Number theory 1F

1 **a** By Fermat's little theorem, $3^6 \equiv 1 \pmod 7$

$\Rightarrow 3^{31} = 3^{30} \times 3 = (3^6)^5 \times 3 \equiv 3 \pmod 7$

So $3^{31} \equiv 3 \pmod 7$

b By Fermat's little theorem, $5^{16} \equiv 1 \pmod{17}$

$\Rightarrow 5^{33} = 5^{32\times 2} \times 5 = (5^{16})^2 \times 5 \equiv 5 \pmod{17}$

So $5^{33} \equiv 5 \pmod{17}$

c By Fermat's little theorem, $128^{16} \equiv 1 \pmod{17}$,

$\Rightarrow 128^{129} = 128^{128} \times 128 = (128^{16})^8 \times 128 \equiv 128 \equiv 9 \pmod{17}$

So $128^{129} \equiv 9 \pmod{17}$

d By Fermat's little theorem, $9^{10} \equiv 1 \pmod{11}$

$\Rightarrow 9^{794} = 9^{790} \times 9^4 = (9^{10})^{79} \times 9^4 \equiv 9^4 \pmod{11}$

As $9 \equiv -2 \pmod{11} \Rightarrow 9^4 \equiv (-2)^4 \equiv 16 \equiv 5 \pmod{11}$

So $9^{794} \equiv 5 \pmod{11}$

2 By Fermat's little theorem, $8^{12} \equiv 1 \pmod{13}$

$\Rightarrow 8^{50} = 8^{48} \times 8^2 = (8^{12})^4 \times 8^2 \equiv 64 \equiv 12 \pmod{13}$

So $8^{50} \equiv 12 \pmod{13}$

3 By Fermat's little theorem, $x^{11} \equiv x \pmod{11}$, for any integer x. Hence:

$4x^{11} \equiv 3 \pmod{11} \Rightarrow 4x \times x^{11} \equiv 3 \times x \pmod{11} \Rightarrow 4x \equiv 3 \pmod{11}$

As $3 \times 4 \equiv 1 \pmod{11}$, multiplying both sides by 3 gives

$3 \times 4x \equiv 3 \times 3 \pmod{11} \Rightarrow x \equiv 9 \pmod{11}$

4 By Fermat's little theorem,

$2^6 \equiv 1 \pmod 7, 3^6 \equiv 1 \pmod 7, 4^6 \equiv 1 \pmod 7, 5^6 \equiv 1 \pmod 7$ and $6^6 \equiv 1 \pmod 7$

Hence
$$\begin{aligned}2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} &= 2^{18} \times 2^2 + 3^{30} + 4^{36} \times 4^4 + 5^{48} \times 5^2 + 6^{60} \\ &= (2^6)^3 \times 2^2 + (3^6)^5 + (4^6)^6 \times 4^4 + (5^6)^8 \times 5^2 + (6^6)^{10} \\ &\equiv 2^2 + 1 + 4^4 + 5^2 + 1 \pmod 7 \\ &\equiv 4 + 1 + 256 + 25 + 1 \pmod 7 \\ &\equiv 287 \pmod 7 \\ &\equiv 0 \pmod 7 \qquad (287 = 41 \times 7)\end{aligned}$$

Therefore, $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ is divisible by 7.

5 **a** If p is a prime number and a is any integer, then $a^p \equiv a \pmod p$.

If a is not divisible by p, then this can be written as $a^{p-1} \equiv 1 \pmod p$.

5 b By Fermat's little theorem, $2^4 \equiv 1 \pmod 5$
$2^{2018} = 2^{2016} \times 2^2 = (2^4)^{504} \times 2^2 \equiv 4 \pmod 5$.

6 a If x is divisible by 11, then x^{103} is divisible by 11, so $x^{103} \not\equiv 4 \pmod{11}$
Therefore, by Fermat's little theorem, $x^{10} \equiv 1 \pmod{11}$
$\Rightarrow x^{103} = x^{100} \times x^3 = (x^{10})^{10} \times x^3 \equiv 1 \times x^3 \equiv x^3 \pmod{11}$
So $x^{103} \equiv 4 \pmod{11}$ can be reduced to $x^3 \equiv 4 \pmod{11}$

b Using trial and error:
$1^3 \equiv 1 \equiv 1 \pmod{11}$, $2^3 \equiv 8 \equiv 8 \pmod{11}$, $3^3 \equiv 27 \equiv 5 \pmod{11}$, $4^3 \equiv 64 \equiv 9 \pmod{11}$
But $5^3 \equiv 125 \equiv 4 \pmod{11}$
Hence 5 satisfies $x^{103} \equiv 4 \pmod{11}$

c $(x+11k)^3 = x^3 + 3(11k)x^2 + 3(11k)^2 x + (11k)^3$
$= x^3 + 11(3x^2k + 33xk^2 + 121k^3) \equiv x^3 \pmod{11}$
So if x satisfies $x^3 \equiv 4 \pmod{11}$, then $(x + 11k)$ satisfies $x^3 \equiv 4 \pmod{11}$ and $x^{103} \equiv 4 \pmod{11}$

7 By Fermat's little theorem, $5^{11} \equiv 5 \pmod{11}$ and $17^{11} \equiv 17 \pmod{11} \equiv 6 \pmod{11}$
$\Rightarrow 5^{22} + 17^{22} = (5^{11})^2 + (17^{11})^2 \equiv 5^2 + 6^2 \equiv 25 + 36 \equiv 61 \equiv 6 \pmod{11}$

8 Let $a = 6$, $p = 3$. Then $a^{p-1} = 6^{3-1} = 36 \equiv 0 \not\equiv 1 \pmod 3$