Finally, we present a theorem that can be used to reduce the work in identifying whether a given integer, n, is prime. In it we show that we need only attempt to divide n by all the primes $p \leqslant \sqrt{n}$. If none of these is a divisor, then n must itself be prime.

Theorem:

If $n \in \mathbb{Z}^+$ is composite, then n has a prime divisor p such that $p \leqslant \sqrt{n}$.

Proof:

Let $n \in \mathbb{Z}^+$ be composite.

$\therefore$ $n = ab$ where $a, b \in \mathbb{Z}^+$ such that $n > a > 1$ and $n > b > 1$.

If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > n$, which is a contradiction.

$\therefore$ at least one of a or b must be $\leqslant \sqrt{n}$.

Without loss of generality, suppose $a \leqslant \sqrt{n}$.

Since $a > 1$, there exists a prime p such that $p \mid a$. {Fundamental Theorem of Arithmetic}

But $a \mid n$, so $p \mid n$. $\{p \mid a$ and $a \mid n \Rightarrow p \mid n\}$

Since $p \leqslant a \leqslant \sqrt{n}$, n has a prime divisor p such that $p \leqslant \sqrt{n}$.

EXERCISE 1E

1 Determine which of the following are primes:

a 143 b 221 c 199 d 223

2 Prove that 2 is the only even prime.

3 Which of the following repunits is prime?

a 11 b 111 c 1111 d 11111

4 Show that if p and q are primes and $p \mid q$, then $p = q$.

5 $2^8 \times 3^4 \times 7^2$ is a perfect square. It equals $(2^4 \times 3^2 \times 7)^2$.

a Prove that:

i all the powers in the prime-power factorisation of $n \in \mathbb{Z}^+$ are even $\Leftrightarrow$ n is a square

ii given $n \in \mathbb{Z}^+$, the number of factors of n is odd $\Leftrightarrow$ n is a square.

b Hence prove that $\sqrt{2}$ is irrational.

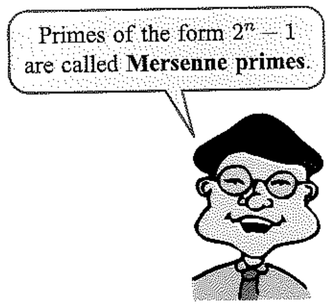
6 a Prove that if $a, n \in \mathbb{Z}^+$, $n \geqslant 2$ and $a^n - 1$ is prime, then $a = 2$.

Hint: Consider $1 + a + a^2 + \dots + a^{n-1}$ and its sum.

b It is claimed that $2^n - 1$ is always prime for $n \geqslant 2$. Is the claim true?

c It is claimed that $2^n - 1$ is always composite for $n \geqslant 2$. Is the claim true?

d If n is prime, is $2^n - 1$ always prime? Explain your answer.



7 Find the prime factorisation of:

a 9555 b 989 c 9999 d 111111

8 Which positive integers have exactly:

a three positive divisors b four positive divisors?

9 a Find all prime numbers which divide 50!

b How many zeros are at the end of 50! when written as an integer?

c Find all $n \in \mathbb{Z}$ such that $n!$ ends in exactly 74 zeros.

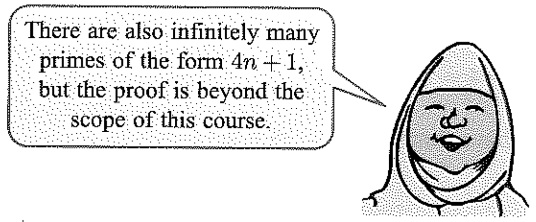
10 Given that p is prime, prove that:

a $p \mid a^n \Rightarrow p^n \mid a^n$ b $p \mid a^2 \Rightarrow p \mid a$ c $p \mid a^n \Rightarrow p \mid a$

11 There are infinitely many primes, and 2 is the only even prime.

a Explain why the form of odd primes can be $4n + 1$ or $4n + 3$.

b Prove that there are infinitely many primes of the form $4n + 3$.



12 The **Fermat primes** are primes of the form $2^{2^n} + 1$.

a Find the first four Fermat primes.

b Fermat conjectured that all such numbers were prime whenever n was prime. By examining the case $n = 5$, show that Fermat was incorrect.

RESEARCH

- The first two **perfect numbers** are 6 and 28. Research how these numbers are connected to the Mersenne primes of the form $2^n - 1$.
- The repunits R_k are prime only if k is prime, and even then only rarely. Thus far, the only prime repunits discovered are R_2, R_{19}, R_{23}, R_{317}, and R_{1031}.
  Research a proof that a repunit R_k may only be prime if k is prime.

$= 17 \times 57 - 22 \times 44$

$= 17 \times 57 - 22(158 - 57(2))$

$= -22 \times 158 + 61 \times 57$

$\therefore\ 11 = -242 \times 158 + 671 \times 57$

$\therefore\ x_0 = -242,\ -y_0 = 671$ is one solution.

$\therefore$ solutions are $x = -242 + (\frac{57}{1})t,\ \ -y = 671 - (\frac{158}{1})t$

$\therefore\ x = -242 + 57t, \qquad y = -671 + 158t$

For positive solutions we require

$-242 + 57t > 0$ *and* $-671 + 158t > 0$

$\therefore\ t > 4.245....$ *and* $t > 4.246....$

$\therefore\ t \geqslant 5$

Thus, there are infinitely many positive integer solutions. These are:

$x = -242 + 57t,\ y = -671 + 158t,\ t \geqslant 5,\ t \in \mathbb{Z}.$

3 $7 \mid a$ and $11 \mid b$

$\Rightarrow a = 7x$ and $b = 11y$ for $x, y \in \mathbb{Z}^+$

$\Rightarrow 7x + 11y = 100$ for $x, y \in \mathbb{Z}^+$

$\gcd(7, 11) = 1$ and $1 \mid 100$

$\therefore$ integer solutions exist.

Now $11 = 7(1) + 4$

$7 = 4(1) + 3$

$4 = 3(1) + 1$

$3 = 1(3) + 0$

Thus $1 = 4 - 3$

$= 4 - (7 - 4)$

$= -7 + 2 \times 4$

$= -7 + 2(11 - 7)$

$= 2 \times 11 - 3 \times 7$

$\therefore\ 100 = 200 \times 11 - 300 \times 7$

$= -300 \times 7 + 200 \times 11$

$\therefore\ x_0 = -300,\ y_0 = 200$ is one solution.

$\therefore$ solutions are $x = -300 + 11t,\ y = 200 - 7t,\ t \in \mathbb{Z}.$

For positive solutions we require

$-300 + 11t > 0$ *and* $200 - 7t > 0$

$\therefore\ 11t > 300$ *and* $7t < 200$

$\therefore\ t > 27.27$ *and* $t < 28.57$

$\therefore\ t = 28$

Hence, $x = 8,\ y = 4$

$\therefore$ the numbers are 56 and 44.

4 Let m = number of men

w = number of women

c = number of children

$\therefore\ m + w + c = 20$ {total number present}

and $5m + 4w + 2c = 62$

Thus $5m + 4w + 2(20 - m - w) = 62$

$\therefore\ 5m + 4w + 40 - 2m - 2w = 62$

$\therefore\ 3m + 2w = 22$

By inspection, one solution is $m_0 = 0,\ w_0 = 11.$

$\therefore\ m = 2t$ and $w = 11 - 3t,\ t \in \mathbb{Z}$ is the general solution.

$\therefore\ c = 20 - m - w$

$= 20 - 2t - 11 + 3t$

$= 9 + t,\ t \in \mathbb{Z}$

But $m > 0, \qquad w > 0, \qquad c > 0$

$\therefore\ 2t > 0, \quad 11 - 3t > 0, \quad 9 + t > 0$

$\therefore\ t > 0, \quad t < 3\frac{2}{3}, \quad t > -9$

$\therefore\ t = 1, 2,$ or 3

So, the possible solutions are:

m	2	4	6
w	8	5	2
c	10	11	12

Check: $5m + 4w + 2c$

$= 5(2) + 4(8) + 2(10) = 62$ ✓

or $5(4) + 4(5) + 2(11) = 62$ ✓

or $5(6) + 4(2) + 2(12) = 62$ ✓

5 Let c = number of cats bought

r = number of rabbits bought

f = number of fish bought

$\therefore\ c + r + f = 100$

and $50c + 10r + 0.5f = 1000$

$\therefore\ 50c + 10r + 0.5(100 - c - r) = 1000$

$\therefore\ 50c + 10r + 50 - \frac{1}{2}c - \frac{1}{2}r = 1000$

$\therefore\ 49\frac{1}{2}c + 9\frac{1}{2}r = 950$

$\therefore\ 99c + 19r = 1900$

By inspection, one solution is $c_0 = 0,\ r_0 = 100.$

$\therefore\ c = 19t,\ r = 100 - 99t,\ t \in \mathbb{Z}$ is the general solution.

$\therefore\ f = 100 - 19t - (100 - 99t)$

$= 80t,\ t \in \mathbb{Z}$

But $c \geqslant 1, \qquad r \geqslant 1, \qquad f \geqslant 1$

$\therefore\ 19t \geqslant 1, \quad 100 - 99t \geqslant 1, \quad 80t \geqslant 1$

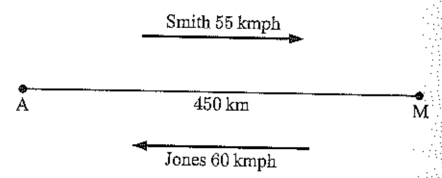
$\therefore\ t \geqslant \frac{1}{19}, \quad t \leqslant 1, \quad t \geqslant \frac{1}{80}$

$\therefore\ t = 1$

Thus $c = 19,\ r = 1,\ f = 80$

$\therefore$ I buy 19 cats, 1 rabbit, and 80 fish.

6



Let Smith travel for x hours and Jones for y hours; $x, y \in \mathbb{Z}^+$

$\therefore$ Smith travels $55x$ km, and Jones $60y$ km.

Thus $55x + 60y = 450$

$\therefore\ 11x + 12y = 90$

where $\gcd(11, 12) = 1$ and $1 \mid 90.$

$\therefore$ integer solutions exist.

Now $12 = 11(1) + 1$

$\therefore\ 1 = 12 - 11$

$\therefore\ 90 = 90 \times 12 - 90 \times 11$

$\therefore$ one solution is $x_0 = -90,\ y_0 = 90$

$\therefore$ solutions are $x = -90 + 12t,\ y = 90 - 11t,\ t \in \mathbb{Z}.$

For positive solutions,

$-90 + 12t > 0$ *and* $90 - 11t > 0$

$\therefore\ 12t > 90$ *and* $11t < 90$

$\therefore\ t > 7.5$ *and* $t < 8.18....$

$\therefore\ t = 8$

Thus $x = 6,\ y = 2$

$\therefore$ Smith travels for 6 hours, Jones for 2 hours

$\therefore$ they meet 330 km from A (or 120 km from B).

7 x = number bought at \$3.50

y = number bought at \$4 ÷ 3

z = number bought at \$0.50

$\therefore\ x + y + z = 100$ and

$3\frac{1}{2}x + \frac{4}{3}y + \frac{1}{2}z = 100$

$\therefore\ x + y + z = 100$ and

$21x + 8y + 3z = 600$

$\therefore\ -3x - 3y - 3z = -300$ and

$21x + 8y + 3z = 600$

$18x + 5y \qquad = 300$

By inspection, one solution is $x_0 = 0,\ y_0 = 60.$

$\therefore\ x = 5t,\ y = 60 - 18t,\ t \in \mathbb{Z}$ is the general solution.

$\therefore\ z = 100 - 5t - (60 - 18t)$

$= 40 + 13t$

For positive solutions

$5t > 0$ *and* $60 - 18t > 0$ *and* $40 + 13t > 0$

$\therefore\ t > 0$ *and* $18t < 60$ *and* $13t > -40$

$\therefore\ t > 0$ *and* $t < 3\frac{1}{3}$ *and* $t > -3.08$

$\therefore\ t = 1, 2,$ or 3

So the possible solutions are:

x	5	10	15
y	42	24	6
z	53	66	79

EXERCISE 1E

1 a $143 = 13 \times 11$ and so 143 is not a prime.

b $221 = 13 \times 17$ and so 221 is not a prime.

c 199 is a prime as 2, 3, 5, 7, 11, and 13 are not factors of 199.
{$\sqrt{199} \approx 14.1$, so we need only check for divisibility by primes less than 14.1}

d 223 is a prime as $\sqrt{223} \approx 14.9$ and 2, 3, 5, 7, 11, and 13 are not factors of 223.

2 Any even number greater than 2 is composite, as it has a factor other than itself and 1 (namely, 2).
So, 2 is the only even prime.

3 a 11 is prime.

b $111 = 3 \times 37$ is not prime.

c $1111 = 11 \times 101$ is not prime.

d $11\,111 = 41 \times 271$ is not prime.

4 If $p \mid q$ then $q = kp$ for some $k \in \mathbb{Z}.$
If $k \neq 1$, q is composite, a contradiction to q being a prime.
Thus $k = 1$
$\therefore\ p = q$

5 a i Suppose the powers in the factorisation of n are even

$\Leftrightarrow n = {p_1}^{2a_1}{p_2}^{2a_2}{p_3}^{2a_3}....{p_k}^{2a_k}$

$\Leftrightarrow n = \left({p_1}^{a_1}{p_2}^{a_2}{p_3}^{a_3}....{p_k}^{a_k}\right)^2$

$\Leftrightarrow n$ is a square number.

ii The power of a prime, p^n has $n + 1$ factors.
These are $1, p, p^2, p^3, ..., p^n$

$\therefore$ by the product principle of counting

$n = {p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}....{p_k}^{n_k}$ has

$(n_1 + 1)(n_2 + 1)(n_3 + 1)....(n_k + 1)$ factors.

The number of factors of n is odd

$\Leftrightarrow$ all of the $(n_i + 1)$s are odd

$\Leftrightarrow$ all of the n_is are even

$\Leftrightarrow n$ is a square. {by i}

b Suppose $\sqrt{2}$ is rational

$\therefore\ \sqrt{2} = \dfrac{p}{q}$ where $\gcd(p, q) = 1,\ q \neq 0$

$\therefore\ p^2 = 2q^2$

a contradiction as the number of factors of p^2 is odd and the number of factors of $2q^2$ is even. {from a ii}

6 a $1 + a + a^2 + a^3 + ... + a^{n-1} = \dfrac{1(a^n - 1)}{a - 1},\ a \neq 1$ {sum of a GS}

$\therefore\ a^n - 1 = (a - 1)(1 + a + a^2 + a^3 + ... + a^{n-1})$

Thus if $a^n - 1$ is prime, $a - 1 = 1$

{otherwise it has two factors other than itself and 1}

$\therefore\ a = 2$

b No, as for example, $2^4 - 1$

$= 15$

$= 3 \times 5$

c No, as for example, $2^3 - 1$

$= 7$ which is not composite.

d No, as for example, $2^{11} - 1$

$= 2047$

$= 23 \times 89$

7 a

$$\begin{array}{r|l} 5 & 9555 \\ 3 & 1911 \\ 7 & 637 \\ 7 & 91 \\ & 13 \end{array}$$

$\therefore\ 9555 = 3 \times 5 \times 7^2 \times 13$

b

$$\begin{array}{r|l} 23 & 989 \\ & 43 \end{array}$$

$\therefore\ 989 = 23 \times 43$

c

$$\begin{array}{r|l} 3 & 9999 \\ 3 & 3333 \\ 11 & 1111 \\ & 101 \end{array}$$

$\therefore\ 9999 = 3^2 \times 11 \times 101$

d

$$\begin{array}{r|l} 3 & 111\,111 \\ 37 & 37\,037 \\ 11 & 1001 \\ 7 & 91 \\ & 13 \end{array}$$

$\therefore\ 111\,111 = 3 \times 7 \times 11 \times 13 \times 37$

8 a The product of two equal primes, p^2 has exactly 3 divisors, $1, p,$ and $p^2.$

b The product of two distinct primes, pq has exactly 4 divisors, $1, p, q,$ and $pq.$

9 a The primes which divide 50! are the primes in the list $1, 2, 3, 4, ..., 49, 50.$
These are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, and 47.

b An end zero results when we have a product 2×5. There is an abundance of factors of 2, so we need only count the factors of 5 in 50!

$\underbrace{5,\ 10,\ 15,\ 20,}_{\text{1 each}}\ \underbrace{25,}_{2}\ \underbrace{30,\ 35,\ 40,\ 45,}_{\text{1 each}}\ \underbrace{50}_{2}$

$\therefore\ 4 + 2 + 4 + 2 = 12$

$\therefore$ 50! ends in 12 zeros.

c In 1 to 25 there are 6 factors of 5
In 26 to 50 there are 6
In 51 to 75 there are 6
In 76 to 100 there are 6
In 101 to 125 there are 7 {125 has 3 factors of 5}
31
In 126 to 250 there are 31
62
In 251 to 300 there are 12
74

$\therefore$ we have 74 ending zeros for 300!, 301!, 302!, 303!, 304!

10 a By the Fundamental Theorem of Arithmetic,
$$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$$
$$\therefore\ a^n = p_1^{na_1} p_2^{na_2} p_3^{na_3} \dots p_k^{na_k}$$
So, if $p \mid a^n$, then p is one of the p_i $(i = 1, 2, 3, \dots, k)$
$\Rightarrow p^n \mid a^n$

b $$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$$
{Fundamental Theorem of Arithmetic}
$$\therefore\ a^2 = p_1^{2a_1} p_2^{2a_2} p_3^{2a_3} \dots p_k^{2a_k}$$
So, if $p \mid a^2$, then p is one of the p_i
$\Rightarrow p \mid a$

c $$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$$
$$\therefore\ a^n = p_1^{na_1} p_2^{na_2} p_3^{na_3} \dots p_k^{na_k}$$
So, if $p \mid a^n$, then p is one of the p_i
$\Rightarrow p \mid a$

11 a All integers have form $4n$, $4n+1$, $4n+2$, or $4n+3$ where $4n$ and $4n+2$ are composites (they are even).
$\therefore$ all odd primes must have form $4n+1$ or $4n+3$.

b Suppose there are a finite number of primes of the form $4n+3$ and these are $p_1, p_2, p_3, p_4, \dots, p_k$ where $p_1 < p_2 < p_3 < p_4 < \dots < p_k$.
Now consider $N = 4(p_1p_2p_3 \dots p_k) + 3$ which is of the form $4n+3$.
If N is a prime number, then p_k is not the largest prime of the form $4n+3$.
If N is composite, then it must contain prime factors of the form $4n+1$ or $4n+3$.
But N cannot contain only prime factors of the form $4n+1$ since the product of such numbers is not of the form $4n+3$.
This is shown by:
$$\begin{aligned}&(4n_1+1)(4n_2+1)\\ &= 16n_1n_2 + 4n_1 + 4n_2 + 1\\ &= 4(4n_1n_2 + n_1n_2) + 1.\end{aligned}$$
Hence, N must contain a prime factor of the form $4n+3$.
Since $p_1, p_2, p_3, \dots, p_k$ are not factors of N, there exists another prime factor of the form $4n+3$.
This is a contradiction.
So, there are infinitely many primes of the form $4n+3$.

12 a If $n = 1$, $2^{2^1} + 1 = 5$, a prime.
If $n = 2$, $2^{2^2} + 1 = 2^4 + 1 = 17$, a prime.
If $n = 3$, $2^{2^3} + 1 = 2^8 + 1 = 257$, a prime.
If $n = 4$, $2^{2^4} + 1 = 2^{16} + 1 = 65\,537$, a prime.

b If $n = 5$, $2^{2^5} + 1 = 4\,294\,967\,297$
$= 641 \times 6\,700\,417$
{using a prime factors calculator via the internet}
$\therefore$ Fermat's conjecture was incorrect.

EXERCISE 1F.1

1 a, b are congruent $(\text{mod } 7) \Leftrightarrow a \equiv b \pmod 7$
$\Leftrightarrow 7 \mid a - b$

a $15 - 1 = 14$ and $7 \mid 14$
$\therefore$ 1, 15 are congruent (mod 7)

b $8 - -1 = 9$ and $7 \nmid 9$
$\therefore$ -1, 8 are *not* congruent (mod 7)

c $99 - 2 = 97$ and $7 \nmid 97$
$\therefore$ 2, 99 are *not* congruent (mod 7)

d $699 - -1 = 700$ and $7 \mid 700$
$\therefore$ -1, 699 are congruent (mod 7)

2 a $29 - 7 = 22$ and 22 has factors 1, 2, 11, 22.
$\therefore$ $m = 1, 2, 11, 22$.

b $100 - 1 = 99$ and 99 has factors 1, 3, 9, 11, 33, 99.
$\therefore$ $m = 1, 3, 9, 11, 33, 99$.

c $53 - 0 = 53$ which is a prime with factors 1, 53.
$\therefore$ $m = 1, 53$.

d $61 - 1 = 60$ which has factors 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.
$\therefore$ $m = 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

3 a $$\begin{aligned}2^{28} &= (2^3)^9 \times 2\\ &\equiv 1 \times 2 \pmod 7 \qquad \{2^3 = 8 \equiv 1\}\\ &\equiv 2 \pmod 7\end{aligned}$$

b $$\begin{aligned}10 &\equiv 3 \pmod 7 \qquad \{10 - 3 = 7 = 1 \times 7\}\\ \therefore\ 10^{33} &\equiv 3^{33} \pmod 7\\ &\equiv (3^3)^{11} \pmod 7\\ &\equiv (-1)^{11} \pmod 7 \qquad \{3^3 = 27 \equiv -1\}\\ &\equiv -1 \pmod 7\\ &\equiv 6 \pmod 7\end{aligned}$$

c $$\begin{aligned}3^{50} &= (3^3)^{16}3^2\\ &\equiv (-1)^{16} \times 2 \pmod 7 \qquad \{3^3 = 27 \equiv -1\}\\ &\equiv 2 \pmod 7\end{aligned}$$

d $$\begin{aligned}41 &\equiv -1 \pmod 7 \qquad \{41 - -1 = 42 = 6 \times 7\}\\ \therefore\ 41^{23} &\equiv (-1)^{23} \pmod 7\\ &\equiv -1 \pmod 7\\ &\equiv 6 \pmod 7\end{aligned}$$

4 a $$\begin{aligned}2^{28} &= (2^5)^5 \times 2^3\\ &\equiv (-5)^5 \times 8 \pmod{37} \qquad \{2^5 = 32 \equiv -5\}\\ &\equiv (-5)^2 \times (-5)^2 \times (-5) \times 8 \pmod{37}\\ &\equiv -12 \times -12 \times -40 \pmod{37}\\ &\qquad \{(-5)^2 = 25 \equiv -12\}\\ &\equiv -12 \times -12 \times -3 \pmod{37}\\ &\equiv -12 \times 36 \pmod{37}\\ &\equiv -12 \times -1 \pmod{37}\\ &\equiv 12 \pmod{37}\end{aligned}$$

b $$\begin{aligned}3^{65} &= (3^3)^{21} \times 3^2\\ &\equiv 1^{21} \times 9 \pmod{13} \qquad \{3^3 = 27 \equiv 1\}\\ &\equiv 9 \pmod{13}\end{aligned}$$

c $$\begin{aligned}7^{44} &= (7^2)^{22}\\ &\equiv 5^{22} \pmod{11} \qquad \{7^2 = 49 \equiv 5\}\\ &\equiv (5^2)^{11} \pmod{11}\\ &\equiv 3^{11} \pmod{11} \qquad \{5^2 = 25 \equiv 3\}\\ &\equiv (3^2)^5 \times 3 \pmod{11}\\ &\equiv (-2)^5 \times 3 \pmod{11} \qquad \{3^2 = 9 \equiv -2\}\\ &\equiv -32 \times 3 \pmod{11}\\ &\equiv 1 \times 3 \pmod{11}\\ &\equiv 3 \pmod{11}\end{aligned}$$

5 a $53 \equiv 14 \pmod{39}$ and $103 \equiv -14 \pmod{39}$
$$\begin{aligned}\therefore\ &53^{103} + 103^{53} \pmod{39}\\ &\equiv 14^{103} + (-14)^{53} \pmod{39}\\ &\equiv 14^{103} - 14^{53} \pmod{39}\\ &\equiv 14^{53}(14^{50} - 1) \pmod{39}\\ &\equiv 14^{53}[(14^2)^{25} - 1] \pmod{39}\\ &\equiv 14^{53}[1^{25} - 1] \pmod{39} \qquad \{14^2 = 196 \equiv 1\}\\ &\equiv 0 \pmod{39}\end{aligned}$$
Thus $53^{103} + 103^{53}$ is divisible by 39.

b $333 \equiv 4 \pmod 7$ and $111 \equiv -1 \pmod 7$
$$\begin{aligned}\therefore\ &333^{111} + 111^{333} \pmod 7\\ &\equiv 4^{111} + (-1)^{333} \pmod 7\\ &\equiv [(4^2)^{55} \times 4 - 1] \pmod 7\\ &\equiv [2^{55} \times 2^2 - 1] \pmod 7 \qquad \{4^2 = 16 \equiv 2\}\\ &\equiv [2^{57} - 1] \pmod 7\\ &\equiv [(2^3)^{19} - 1] \pmod 7\\ &\equiv [1^{19} - 1] \pmod 7 \qquad \{2^3 = 8 \equiv 1\}\\ &\equiv 0 \pmod 7\end{aligned}$$
$\therefore$ $333^{111} - 111^{333}$ is divisible by 7.

6 $$\begin{aligned}&2^{100} + 3^{100}\\ &= (2^2)^{50} + (3^4)^{25}\\ &\equiv (-1)^{50} + 1^{25} \pmod 5 \qquad \{2^2 = 4 \equiv -1;\ 3^4 = 81 \equiv 1\}\\ &\equiv 1 + 1 \pmod 5\\ &\equiv 2 \pmod 5\end{aligned}$$
$\therefore$ the remainder when $2^{100} + 3^{100}$ is divided by 5 is 2.

7 $203 \equiv 3 \pmod{100}$
$$\begin{aligned}\therefore\ 203^{20} &\equiv 3^{20} \pmod{100}\\ &\equiv (3^4)^5 \pmod{100}\\ &\equiv (-19)^5 \pmod{100} \qquad \{3^4 = 81 \equiv -19\}\\ &\equiv 361 \times 361 \times -19 \pmod{100}\\ &\equiv -39 \times -39 \times -19 \pmod{100}\\ &\equiv 1521 \times -19 \pmod{100}\\ &\equiv 21 \times -19 \pmod{100}\\ &\equiv -399 \pmod{100}\\ &\equiv 1 \pmod{100}\end{aligned}$$
$\therefore$ last two digits are 01.

8 a $5! = 120 \equiv 0 \pmod{20}$
$\therefore$ $k! \equiv 0 \pmod{20}$ for all $k \geqslant 5$
$$\begin{aligned}\therefore\ \sum_{k=1}^{50} k! \pmod{20} &\equiv (1! + 2! + 3! + 4!) \pmod{20}\\ &\equiv 1 + 2 + 6 + 24 \pmod{20}\\ &\equiv 33 \pmod{20}\\ &\equiv 13 \pmod{20}\end{aligned}$$

b $7! = 5040 \equiv 0 \pmod{42}$
$\therefore$ $k! \equiv 0 \pmod{42}$ for all $k \geqslant 7$
$$\begin{aligned}\therefore\ &\sum_{k=1}^{50} k! \pmod{42}\\ &\equiv (1! + 2! + 3! + 4! + 5! + 6!) \pmod{42}\\ &\equiv 873 \pmod{42}\\ &\equiv 33 \pmod{42}\end{aligned}$$

c 4×3 is contained in 10!
$\therefore$ $10! \equiv 0 \pmod{12}$
$\therefore$ $k! \equiv 0 \pmod{12}$ for all $k \geqslant 10$
$$\therefore\ \sum_{k=10}^{100} k! \pmod{12} \equiv 0 \pmod{12}$$

d 2×5 is contained in 5!
$\therefore$ $5! \equiv 0 \pmod{10}$
$\therefore$ $k! \equiv 0 \pmod{10}$ for all $k \geqslant 5$.
$$\begin{aligned}\text{Now}\ \sum_{k=4}^{30} k! &= 4! + \sum_{k=5}^{30} k!\\ &\equiv 24 + 0 \pmod{10}\\ &\equiv 4 \pmod{10}\end{aligned}$$

9 a i $$\begin{aligned}&5^{10} \pmod{11}\\ &\equiv 25^5 \pmod{11}\\ &\equiv 3^5 \pmod{11}\\ &\equiv 1 \pmod{11}\end{aligned}$$

ii $$\begin{aligned}&3^{12} \pmod{13}\\ &\equiv (3^3)^4 \pmod{13}\\ &\equiv 27^4 \pmod{13}\\ &\equiv 1^4 \pmod{13}\\ &\equiv 1 \pmod{13}\end{aligned}$$

iii $$\begin{aligned}&2^{18} \pmod{19}\\ &\equiv (2^4)^4 2^2 \pmod{19}\\ &\equiv 16^4 \times 4 \pmod{19}\\ &\equiv (-3)^4 \times 4 \pmod{19}\\ &\equiv 81 \times 4 \pmod{19}\\ &\equiv 5 \times 4 \pmod{19}\\ &\equiv 1 \pmod{19}\end{aligned}$$

iv $$\begin{aligned}&7^{16} \pmod{17}\\ &\equiv (7^2)^8 \pmod{17}\\ &\equiv 49^8 \pmod{17}\\ &\equiv (-2)^8 \pmod{17}\\ &\equiv 2^8 \pmod{17}\\ &\equiv (2^4)^2 \pmod{17}\\ &\equiv 16^2 \pmod{17}\\ &\equiv (-1)^2 \pmod{17}\\ &\equiv 1 \pmod{17}\end{aligned}$$

b *Conjecture:* (from a)
For $a \in \mathbb{Z}$, $a^{n-1} \equiv 1 \pmod n$. n may have to be prime.

c i $$\begin{aligned}&4^{11} \pmod{12}\\ &\equiv (4^3)^3 \times 4^2 \pmod{12}\\ &\equiv 64^3 \times 16 \pmod{12}\\ &\equiv 4^3 \times 4 \pmod{12}\\ &\equiv 4 \times 4 \pmod{12}\\ &\equiv 16 \pmod{12}\\ &\equiv 4 \pmod{12}\end{aligned}$$

ii $$\begin{aligned}&5^8 \pmod 9\\ &\equiv (5^2)^4 \pmod 9\\ &\equiv (-2)^4 \pmod 9\\ &\equiv 16 \pmod 9\\ &\equiv 7 \pmod 9\end{aligned}$$

iii $$\begin{aligned}&33^{10} \pmod{11}\\ &\equiv 0^{10} \pmod{11}\\ &\equiv 0 \pmod{11}\end{aligned}$$

iv $$\begin{aligned}&34^{16} \pmod{17}\\ &\equiv 0^{16} \pmod{17}\\ &\equiv 0 \pmod{17}\end{aligned}$$

d *New conjecture:* based on c examples.
For $a \in \mathbb{Z}$, and p a prime, if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$.

10 a i $$\begin{aligned}&2! \pmod 3\\ &\equiv 2 \pmod 3\end{aligned}$$

ii $$\begin{aligned}&4! \pmod 5\\ &\equiv 24 \pmod 5\\ &\equiv 4 \pmod 5\end{aligned}$$