Number theory 1C

1 **a** $1 \equiv 13 \pmod{12}$

b $8 \equiv 20 \pmod{12}$

c $4 \equiv 100 \pmod{12}$

d $3 \equiv 999 \pmod{12}$ $(999 = 80 \times 12 + 39 = 83 \times 12 + 3)$

2 **a** $15 - 3 = 12$ and $6 \mid 12$ so true

b $19 - (-6) = 25$ and $5 \mid 25$ so true

c $102 - 245 = -143$ which is not divisible by 2, so false

d $431 - 277 = 154$ and $11 \mid 154$ so true

e 4 does not divide 2146, so false

f $-50 - 118 = -168$ and $12 \mid -168$ so true

3 **a** 1, 8, 15, 22…

b –6, –13, –20, –27…

c 1

4 Suppose $a \equiv b \pmod{m}$, then $b = a + mq$ for some integer q
Hence $a = b + m(-q)$, and $b \equiv a \pmod{m}$

5 **a** $2 \not\equiv -2 \pmod{5}$ as $2 - (-2) = 4$ which is not divisible by 5

b $a \equiv -a \pmod{m} \Rightarrow -a = a + mq$ for some $q \in \mathbb{Z}$

So $2a = -mq \Rightarrow a = -\frac{mq}{2}$

Thus Amy's rule will be true when a is a multiple of $\frac{m}{2}$

6 **a** $1 \equiv 5117787550 \pmod{9}$, yes the serial number is genuine

b $6 \equiv 8810024532 \pmod{9}$, no the serial number is not genuine

7 **a** $21 \equiv 1 \pmod{5} \Rightarrow 21^{201} \equiv 1^{201} \equiv 1 \pmod{5}$

b $99 \equiv -1 \pmod{10} \Rightarrow 99^{99} \equiv (-1)^{99} \equiv -1 \pmod{10}$

c $217 \equiv 0 \pmod{7} \Rightarrow 217^{1000} \equiv 0^{1000} \equiv 0 \pmod{7}$

7 d $23 \equiv -1 \pmod 8 \Rightarrow 23^{75} \equiv (-1)^{75} \equiv -1 \equiv 7 \pmod 8$

8 $218 = 24 \times 9 + 2 \Rightarrow 218 \equiv 2 \pmod 9$, so $218^6 \equiv 2^6 \equiv 64 \pmod 9$

$64 = 7 \times 9 + 1 \Rightarrow 64 \equiv 1 \pmod 9$, therefore $218^6 \equiv 1 \pmod 9$

So the remainder when 218^6 is divided by 9 is 1

9 a $7^{50} = 7^{2\times 25} = 49^{25}$

$49 \equiv -1 \pmod{50} \Rightarrow 49^{25} \equiv (-1)^{25} \equiv -1 \equiv 49 \pmod{50}$

So the remainder when 7^{50} is divided by 50 is 1

b $7^{50} \equiv -1 \pmod{50} \Rightarrow 7 \times 7^{50} \equiv 7 \times -1 \pmod{50}$ by the rules of arithmetic for modular congruences

So $7^{51} \equiv -7 \equiv 43 \pmod{50}$

10 $1004 \equiv 4 \pmod{10} \Rightarrow 1004^{200} \equiv 4^{200} \pmod{10}$

The last digit of 4^n, where $n \in \mathbb{N}$, is 4 if n is odd, and 6 if n is even.
In this case, n is even, so the last digit of 1004^{200} will be 6.

11 When $n \geqslant 7$, $n! \equiv 0 \pmod{21}$, as $n!$ contains both factors 3 and 7, and hence 21. Hence

$$\begin{aligned} 1! + 2! + 3! + \ldots + 50! \pmod{21} &\equiv 1! + 2! + 3! + 4! + 5! + 6! + 7! \pmod{21} \\ &\equiv 1 + 2 + 6 + 24 + 120 + 720 \pmod{21} \\ &\equiv 1 + 2 + 6 + 3 + 15 + 6 \pmod{21} \\ &\equiv 33 \equiv 12 \pmod{21} \end{aligned}$$

So the remainder is 12.

12 $2 \equiv -1 \pmod 3$, $3 \equiv 0 \pmod 3$, $4 \equiv 1 \pmod 3$, $5 \equiv -1 \pmod 3$

$$\begin{aligned} \text{So } 2^{100} + 3^{100} + 4^{100} + 5^{100} \pmod 3 &\equiv (-1)^{100} + (0)^{100} + 1^{100} + (-1)^{100} \pmod 3 \\ &\equiv 3 \pmod 3 \equiv 0 \pmod 3 \end{aligned}$$

13 a Base case: $k = 0$ holds since $1 \equiv 1 \pmod m$

Assume $a^k \equiv b^k \pmod m$, then $a^{k+1} \equiv a \times a^k \equiv b \times b^k \equiv b^{k+1} \pmod m$

Hence by the inductive hypothesis the statement holds for all $k \in \mathbb{Z}^+$

b For instance $1^4 \equiv 2^4 \pmod 5$ as $1 \equiv 16 \pmod 5$, but $1 \not\equiv 2 \pmod 5$.

14 $5^{22} + 17^{22} \equiv 25^{11} + 289^{11} \pmod{11}$

$25 = 2 \times 11 + 3$, so $25 \equiv 3 \pmod{11} \Rightarrow 25^{11} \equiv 3^{11} \pmod{11}$

$289 = 26 \times 11 + 3$, so $289 \equiv 3 \pmod{11} \Rightarrow 289^{11} \equiv 3^{11} \pmod{11}$

Hence $5^{22} + 17^2 \pmod{11} = 25^{11} + 289^{11} \pmod{11} = 3^{11} + 3^{11} \pmod{11}$

$3^5 \equiv 243 \equiv 1 \pmod{11}$

So $5^{22} + 17^{22} \equiv 3^{11} + 3^{11} \equiv 2 \times 3^{11} \equiv 2 \times 3 \times 3^{5\times 2} \equiv 2 \times 3 \times 1^2 \equiv 6 \pmod{11}$.

15 a $2018 \equiv -2 \pmod{10} \Rightarrow 2018^9 \equiv (-2)^9 \equiv -512 \equiv 8 \pmod{10}$

15 b $9^{2018} \equiv (-1)^{2018} \equiv 1 \text{ (mod 10)}$

c $2018^9 + 9^{2018} \equiv 8 + 1 \equiv 9 \text{ (mod 10)}$

16 $129 \equiv 2 \text{ (mod 127)} \Rightarrow 129^{123} \equiv 2^{123} \text{ (mod 127)}$

$2^7 = 128 \Rightarrow 2^7 \equiv 1 \text{ (mod 127)}$

$123 = 17 \times 7 + 4$

So $129^{123} \equiv 2^{123} \equiv 2^{17\times7+4} = (1)^{17} \times 16 = 16 \text{ (mod 127)}$

17 a As terms past and including $r = 5$ don't count as they have factors 2 and 5:

$$\sum_{r=1}^{100} r! \equiv \sum_{r=1}^{4} r! \equiv 1+2+6+24 \equiv 33 \equiv 3 \text{ (mod 10)}$$

b The final two digits will be given as the reminder when n is divided by 100.

As $100 = 2^2 \times 5^2$, the first term that will not count is $10!$, therefore:

$$\sum_{r=1}^{100} r! \equiv \sum_{r=1}^{9} r! \equiv 1+2+6+24+5!+6!+7!+8!+9! \text{ (mod 100)}$$

By part a, the last digit must be 3 and the factorial sum $5!+6!+7!+8!+9!$ will end in a zero.

The tens digit from the first four factorials will be 3 as $1+2+6+24=33$

As $5! = 120$, $6! = 720$, $7! = \ldots 40$, $8! = \ldots 20$, $9! = \ldots 80$, the tens digit of the remainder will be the unit digit of

$3 + 2 + 2 + 4 + 2 + 8 \equiv 21$, i.e. 1

So the final two digits of n are 13.

Challenge

a $19^{198} = 361^{99}$, and final two digits will be the same as for 61^{99}

Trying a few powers:

$61^1 = 61$, $61^2 = \ldots 21$, $61^3 = \ldots 81$, $61^4 = \ldots 41$, $61^5 = \ldots 01$, $61^6 = \ldots 61$, $61^7 = \ldots 21$, $61^8 = \ldots 81$

There is a pattern, and the last two digits have a cycle of 5.

As $99 \equiv 4 \text{ (mod 5)}$, the last two digits are 41.

b The last two digits of 11^m are cyclic, and for $m = 1, 2, 3\ldots$ are given by:

$11, \ldots 21, \ldots 31, \ldots 41, \ldots 51, \ldots 61, \ldots 71, \ldots 81, \ldots 91, \ldots 01, \ldots 11, \ldots 21, \ldots$

There is a cycle of length 10.

So find 12^{13}(mod 10)

As $12^{13} \equiv 2^{13} \equiv 8192 \equiv 2 \text{ (mod 10)}$ and so the last two digits are 21.

c The last two digits of 11^n for $n = 1, 2, 3\ldots$ are

$7, 49, \ldots 43, \ldots 01, \ldots 07, \ldots 49, \ldots 43, \ldots 01, \ldots 07, \ldots$

There is a cycle of length 4.

So find $7^{7^{7^7}} \text{ (mod 4)}$

As $7 \equiv (-1) \text{ (mod 4)} \Rightarrow 7^{7^{7^7}} \equiv (-1)^{7^{7^7}} \equiv -1 \equiv 3 \text{ (mod 4)}$ and so the last two digits are 43.