therefore\ A \equiv 0 \pmod 3$
$\therefore\ A$ is divisible by 3.

b i $A = 1\,001\,110\,101\,000$
$= 2^{12} + 2^9 + 2^8 + 2^7 + 2^5 + 2^3$
$= 2^3\underbrace{(2^9 + 2^6 + 2^5 + 2^4 + 2^2 + 1)}_{\text{odd}}$
$\therefore$ highest power of 2 is $2^3$.

ii $A \equiv 1+2+1+2+2+2 \pmod 3$
$\therefore\ A \equiv 10 \pmod 3$
$\therefore\ A \equiv 1 \pmod 3$
$\therefore\ A$ is not divisible by 3.

c i $A = 1\,010\,101\,110\,100\,100$
$= 2^{15} + 2^{13} + 2^{11} + 2^9 + 2^8 + 2^7 + 2^5 + 2^2$
$= 2^2\underbrace{(2^{13} + 2^{11} + 2^9 + 2^7 + 2^6 + 2^5 + 2^3 + 1)}_{\text{odd}}$
$\therefore$ highest power of 2 is $2^2$.

ii $A \equiv 2+2+2+2+1+2+2+1 \pmod 3$
$\therefore\ A \equiv 14 \pmod 3$
$\therefore\ A \equiv 2 \pmod 3$
$\therefore\ A$ is not divisible by 3.

**Note:** The highest power of 2 that divides a binary number is $2^n$, where $n$ is the number of 0s at the end of the number.

15 a i $A = 10\,200\,122\,221\,210$
$A = (3^{13}) + 2(3^{11}) + (3^8) + 2(3^7) + 2(3^6) + 2(3^5) + 2(3^4) + (3^3) + 2(3^2) + 3^1$
$\therefore$ highest power of 3 is $3^1$.

ii **Note:** $3^n \equiv 1^n \pmod 2$
$\therefore\ 3^n \equiv 1 \pmod 2$ for all $n \in \mathbb{N}$
$\therefore\ A \equiv 1+2+1+2+2+2+2+1+2+1 \pmod 2$
$\equiv 16 \pmod 2$
$\equiv 0 \pmod 2$
$\therefore\ A$ is divisible by 2.

iii **Note:**

| $3^{2n}$ | $3^{2n+1}$ |
|---|---|
| $= 9^n$ | $= 9^n \times 3$ |
| $\equiv 1^n \pmod 4$ | $\equiv 1 \times 3 \pmod 4$ |
| $\equiv 1 \pmod 4$ | $\equiv 3 \pmod 4$ |

$\therefore\ A \equiv 3 + 2(3) + 1 + 2(3) + 2(1) + 2(3) + 2(1) + 3 + 2(1) + 3 \pmod 4$
$\therefore\ A \equiv 34 \pmod 4$
$\therefore\ A \equiv 2 \pmod 4$
$\therefore\ A$ is not divisible by 4.

b i $A = 221\,021\,010\,020\,120$
$\therefore\ A = 2(3^{14}) + 2(3^{13}) + 3^{12} + 2(3^{10}) + 3^9 + 3^7 + 2(3^4) + 3^2 + 2(3)$
$\therefore$ highest power of 3 is $3^1$.

ii $A \equiv 2+2+1+2+1+1+2+1+2 \pmod 2$
$\equiv 14 \pmod 2$
$\equiv 0 \pmod 2$
$\therefore\ A$ is divisible by 2.

iii $A \equiv 2(1) + 2(3) + 1 + 2(1) + 3 + 3 + 2(1) + 1 + 2(3) \pmod 4$
$\equiv 26 \pmod 4$
$\equiv 2 \pmod 4$
$\therefore\ A$ is not divisible by 4.

c i $A = 1\,010\,101\,110\,100\,100$
$= 3^{15} + 3^{13} + 3^{11} + 3^9 + 3^8 + 3^7 + 3^5 + 3^2$
$\therefore$ highest power of 3 is $3^2$.

ii $A \equiv 8 \pmod 2$
$\therefore\ A \equiv 0 \pmod 2$
$\therefore\ A$ is divisible by 2.

iii $A \equiv 3+3+3+3+1+3+3+1 \pmod 4$
$\equiv 20 \pmod 4$
$\equiv 0 \pmod 4$
$\therefore\ A$ is divisible by 4.

16 Let
$A = a_{n-1}8^{n-1} + a_{n-2}8^{n-2} + .... + a_38^3 + a_28^2 + a_18 + a_0$
Now $8^k \equiv 1^k \pmod 7$
$\therefore\ 8^k \equiv 1 \pmod 7$ for all $k = 1, 2, ...., n-1$
$\therefore\ A \equiv a_{n-1} + a_{n-2} + .... + a_3 + a_2 + a_1 + a_0 \pmod 7$
$\therefore\ A$ is divisible by 7 if the sum of its digits is divisible by 7.
*Generalisation*: If $A$ is a base $n$ number, $A$ is divisible by $n-1$ if the sum of its digits is divisible by $n-1$.

17 Let
$A = a_{n-1}8^{n-1} + a_{n-2}8^{n-2} + .... + a_38^3 + a_28^2 + a_18 + a_0$
Now $8 \equiv (-1) \pmod 9$
$\therefore\ 8^{2k} \equiv (-1)^{2k} \pmod 9$
$\therefore\ 8^{2k} \equiv 1 \pmod 9$
and $8^{2k+1} \equiv -1 \pmod 9$
$\therefore\ A \equiv a_0 - a_1 + a_2 - a_3 + a_4 - .... \pmod 9$
$\therefore\ A \equiv [a_0 + a_2 + a_4 + ....] - [a_1 + a_3 + a_5 + ....] \pmod 9$
$\therefore\ A$ is divisible by 9 if the sum of the digits in the even positions minus the sum of the digits in the odd positions is divisible by 9.
*Generalisation:*
If $A$ is a base $n$ number, $A$ is divisible by $n+1$ if the sum of the digits in the even positions minus the sum of the digits in the odd positions is divisible by $n+1$.

18 a $X = (x_nx_{n-1}x_{n-2}....x_3x_2x_1x_0)_{25}$
$= x_n25^n + x_{n-1}25^{n-1} + .... + x_225^2 + x_125 + x_0$
Now $25^k \equiv 0 \pmod 5$ for all $k = 1, 2, ...., n$
$\therefore\ X \equiv x_0 \pmod 5$
$\therefore\ X$ is divisible by 5 if $x_0$ is divisible by 5.

b As $25 \equiv 1 \pmod 2$
then $25^k \equiv 1 \pmod 2$ for all $k = 1, 2, ...., n$
$\therefore\ X \equiv x_n + x_{n-1} + .... + x_2 + x_1 + x_0 \pmod 2$
$\therefore\ X$ is divisible by 2 if the sum of its digits is divisible by 2.

c As $25 \equiv 1 \pmod 4$
then $25^k \equiv 1 \pmod 4$ for all $k = 1, 2, ...., n$
$\therefore\ X \equiv x_n + x_{n-1} + .... + x_2 + x_1 + x_0 \pmod 4$
$\therefore\ X$ is divisible by 4 if the sum of its digits is divisible by 4.
Now if $X = (664\,089\,735)_{25}$
we see that $5 \mid X$ $\{$as $x_0 = 5\}$
Also the sum of the digits of $X$ is
$6+6+4+0+8+9+7+3+5 = 48$ where $4 \mid 48$
$\therefore\ 4 \mid X$
As $\gcd(4, 5) = 1$ and $4 \mid X,\ 5 \mid X$ then $4 \times 5 \mid X$
$\therefore\ 20 \mid X$

## EXERCISE 1I

1 a $5^{152} \pmod{13}$
$\equiv (5^{12})^{12} \times 5^8 \pmod{13}$
$\equiv 1^{12} \times 25^4 \pmod{13}$ {FLT}
$\equiv 1 \times (-1)^4 \pmod{13}$
$\equiv 1 \pmod{13}$

b $4^{56} \pmod 7$
$\equiv (4^6)^9 \times 4^2 \pmod 7$
$\equiv 1^9 \times 16 \pmod 7$ {FLT}
$\equiv 1 \times 2 \pmod 7$
$\equiv 2 \pmod 7$

c $8^{205} \pmod{17}$
$\equiv (8^{16})^{12} \times 8^{13} \pmod{17}$
$\equiv 1^{12} \times 64^6 \times 8 \pmod{17}$ {FLT}
$\equiv 1 \times (-4)^6 \times 8 \pmod{17}$ $\{17 \times 4 = 68\}$
$\equiv 16^3 \times 8 \pmod{17}$
$\equiv (-1)^3 \times 8 \pmod{17}$
$\equiv -8 \pmod{17}$
$\equiv 9 \pmod{17}$

d $3^{95} \pmod{13}$
$\equiv (3^{12})^7 \times 3^{11} \pmod{13}$
$\equiv 1^7 \times (3^3)^3 \times 3^2 \pmod{13}$ {FLT}
$\equiv 1 \times 27^3 \times 9 \pmod{13}$
$\equiv 1^3 \times 9 \pmod{13}$
$\equiv 9 \pmod{13}$

2 a $3x \equiv 5 \pmod 7$ where $7 \nmid 3$
$\therefore\ x \equiv 3^5 \times 5 \pmod 7$
$\therefore\ x \equiv (3^2)^2 \times 15 \pmod 7$
$\therefore\ x \equiv 2^2 \times 1 \pmod 7$
$\therefore\ x \equiv 4 \pmod 7$

b $8x \equiv 3 \pmod{13}$ where $13 \nmid 8$
$\therefore\ x \equiv 8^{11} \times 3 \pmod{13}$
$\therefore\ x \equiv (8^2)^5 \times 24 \pmod{13}$
$\therefore\ x \equiv 64^5 \times (-2) \pmod{13}$
$\therefore\ x \equiv (-1)^5 \times (-2) \pmod{13}$ $\{65 = 13 \times 5\}$
$\therefore\ x \equiv 2 \pmod{13}$

c $7x \equiv 2 \pmod{11}$ where $11 \nmid 7$
$\therefore\ x \equiv 7^9 \times 2 \pmod{11}$
$\therefore\ x \equiv (7^2)^4 \times 14 \pmod{11}$
$\therefore\ x \equiv 49^4 \times 3 \pmod{11}$
$\therefore\ x \equiv 5^4 \times 3 \pmod{11}$
$\therefore\ x \equiv (25)^2 \times 3 \pmod{11}$
$\therefore\ x \equiv 3^2 \times 3 \pmod{11}$
$\therefore\ x \equiv 27 \pmod{11}$
$\therefore\ x \equiv 5 \pmod{11}$

d $4x \equiv 3 \pmod{17}$ where $17 \nmid 4$
$\therefore\ x \equiv 4^{15} \times 3 \pmod{17}$
$\therefore\ x \equiv (4^2)^7 \times 12 \pmod{17}$
$\therefore\ x \equiv 16^7 \times 12 \pmod{17}$
$\therefore\ x \equiv (-1)^7 \times 12 \pmod{17}$
$\therefore\ x \equiv -12 \pmod{17}$
$\therefore\ x \equiv 5 \pmod{17}$

3 a $2^{63} = (2^6)^{10} \times 2^3$
$= (64)^{10} \times 8$
$\equiv 1^{10} \times 8 \pmod{63}$
$\equiv 8 \pmod{63}$
$\not\equiv 2 \pmod{63}$ $\therefore$ 63 is not prime.

b $2^{117} = (2^7)^{16} \times 2^5$ $\{2^7 \equiv 128$ is close to $117\}$
$\equiv 11^{16} \times 2^5 \pmod{117}$
$\equiv 121^8 \times 2^5 \pmod{117}$
$\equiv 4^8 \times 2^5 \pmod{117}$
$\equiv 2^{21} \pmod{117}$
$\equiv (2^7)^3 \pmod{117}$
$\equiv 11^3 \pmod{17}$
$\equiv 121 \times 11 \pmod{117}$
$\equiv 4 \times 11 \pmod{117}$
$\equiv 44 \pmod{117}$
$\not\equiv 2 \pmod{117}$ $\therefore$ 117 is not prime.

c $2^{29} = (2^5)^5 \times 2^4$
$= 32^5 \times 16$
$\equiv 3^5 \times 16 \pmod{29}$
$\equiv 3^3 \times 3^2 \times 16 \pmod{29}$
$\equiv -2 \times 144 \pmod{29}$
$\equiv -2 \times -1 \pmod{29}$ $\{29 \times 5 = 145\}$
$\equiv 2 \pmod{29}$

This **does not** prove that 29 is a prime, as there exist Carmichael numbers which are composite and $a^n \equiv a \pmod n$.
{See note on page 84}

4 $3^{10} = (3^2)^5$
$= 9^5$
$\equiv (-2)^5 \pmod{11}$
$\equiv -32 \pmod{11}$
$\equiv 1 \pmod{11}$ $\{33 = 3 \times 11\}$

5 19 is prime and $19 \nmid 13$.
$\therefore\ 13^{18} \equiv 1 \pmod{19}$ {FLT} .... $(*)$
Thus $13^{133} + 5$
$= (13^{18})^7 \times 13^7 + 5$
$\equiv 1^7 \times 13^7 + 5 \pmod{19}$ {from $*$}
$\equiv (13^2)^3 \times 13 + 5 \pmod{19}$
$\equiv (-2)^3 \times 13 + 5 \pmod{19}$ $\{171 = 9 \times 19\}$
$\equiv -8 \times 13 + 5 \pmod{19}$
$\equiv -99 \pmod{19}$
$\equiv 15 \pmod{19}$
$\therefore$ the remainder is 15.

6 a 13 is a prime and $13 \nmid 11$
$\therefore\ 11^{12} \equiv 1 \pmod{13}$ {FLT} .... $(*)$
Thus $11^{204} + 1$
$= (11^{12})^{17} + 1$
$\equiv 1^{17} + 1 \pmod{13}$ {using $*$}
$\equiv 2 \pmod{13}$
$\not\equiv 0 \pmod{13}$
$\therefore\ 11^{204} + 1$ is not divisible by 13.

b 17 is a prime and $17 \nmid 11$
$\therefore\ 11^{16} \equiv 1 \pmod{17}$ {FLT} .... $(*)$
Thus $11^{204} + 1$
$= (11^{16})^{12} \times 11^{12} + 1$
$\equiv 1^{12} \times (121)^6 + 1 \pmod{17}$ {using $*$}
$\equiv 2^6 + 1 \pmod{17}$ $\{17 \times 7 = 119\}$
$\equiv 65 \pmod{17}$
$\equiv 14 \pmod{17}$
$\not\equiv 0 \pmod{17}$
$\therefore\ 11^{204} + 1$ is not divisible by 17.

7 a $13^{16n+2} + 1$
$= (13^{16})^n \times 13^2 + 1$
$\equiv 1^n \times 169 + 1 \pmod{17}$ {FLT}
$\equiv 170 \pmod{17}$
$\equiv 0 \pmod{17}$
$\therefore\ 17 \mid (13^{16n+2} + 1),\ n \in \mathbb{Z}^+$.

b $9^{12n+4} - 9$
$= (9^{12})^n \times 9^4 - 9$
$\equiv 1^n \times (-4)^4 - 9 \pmod{13}$ {FLT}
$\equiv 247 \pmod{13}$
$\equiv 0 \pmod{13}$ $\{247 = 19 \times 13\}$
$\therefore\ 13 \mid (9^{12n+4} - 9),\ n \in \mathbb{Z}^+$.

8 $7^{100} = (7^2)^{50}$
$= 49^{50}$
$\equiv (-1)^{50} \pmod{10}$
$\equiv 1 \pmod{10}$
$\therefore$ the units digit is 1.
**Note:** As 10 is not prime we cannot use FLT.

9 a If $x \equiv a^{p-2} b \pmod p$
then $ax \equiv a^{p-1} b \pmod p$
$\therefore\ ax \equiv (1)b \pmod p$ {FLT}
$\therefore\ ax \equiv b \pmod p$ is verified.

b i $7x \equiv 12 \pmod{17}$
$\therefore\ x \equiv 7^{15} \times 12 \pmod{17}$
$\therefore\ x \equiv (49)^7 \times 7 \times 12 \pmod{17}$
$\therefore\ x \equiv (-2)^7 \times 84 \pmod{17}$ $\{17 \times 3 = 51\}$
$\therefore\ x \equiv 32 \times -4 \times 84 \pmod{17}$
$\therefore\ x \equiv -2 \times -4 \times -1 \pmod{17}$ $\{17 \times 5 = 85\}$
$\therefore\ x \equiv -8 \pmod{17}$
$\therefore\ x \equiv 9 \pmod{17}$
Also $4x \equiv 11 \pmod{19}$
$\therefore\ x \equiv 4^{17} \times 11 \pmod{19}$
$\therefore\ x \equiv 16^8 \times 4 \times 11 \pmod{19}$
$\therefore\ x \equiv (-3)^8 \times 6 \pmod{19}$ $\{19 \times 2 = 38\}$
$\therefore\ x \equiv (81)^2 \times 6 \pmod{19}$
$\therefore\ x \equiv 5^2 \times 6 \pmod{19}$ $\{19 \times 4 = 76\}$
$\therefore\ x \equiv 150 \pmod{19}$
$\therefore\ x \equiv 17 \pmod{19}$ $\{19 \times 7 = 133\}$
Using the Chinese Remainder Theorem, for
$x \equiv 9 \pmod{17},\ x \equiv 17 \pmod{19}$
$M = 17 \times 19 = 323$
$\therefore\ M_1 = 19,\ M_2 = 17.$
Now $19x_1 \equiv 1 \pmod{17}$
$\Rightarrow\ 2x_1 \equiv 1 \pmod{17}$
$\Rightarrow\ x_1 = 9$
and $17x_2 \equiv 1 \pmod{19}$
$\Rightarrow\ -2x_2 \equiv 1 \pmod{19}$
$\Rightarrow\ x_2 = 9$
$\therefore$ the solution is
$x \equiv a_1 M_1 x_1 + a_2 M_2 x_2 \pmod{323}$
$\therefore\ x \equiv (9)(19)(9) + (17)(17)(9) \pmod{323}$
$\therefore\ x \equiv 4140 \pmod{323}$
$\therefore\ x \equiv 264 \pmod{323}$

ii $2x \equiv 1 \pmod{31}$
$\therefore\ x \equiv 2^{29} \times 1 \pmod{31}$
$\therefore\ x \equiv (2^5)^5 \times 2^4 \pmod{31}$
$\therefore\ x \equiv 1^5 \times 16 \pmod{31}$
$\therefore\ x \equiv 16 \pmod{31}$
and $6x \equiv 5 \pmod{11}$
$\therefore\ x \equiv 6^9 \times 5 \pmod{11}$
$\therefore\ x \equiv (6^2)^4 \times 30 \pmod{11}$
$\therefore\ x \equiv 3^4 \times (-3) \pmod{11}$
$\therefore\ x \equiv 3^3 \times -9 \pmod{11}$
$\therefore\ x \equiv 5 \times 2 \pmod{11}$
$\therefore\ x \equiv 10 \pmod{11}$
also $3x \equiv 17 \pmod{29}$
$\therefore\ x \equiv 3^{27} \times 17 \pmod{29}$
$\therefore\ x \equiv (3^3)^9 \times 17 \pmod{29}$
$\therefore\ x \equiv (-2)^9 \times 17 \pmod{29}$
$\therefore\ x \equiv -32 \times 16 \times 17 \pmod{29}$
$\therefore\ x \equiv -3 \times 16 \times 17 \pmod{29}$
$\therefore\ x \equiv -24 \times 34 \pmod{29}$
$\therefore\ x \equiv 5 \times 5 \pmod{29}$
$\therefore\ x \equiv 25 \pmod{29}$
Using the Chinese Remainder Theorem, as 31, 11, and 29 are relatively prime
$M = 31 \times 11 \times 29 = 9889$
$M_1 = 319,\ M_2 = 899,\ M_3 = 341.$
Now $319x_1 \equiv 1 \pmod{31}$
$\Rightarrow\ 9x_1 \equiv 1 \pmod{31}$
$\Rightarrow\ x_1 = 7$
and $899x_2 \equiv 1 \pmod{11}$
$\Rightarrow\ 8x_2 \equiv 1 \pmod{11}$
$\Rightarrow\ x_2 = 7$
and $341x_3 \equiv 1 \pmod{29}$
$\Rightarrow\ 22x_3 \equiv 1 \pmod{29}$
$\Rightarrow\ x_3 = 4$
$\therefore\ x \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 \pmod{9889}$
$\therefore\ x \equiv (16)(319)(7) + (10)(899)(7)$
$+ (25)(341)(4) \pmod{9889}$
$\therefore\ x \equiv 132\,758 \pmod{9889}$
$\therefore\ x \equiv 4201 \pmod{9889}$

10 a Since $p$ is an odd prime, then
$1 \leqslant k \leqslant p-1 \ \Rightarrow\ p \nmid k$
Thus $k^{p-1} \equiv 1 \pmod p$ {FLT}

Hence $\sum_{k=1}^{p-1} k^{p-1} \equiv \sum_{k=1}^{p-1} 1 \pmod p$

$\equiv p-1 \pmod p$

$\equiv -1 \pmod p$

b Since $p$ is an odd prime, then

$1 \leqslant k \leqslant p-1 \;\Rightarrow\; p \nmid k$

$\therefore\ k^p \equiv k \pmod p$ {Corollary of FLT}

$\therefore\ \sum_{k=1}^{p-1} k^p \equiv \sum_{k=1}^{p-1} k \pmod p$

$\equiv 1+2+3+ \dots + (p-1) \pmod p$

$\equiv \dfrac{(p-1)(p)}{2} \pmod p$

$\equiv p\left(\dfrac{p-1}{2}\right) \pmod p$

$\equiv 0 \pmod p$ {as $p$ is odd, $\dfrac{p-1}{2} \in \mathbb{Z}^+$}

11 Suppose $3^{100} = a_n7^n + a_{n-1}7^{n-1} + \dots + a_27^2 + a_17 + a_0$ then $3^{100} \pmod 7 = a_0$.

Now $3^{100} \pmod 7$

$\equiv (3^6)^{16} \times 3^4 \pmod 7$

$\equiv 1^{16} \times 9 \times 9 \pmod 7$ {FLT}

$\equiv 2 \times 2 \pmod 7$

$\equiv 4 \pmod 7$

$\therefore$ the last digit is 4.

12 a Since $\gcd(7, 11) = 1$ the FLT applies.

$7^{11} \equiv 7 \pmod{11}$

$7^{10} \equiv 1 \pmod{11}$

$7^3 \equiv 2 \pmod{11}$

$7^2 \equiv 5 \pmod{11}$

$\therefore\ X \equiv t(7) + 4(1) + (6-t)(2) + 2t(5) + 7t + 3 \pmod{11}$

$\therefore\ X \equiv 7t + 4 + 12 - 2t + 10t + 7t + 3 \pmod{11}$

$\therefore\ X \equiv 22t + 19 \pmod{11}$

$\therefore\ X \equiv 8 \pmod{11}$

$\therefore\ x_0 = 8.$

b If $t = 1$

$X = 7^{11} + 4 \times 7^{10} + 5 \times 7^3 + 2 \times 7^2 + 7 + 3$

$\therefore\ X = 3\,107\,229\,562_{10}$

| | | |
|---|---|---|
| 11 | 3 107 229 562 | $r$ |
| 11 | 282 475 414 | 8 |
| 11 | 25 679 583 | 1 |
| 11 | 2 334 507 | 6 |
| 11 | 212 227 | 10 |
| 11 | 19 293 | 4 |
| 11 | 1753 | 10 |
| 11 | 159 | 4 |
| 11 | 14 | 5 |
| | 1 | 3 |

$\therefore\ X = (1\,3\,5\,4\,(10)\,4\,(10)\,6\,1\,8)_{11}$

13 a Let $N = (a_na_{n-1}\dots a_2a_1a_0)_{14}$

$\therefore\ N = a_n14^n + a_{n-1}14^{n-1} + \dots + a_214^2 + a_114 + a_0$

$\therefore\ N = 14A + a_0$ for some $A \in \mathbb{Z}$

$\therefore\ N \equiv a_0 \pmod{14}$

$\therefore\ N^7 \equiv a_0^7 \pmod{14}$ .... (1)

Now $a_0 \equiv 0, 1 \pmod 2$

$\therefore\ a_0^7 \equiv 0^7, 1^7 \pmod 2$

$\therefore\ a_0^7 \equiv 0, 1 \pmod 2$

$\therefore\ a_0^7 \equiv a_0 \pmod 2$ .... (2)

**and** $a_0^7 \equiv a_0 \pmod 7$ .... (3) {Corollary of FLT}

From (2) and (3),

$a_0^7 - a_0 \equiv 0$ (mod 2 and mod 7)

$\therefore\ 2 \mid (a_0^7 - a_0)$ and $7 \mid (a_0^7 - a_0)$

$\therefore\ 14 \mid (a_0^7 - a_0)$ {as $\gcd(2, 7) = 1$}

$\therefore\ a_0^7 \equiv a_0 \pmod{14}$

$\therefore\ N^7 \equiv a_0 \pmod{14}$ {using (1)}

As $N \equiv a_0 \pmod{14}$ and $N^7 \equiv a_0 \pmod{14}$, both $N$ and $N^7$ have last digit $a_0$ in base 14.

b Let $N = (a_na_{n-1}\dots a_2a_1a_0)_{21}$

$\therefore\ N = 21B + a_0$ for some $B \in \mathbb{Z}$

$\therefore\ N \equiv a_0 \pmod{21}$

$\therefore\ N^7 \equiv a_0^7 \pmod{21}$ .... (1)

Now $a_0 \equiv 0, 1, \text{ or } 2 \pmod 3$

$\therefore\ a_0^7 \equiv 0^7, 1^7, \text{ or } 2^7 \pmod 3$

$\therefore\ a_0^7 \equiv 0, 1, \text{ or } 128 \pmod 3$

$\therefore\ a_0^7 \equiv 0, 1, \text{ or } 2 \pmod 3$

$\therefore\ a_0^7 \equiv a_0 \pmod 3$ .... (2)

and $a_0^7 \equiv a_0 \pmod 7$ .... (3) {Corollary to FLT}

$\therefore$ from (2) and (3),

$3 \mid (a_0^7 - a_0)$ and $7 \mid (a_0^7 - a_0)$

$\therefore\ 21 \mid (a_0^7 - a_0)$ {as $\gcd(3, 7) = 1$}

$\therefore\ a_0^7 \equiv a_0 \pmod{21}$

$\therefore\ N^7 \equiv a_0 \pmod{21}$ {using (1)}

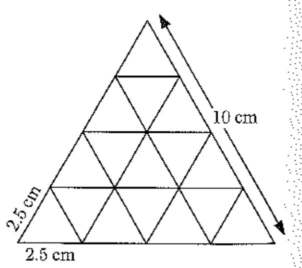
As $N \equiv a_0 \pmod{21}$ and $N^7 \equiv a_0 \pmod{21}$ both $N$ and $N^7$ have last digit $a_0$ in base 21.

## EXERCISE 1J

1 There are 12 months in a year, so by the Pigeonhole Principle there will be at least one month (pigeonhole) which is the birth month of two or more people (pigeons).

2 Divide the dartboard into 6 equal sectors. The maximum distance between any two points in a sector is 10 cm. Since there are 7 darts, at least two must be in the same sector (Pigeonhole Principle). Hence there are two darts which are at most 10 cm apart.

3 Divide the equilateral triangle into 16 identical triangles as shown. The length of each side of the small triangles is 2.5 cm.




If there are 17 points, then at least two must be in the same triangle (Pigeonhole Principle). Hence, there are at least two points which are at most 2.5 cm apart.

4 Suppose they each receive a different number of prizes. Since each child receives at least one prize, the smallest number of prizes there can be is

$1+2+3+4+5+6+7+8+9+10 = 55.$

But there are only 50 prizes. Hence, at least two children must receive the same number.

5 The pairs of numbers 1 & 12, 2 & 11, 3 & 10, 4 & 9, 5 & 8, 6 & 7 all add up to 13. Consider the three numbers which are *not* selected. These can come from at most 3 of the pairs. Hence, there are at least 3 pairs for which both numbers are selected.

6 The maximum number of days in a year is 366. So if 367 or more are present this will ensure that at least two people present have the same birthday.

$\therefore$ the minimum number of people needed = 367. {PHP}

7 a There are 2 different colours, so selecting 3 socks will ensure that 2 of the socks are the same colour.

b It is possible that if we select 14 socks all of them could be white.

$\therefore$ if we select 15 this will ensure that two different colours will be selected. {PHP}

8 There are 26 letters in the English alphabet and $27 > 26$. Therefore, at least two words will start with the same letter. {PHP}

9 $\dfrac{90\,000}{366} \approx 245.9$ .

$\therefore$ by the PHP there will be a group of 246 people who have the same birthday.

10 The pairs with sum 11 are:

$\{1, 10\}, \{2, 9\}, \{3, 8\}, \{4, 7\}, \{5, 6\}.$

This set of subsets of $\{1, 2, 3, 4, \dots, 10\}$ partition the integers 1, 2, 3, 4, ...., 10.

If the subsets are the pigeonholes and we select any 6 distinct numbers (pigeons) then there will be two such numbers with a sum of 11.

11 A units digit could be one of 10 possibilities, 0, 1, 2, 3, ...., 9. Let these possibilities be pigeonholes.

If we select 11 integers and place then into a pigeonhole corresponding to its units digit, then by the PHP at least one pigeonhole contains two of the integers and so at least two of them will have the same units digit.

12 Suppose there are $n \geqslant 2$ people at a cocktail party.

**Case (1)** (Each person has at least 1 acquaintance.)

Each person has 1, 2, 3, 4, ...., $n-1$ acquaintances. If these values are the pigeonholes, we place each person in a pigeonhole corresponding to their number of acquaintances.

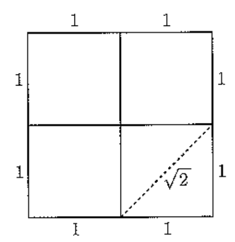
Since $n > n-1$, by the PHP, there will be two people in the same pigeonhole, that is, with the same number of acquaintances.

**Case (2)** (Someone has no acquaintances.)

Each other person can have at most $n-2$ acquaintances at the party.

Thus each of the other $n-1$ people have 1, 2, 3, ...., or $n-2$ acquaintances. We let these $n-2$ values be the pigeonholes.

Then, by the PHP, since $n-1 > n-2$ there will be two people who have the same number of acquaintances.

13 


We divide the square into 4 squares which are 1 unit by 1 unit and let these smaller squares be the pigeonholes.

If 5 (> 4) points are arbitrarily placed inside the $2 \times 2$ square then by the PHP one smaller square will contain at least two points.

The distance between these points is at most the length of a diagonal of a small square, which is $\sqrt{2}$ units.

$\therefore$ the distance between these two points is at most $\sqrt{2}$ units.

14 Let their test scores 7, 6, 5, or 4 be the pigeonholes. Since there are 25 students and 4 pigeonholes, one pigeonhole contains at least $\frac{25}{4} = 6.25$ students. So, there exists one pigeonhole containing at least 7 students. Thus it is guaranteed that there will be 7 students having the same score.

(Although possible, no greater number can be guaranteed.)

15 There are infinitely many powers of 2 (the pigeons). The 2001 residue classes modulo 2001 are the pigeonholes.

By the PHP there will be two powers of 2 in the same residue class, and they will differ by a multiple of 2001.

16 a The 'worst case' is when the red balls are selected last.

$\therefore$ least number $= 8 + 10 + 7 + \underset{\substack{\uparrow \\ \text{red}}}{3} = 28.$

b The 'worst case' is when two of each colour are selected first.

$\therefore$ least number $= 2+2+2+2+1 = 9.$

c The 'worst case' is when all green and blue balls are selected first.

$\therefore$ least number $= 10 + 8 + 1$ other $= 19.$

17 a When 3 dice are rolled the possible totals are

$\underset{\substack{\uparrow \\ \text{three 1s}}}{3}, 4, 5, 6, 7, \dots, \underset{\substack{\uparrow \\ \text{three 6s}}}{18}.$

So, there are 16 different totals.

$\therefore$ by the PHP, 17 rolls are needed to guarantee a repeated total.

b The 'worst case' is when each total appears twice first.

$\therefore$ least number $= 16 \times 2 + 1 = 33$ rolls.

## EXERCISE 2A

1 a i 4 ii 4 iii 2, 2, 2, 2

b i 4 ii 6 iii 2, 3, 3, 4

c i 4 ii 6 iii 2, 2, 4, 4

d i 2 ii 1 iii 1, 1

e i 5 ii 4 iii 1, 1, 2, 2, 2

f i 6 ii $5+4+3+2+1 = 15$ iii 5, 5, 5, 5, 5, 5

2 i Simple: a, d, e, f.

ii Connected: a, b, c, d, f.

iii Complete: d, f. {f is complete $K_6$}

3 a **Note:** These are *examples only.*