SOLUTIONS

1. $3k + 2$ and $5k + 3$, $k \in \mathbb{Z}$ are relatively prime
if, for all k, there exist $m, n \in \mathbb{Z}$ such that
$m(3k + 2) + n(5k + 3) = 1$ R1M1A1
$\Rightarrow 3m + 5n = 0$ A1
$2m + 3n = 1$ A1
$m = 5, n = -3$ A1
hence they are relatively prime AG

[6]

2. (a) **EITHER**

$3 \mid m \Rightarrow m \equiv 0 \pmod 3$ (R1)
if this is false then $m \equiv 1$ or $2 \pmod 3$ and $m^2 \equiv 1$ or $4 \pmod 3$ R1A1
since $4 \equiv 1 \pmod 3$ then $m^2 \equiv 1 \pmod 3$ A1
similarly $n^2 \equiv 1 \pmod 3$ A1
hence $m^2 + n^2 \equiv 2 \pmod 3$
but $m^2 + n^2 \equiv 0 \pmod 3$ (R1)
this is a contradiction so $3 \mid m$ and $3 \mid n$ R1AG

OR

$m \equiv 0, 1$ or $2 \pmod 3$ and $n = 0, 1$ or $2 \pmod 3$ M1R1
$\Rightarrow m^2 \equiv 0$ or $1 \pmod 3$ and $n^2 \equiv 0$ or $1 \pmod 3$ A1A1
so $m^2 + n^2 \equiv 0, 1, 2 \pmod 3$ A1
but $3 \mid m^2 + n^2$, so $m^2 + n^2 \equiv 0 \pmod 3$ R1
$m \equiv 0 \pmod 3$ and $n \equiv 0 \pmod 3$ R1
$\Rightarrow 3 \mid m$ and $3 \mid n$ AG

(b) suppose $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and a and b are coprime M1
then
$2b^2 = a^2$ A1
$a^2 + b^2 = 3b^2$ A1
$3b^2 \equiv 0 \pmod 3$ A1

but by (a) a and b have a common factor so $\sqrt{2} \neq \frac{a}{b}$ R1

$\Rightarrow \sqrt{2}$ is irrational AG

[12]

3. (a) $457128 = 2 \times 228\,564$
$228\,564 = 2 \times 114\,282$
$114\,282 = 2 \times 57141$
$57141 = 3 \times 19047$
$19\,047 = 3 \times 6349$
$6349 = 7 \times 907$ M1A1

trial division by 11, 13, 17, 19, 23 and 29 shows that 907 is prime R1
therefore $457128 = 2^3 \times 3^2 \times 7 \times 907$ A1

(b) we require the least integer such that $2^{2^n} \geq 10^{10^6}$
taking logs twice gives M1M1
$2^n \ln 2 \geq 10^6 \ln 10$
$n \ln 2 \geq \ln\left(\frac{10^6 \ln 10}{\ln 2}\right)$
$= 6 \ln 10 + \ln \ln 10 - \ln \ln 2$
$n \geq 21.7$ (A1)
least n is 22 A1

(c) by a corollary to Fermat's Last Theorem
$5^{11} \equiv 5 \pmod{11}$ and $17^{11} \equiv 17 \pmod{11}$ M1A1
$5^{11} + 17^{11} \equiv 5 + 17 \equiv 0 \pmod{11}$ A1
this combined with the evenness of LHS implies $25 \mid 5^{11} + 17^{11}$ R1AG

[12]

4. (a) any clearly indicated method of dividing 1189 by successive numbers M1
find that 1189 has factors 29 and/or 41 A2
it follows that 1189 is not a prime number A1

Note: If no method is indicated, award A1 for the factors and A1 for the conclusion.

(b) (i) every positive integer, greater than 1, is either prime or can be expressed uniquely as a product of primes A1A1

Note: Award A1 for "product of primes" and A1 for "uniquely".

(ii) **METHOD 1**

let M and N be expressed as a product of primes as follows

$M = AB$ and $N = AC$ M1A1

where A denotes the factors that are common and B, C the disjoint factors that are not common

it follows that $G = A$ A1

and $L = GBC$ A1

from these equations, it follows that

$GL = A \times ABC = MN$ AG

METHOD 2

Let $M = 2^{x_1} \times 3^{x_2} \times \ldots p_n{}^{x_n}$ and $N = 2^{y_1} \times 3^{y_2} \times \ldots p_n{}^{y_n}$ where p_n denotes the n^{th} prime M1

Then $G = 2^{\min(x_1, y_1)} \times 3^{\min(x_2, y_2)} \times \ldots p_n{}^{\min(x_n, y_n)}$ A1

and $L = 2^{\max(x_1, y_1)} \times 3^{\max(x_2, y_2)} \times \ldots p_n{}^{\max(x_n, y_n)}$ A1

It follows that $GL = 2^{x_1} \times 2^{y_1} \times 3^{x_2} \times 3^{y_2} \times \ldots \times p_n{}^{x_n} \times p_n{}^{y_n}$ A1

$= MN$ AG

[10]

5. (a) 14641 (base $a > 6$) $= a^4 + 4a^3 + 6a^2 + 4a + 1$, M1A1

$= (a + 1)^4$ A1

this is the fourth power of an integer AG

(b) (i) aRa since $\frac{a}{a} = 1 = 2^0$, hence R is reflexive A1

$aRb \Rightarrow \frac{a}{b} = 2^k \Rightarrow \frac{b}{a} = 2^{-k} \Rightarrow bRa$

so R is symmetric A1

aRb and $bRc \Rightarrow \frac{a}{b} = 2^m, m \in \mathbb{Z}$ and $bRc \Rightarrow \frac{b}{c} = 2^n, n \in \mathbb{Z}$ M1

$\Rightarrow \frac{a}{b} \times \frac{b}{c} = \frac{a}{c} = 2^{m+n}, m + n \in \mathbb{Z}$ A1

$\Rightarrow aRc$ so transitive R1

hence R is an equivalence relation AG

(ii) equivalence classes are $\{1, 2, 4, 8\}$, $\{3, 6\}$, $\{5, 10\}$, $\{7\}$, $\{9\}$ A3

Note: Award A2 if one class missing,
A1 if two classes missing,
A0 if three or more classes missing.

[11]

6. (a) $N = a_n \times 2^n + a_{n-1} \times 2^{n-1} + ... + a_1 \times 2 + a_0$ M1

If $a_0 = 0$, then N is even because all the terms are even. R1

Now consider

$$a_0 = N - \sum_{r=1}^{n} a_r \times 2^r$$ M1

If N is even, then a_0 is the difference of two even numbers and is therefore even. R1

It must be zero since that is the only even digit in binary arithmetic. R1

(b) $N = a_n \times 3^n + a_{n-1} \times 3^{n-1} + ... + a_1 \times 3 + a_0$

$= a_n \times (3^n - 1) + a_{n-1} \times (3^{n-1} - 1) + ... + a_1 \times (3 - 1) + a_n + a_{n-1} + ... + a_1 + a_0$ M1A1

Since 3^n is odd for all $n \in \mathbb{Z}^+$, it follows that $3^n - 1$ is even. R1

Therefore if the sum of the digits is even, N is the sum of even numbers and is even. R1

Now consider

$$a_n + a_{n-1} + ... + a_1 + a_0 = N - \sum_{r=1}^{n} a_r \left(3^r - 1\right)$$ M1

If N is even, then the sum of the digits is the difference of even numbers and is therefore even. R1

[11]

7. consider the following

n	$(n^2 + 2n + 3)(\text{mod } 8)$
1	6
2	3
3	2
4	3
5	6
6	3
7	2
8	3

M1A2

we see that the only possible values so far are 2, 3 and 6 R1
also, the table suggests that these values repeat themselves but we have to prove this
let $f(n) = n^2 + 2n + 3$, consider
$f(n + 4) - f(n) = (n + 4)^2 + 2(n + 4) + 3 - n^2 - 2n - 3$ M1
$= 8n + 24$ A1
since $8n + 24$ is divisible by 8, M1
$f(n + 4) = f(n)(\text{mod } 8)$ A1
this confirms that the values do repeat every 4 values of n so that 2, 3 and 6 are the only values taken for all values of n R1

[9]

8. (a) $a = \lambda c + 1$ M1
so $ab = \lambda bc + b \Rightarrow ab \equiv b \ (\text{mod } c)$ A1 AG

(b) the result is true for $n = 0$ since $9^0 = 1 \equiv 1 \ (\text{mod } 4)$ A1
assume the result is true for $n = k$, i.e. $9^k \equiv 1(\text{mod } 4)$ M1
consider $9^{k+1} = 9 \times 9^k$ M1
$\equiv 9 \times 1 \ (\text{mod } 4)$ **or** $1 \times 9^k \ (\text{mod } 4)$ A1
$\equiv 1 \ (\text{mod } 4)$ A1
so true for $n = k \Rightarrow$ true for $n = k + 1$ and since true for $n = 0$
result follows by induction R1

Note: Do not award the final R1 unless both M1 marks have been awarded.

Note: Award the final R1 if candidates state $n = 1$ rather than $n = 0$

(c) let $M = (a_n a_{n-1} \dots a_0)_9$ (M1)

$= a \times 9^n + a_{n-1} \times 9^{n-1} + \dots + a_0 \times 9^0$ A1

EITHER

$\equiv a_n \pmod 4 + a_{n-1} \pmod 4 + \dots + a_0 \pmod 4$ A1

$\equiv \sum a_i \pmod 4$ A1

so M is divisible by 4 if $\sum a_i$ is divisible by 4 AG

OR

$= a_n(9^n - 1) + a_{n-1}(9^{n-1} - 1) + \dots + a_1(9^1 - 1)$
$+ a_n + a_{n-1} + \dots + a_1 + a_0$ A1

Since $9^n \equiv 1 \pmod 4$, it follows that $9^n - 1$ is divisible by 4, R1

so M is divisible by 4 if $\sum a_i$ is divisible by 4 AG

[12]

9. $67^{101} \equiv 2^{101} \pmod{65}$ A1

$2^6 \equiv -1 \pmod{65}$ (M1)

$2^{101} \equiv (2^6)^{16} \times 2^5$ A1

$\equiv (-1)^{16} \times 32 \pmod{65}$ A1

$\equiv 32 \pmod{65}$ A1

$\therefore$ remainder is 32 A1 N2

[6]

10. **EITHER**

we work modulo 3 throughout
the values of a, b, c, d can only be 0, 1, 2 R2
since there are 4 variables but only 3 possible values, at least 2 of the variables must be equal (mod 3) R2
therefore at least 1 of the differences must be 0 (mod 3) R2
the product is therefore 0 (mod 3) R1AG

OR

we attempt to find values for the differences that do not give 0 (mod 3) for the product
we work modulo 3 throughout
we note first that none of the differences can be zero R1
$a - b$ can therefore only be 1 or 2 R1
suppose it is 1, then $b - c$ can only be 1
since if it is 2, $(a - b) + (b - c) \equiv 3 \equiv 0 (\text{mod } 3)$ R1
$c - d$ cannot now be 1 because if it is
$(a - b) + (b - c) + (c - d) = a - d \equiv 3 \equiv 0(\text{mod } 3)$ R1
$c - d$ cannot now be 2 because if it is
$(b - c) + (c - d) = b - d \equiv 3 \equiv 0(\text{mod } 3)$ R1
we cannot therefore find values of c and d to give the required result R1
a similar argument holds if we suppose $a - b$ is 2, in which case $b - c$ must be 2 and we cannot find a value of $c - d$ R1
the product is therefore 0 (mod 3) AG

[7]

11. (a) Let $p_1, ..., p_n$ be the set of primes that divide either a or b M1
Then $a = p_1^{\alpha_2} p_2^{\alpha_2} ... p_n^{\alpha_n}$ and $b = p_1^{\beta_1} p_2^{\beta_2} ... p_n^{\beta_n}$ A1A1
Hence $ab = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} ... p_n^{\alpha_n+\beta_n}$ A1
Furthermore $\min\{\alpha_j, \beta_j\} + \max\{\alpha_j, \beta_j\} = \alpha_j + \beta_j$ for $j = 1,2,...,n$ A1
Hence $ab = p_1^{\min\{\alpha_1,\beta_1\}+\max\{\alpha_1,\beta_1\}} ... p_n^{\min\{\alpha_n,\beta_n\}+\max\{\alpha_n,\beta_n\}}$ A1
$ab = \gcd(a,b) \times \text{lcm}(a,b)$ AG

(b) $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ A1
Hence $\gcd(a,b) \mid a + b$ A1
so that $\gcd(a,b) \mid \gcd(a,a + b)$ * A1
Also $\gcd(a,a + b) \mid a$ and $\gcd(a,b) \mid a + b$ A1
Hence $\gcd(a,a + b) \mid b$ A1
so that $\gcd(a,a + b) \mid \gcd(a,b)$ ** A1
From * and ** : $\gcd(a,b) = \gcd(a,a + b)$ A1AG

[13]

12. (a) $10201 = a \times 8^4 + b \times 8^3 + c \times 8^2 + d \times 8 + e$ M1
$= 4096a + 512b + 64c + 8d + e \Rightarrow a = 2$ A1
$= 10201 - 2 \times 4096 = 2009 = 512b + 64c + 8d + e \Rightarrow b = 3$
$2009 - 3 \times 512 = 473 = 64c + 8d + e \Rightarrow c = 7$
$473 - 7 \times 64 = 25 = 8d + e \Rightarrow d = 3$ and $e = 1$
$10201 = 23731$ (base 8) A2 N2

(b) $8^n \equiv 1 \pmod 7$ for positive integer n A1
Consider the octal number
$u_n u_{n-1} \ldots u_1 u_0 = u_n + u_{n-1} + u_1 + u_0 \pmod 7$ (M1)
from which it follows that an octal number is divisible by 7 if and only if A1
the sum if the digits is divisible by 7. R1
Hence $10201 \equiv a + b + c + d + e \pmod 7$ A1

(c) $10201 \equiv 2 + 3 + 7 + 3 + 1 \equiv 2 \pmod 7$ A2

[11]

13. (a) let $N = a_n a_{n-1} \ldots a_1 a_0 = a_n \times 9^n + a_{n-1} \times 9^{n-1} + \ldots + a_1 \times 9 + a_0$ M1A1
all terms except the last are divisible by 3 and so therefore is their sum R1
it follows that N is divisible by 3 if a_0 is divisible by 3 AG

(b) **EITHER**

consider N in the form

$N = a_n \times (9^n - 1) + a_{n-1} \times (9^{n-1} - 1) + \ldots + a_1(9 - 1) + \sum_{i=0}^{n} a_i$ M1A1

all terms except the last are even so therefore is their sum R1

it follows that N is even if $\sum_{i=0}^{n} a_i$ is even AG

OR

working modulo 2, $9^k \equiv 1 \pmod 2$ M1A1
hence $N = a_n a_{n-1} \ldots a_1 a_0 = a_n \times 9^n + a_{n-1} \times 9^{n-1} + \ldots + a_1 \times 9 + a_0$

$\equiv \sum_{i=0}^{n} a_i \pmod 2$ R1

it follows that N is even if $\sum_{i=0}^{n} a_i$ is even AG

(c) the number is divisible by 3 because the least significant digit is 3 — R1
it is divisible by 2 because the sum of the digits is 44, which is even — R1
dividing the number by 2 gives $(232430286)_9$, — M1A1
which is even because the sum of the digits is 30 which is even — R1
N is therefore divisible by a further 2 and is therefore divisible by 12 — R1

Note: Accept alternative valid solutions

[12]

14. (a) $x \equiv y \pmod{n} \Rightarrow x = y + kn$, $(k \in \mathbb{Z})$ — A1

(b) $x \equiv y(\text{mod } n)$

$\Rightarrow x = y + kn$ — M1

$x^2 = y^2 + 2kny + k^2n^2$ — A1

$\Rightarrow x^2 = y^2 + (2ky + k^2n)\, n$ — M1A1

$\Rightarrow x^2 \equiv y^2 \pmod{n}$ — AG

(c) **EITHER**

$x^2 \equiv y^2 \pmod{n}$

$\Rightarrow x^2 - y^2 = 0(\text{mod } n)$ — M1

$\Rightarrow (x - y)(x + y) = 0(\text{mod } n)$ — A1

This will be the case if

$x + y = 0(\text{mod } n)$ or $x = -y(\text{mod } n)$ — R1

so $x \neq y(\text{mod } n)$ in general — R1

OR

Any counter example, e.g. $n = 5$, $x = 3$, $y = 2$, in which case — R2

$x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv y \pmod{n}$. — (false) R1R1

[9]

15. (a) consider the decimal number $A = a_n a_{n-1}, \dots a_0$ M1

$A = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_1 \times 10 + a_0$ M1

$= a_n \times (10^n - 1) + a_{n-1} \times (10^{n-1} - 1) + \dots + a_1 \times (10 - 1)$
$+ a_n + a_{n-1} + \dots + a_0$ M1A1

$= a_n \times 99\dots9$ (n digits) $+ a_{n-1} \times 99\dots9$($n - 1$ digits)
$+ \dots + 9a_1 + a_n + a_{n-1} + \dots + a_0$ A1

all the numbers of the form 99…9 are divisible by 9 (to give 11…1), R1

hence A is divisible by 9 if $\sum_{i=0}^{n} a_i$ is divisible by 9 R1

Note: A method that uses the fact that $10^t \equiv 1 \pmod 9$ is equally valid.

(b) by Fermat's Little Theorem $5^6 \equiv 1 \pmod 7$ M1A1

$(126)_7 = (49 + 14 + 6)_{10} = (69)_{10}$ M1A1

$5^{(126)_7} \equiv 5^{(11\times6+3)_{10}} \equiv 5^{(3)_{10}} \pmod 7$ M1A1

$5^{(3)_{10}} = (125)_{10} = (17 \times 7 + 6)_{10} \equiv 6 \pmod 7$ M1A1

hence $a_0 = 6$ A1

[16]

16. (a) using Fermat's little theorem $n^5 \equiv n \pmod 5$ (M1)

$n^5 - n \equiv 0 \pmod 5$ A1

now $n^5 - n = n(n^4 - 1)$ (M1)

$= n(n^2 - 1)(n^2 + 1)$

$= n(n - 1)(n + 1)(n^2 + 1)$ A1

hence one of the first two factors must be even R1

i.e. $n^5 - n \equiv 0 \pmod 2$

thus $n^5 - n$ is divisible by 5 and 2

hence it is divisible by 10 R1

in base 10, since $n^5 - n$ is divisible by 10, then $n^5 - n$ must end in zero and hence n^5 and n must end with the same digit R1

(b) consider $n^5 - n = n(n - 1)(n + 1)(n^2 + 1)$

this is divisible by 3 since the first three factors are consecutive integers R1

hence $n^5 - n$ is divisible by 3, 5 and 2 and therefore divisible by 30

in base 30, since $n^5 - n$ is divisible by 30, then $n^5 - n$ must end in zero and hence n^5 and n must end with the same digit R1

[9]

17. (a) **EITHER**

if p is a prime $a^p \equiv a(\text{mod } p)$ A1A1

OR

if p is a prime and $a \not\equiv 0(\text{mod } p)$ then $a^{p-1} \equiv 1(\text{mod } p)$ A1A1

Note: Award A1 for p being prime and A1 for the congruence.

(b) $a_0 \equiv X\,(\text{mod } 7)$ M1

$X = k \times 5^6 + 25 + 15 + 5 - k$

by Fermat $5^6 \equiv 1(\text{mod } 7)$ R1

$X \equiv k + 45 - k\ (\text{mod } 7)$ (M1)

$X \equiv 3\ (\text{mod } 7)$ A1

$a_0 = 3$ A1

(c) $X = 2 \times 5^6 + 25 + 15 + 3 = 31293$ A1

EITHER

$X - 7^5 = 14486$ (M1)

$X - 7^5 - 6 \times 7^4 = 80$

$X - 7^5 - 6 \times 7^4 - 7^2 = 31$

$X - 7^5 - 6 \times 7^4 - 7^2 - 4 \times 7 = 3$

$X = 7^5 + 6 \times 7^4 + 7^2 + 4 \times 7 + 3$ (A1)

$X = (160143)_7$ A1

OR

$31293 = 7 \times 4470 + 3$ (M1)

$4470 = 7 \times 638 + 4$

$638 = 7 \times 91 + 1$

$91 = 7 \times 13 + 0$

$13 = 7 \times 1 + 6$ (A1)

$X = (160143)_7$ A1

[11]

18. (a) **EITHER**

since gcd(a, b) = 1 and gcd(a, c) = 1 then
$ax + by = 1$ and $ap + cq = 1$ for $x, y, p, q \in \mathbb{Z}$ M1A1
hence
$(ax + by)(ap + cq) = 1$ A1
$a(xap + xcq + byp) + bc\,(yq) = 1$ M1
since $(xap + xcq + byp)$ and (yq) are integers R1
then gcd(a, bc) = 1 AG

OR

if gcd(a, bc) $\neq 1$, some prime p divides a and bc M1A1
$\Rightarrow$ p divides b or c M1
either gcd(a, b) or gcd(a, c) $\neq 1$ A1
contradiction $\Rightarrow$ gcd (a, bc) = 1 R1

[5]

19. (a) $324 = 2 \times 129 + 66$ M1
$129 = 1 \times 66 + 63$
$66 = 1 \times 63 + 3$ A1
hence gcd (324, 129) = 3 A1

(b) **METHOD 1**

Since 3 | 12 the equation has a solution M1

$3 = 1 \times 66 - 1 \times 63$ M1
$3 = -1 \times 129 + 2 \times 66$
$3 = 2 \times (324 - 2 \times 129) - 129$

$3 = 2 \times 324 - 5 \times 129$ A1
$12 = 8 \times 324 - 20 \times 129$ A1
$(x, y) = (8, -20)$ is a particular solution A1

Note: A calculator solution may gain M1M1A0A0A1.

A general solution is $x = 8 + \dfrac{129}{3}t = 8 + 43t$, $y = -20 - 108t$, $t \in \mathbb{Z}$ A1

METHOD 2

$324x + 129y = 12$
$108x + 43y = 4$ A1
$108x \equiv 4 \pmod{43} \Rightarrow 27x \equiv 1 \pmod{43}$ A1
$x = 8 + 43t$ A1
$108(8 + 43t) + 43y = 4$ M1
$864 + 4644t + 43y = 4$
$43y = -860 - 4644t$
$y = -20 - 108t$ A1
a particular solution (for example $t = 0$) is $(x, y) = (8, -20)$ A1

(c) **EITHER**

The left side is even and the right side is odd so there are no solutions M1R1AG

OR

gcd (82, 140) = 2 A1

2 does not divide 3 therefore no solutions R1AG

[11]

20. (a) $315 = 5 \times 56 + 35$ M1

$56 = 1 \times 35 + 21$

$35 = 1 \times 21 + 14$ A1

$21 = 1 \times 14 + 7$

$14 = 2 \times 7$ A1

therefore gcd = 7 A1

(b) (i) $7 = 21 - 14$ M1

$= 21 - (35 - 21)$

$= 2 \times 21 - 35$ (A1)

$= 2 \times (56 - 35) - 35$

$= 2 \times 56 - 3 \times 35$ (A1)

$= 2 \times 56 - 3 \times (315 - 5 \times 56)$

$= 17 \times 56 - 3 \times 315$ (A1)

therefore $56 \times 51 + 315 \times (-9) = 21$ M1

$x = 51$, $y = -9$ is a solution (A1)

the general solution is $x = 51 + 45N$, $y = -9 - 8N$, $N \in \mathbb{Z}$ A1A1

(ii) putting $N = -2$ gives $y = 7$, which is the required value of x A1

[13]

21. $7854 = 2 \times 3315 + 1224$ M1A1

$3315 = 2 \times 1224 + 867$ A1

$1224 = 1 \times 867 + 357$

$867 = 2 \times 357 + 153$

$357 = 2 \times 153 + 51$

$153 = 3 \times 51$ A1

The gcd is 51. A1

Since 51 does not divide 41, R1

there are no solutions. A1

[7]

22. (a) $12\,306 = 4 \times 2976 + 402$ M1

$2976 = 7 \times 402 + 162$ M1

$402 = 2 \times 162 + 78$ A1

$162 = 2 \times 78 + 6$ A1

$78 = 13 \times 6$

therefore gcd is 6 R1

(b) $6 \mid 996$ means there is a solution

$6 = 162 - 2(78)$ (M1)(A1)

$= 162 - 2(402 - 2(162))$

$= 5\,(162) - 2\,(402)$ (A1)

$= 5\,(2976 - 7\,(402)) - 2\,(402)$

$= 5\,(2976) - 37\,(402)$ (A1)

$= 5(2976) - 37(12\,306 - 4(2976))$

$= 153(2976) - 37(12\,306)$ (A1)

$996 = 25\,398(2976) - 6142(12\,306)$

$\Rightarrow\ x_0 = -6142,\ y_0 = 25\,398$ (A1)

$\Rightarrow x = -6142 + \left(\frac{2976}{6}\right)t = -6142 + 496t$

$\Rightarrow y = 25398 - \left(\frac{12306}{6}\right)t\ = 25398 - 2051t$ M1A1A1

[14]

23. (a) $ax \equiv b \pmod p$

$\Rightarrow\ a^{p-2} \times ax \equiv a^{p-2} \times b \pmod p$ M1A1

$\Rightarrow\ a^{p-1}x \equiv a^{p-2} \times b \pmod p$ A1

but $a^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem R1

$\Rightarrow\ x = a^{p-2} \times b \pmod p$ AG

Note: Award M1 for some correct method and A1 for correct statement.

(b) (i) $17x \equiv 14 \pmod{21}$

$\Rightarrow x \equiv 17^{19} \times 14 \pmod{21}$ M1A1

$17^6 \equiv 1 \pmod{21}$ A1

$\Rightarrow x \equiv (1)^3 \times 17 \times 14 \pmod{21}$ A1

$\Rightarrow x = 7 \pmod{21}$ A1

(ii) $x \equiv 7 \pmod{21}$

$\Rightarrow x = 7 + 21t,\ t \in \mathbb{Z}$ M1A1

$\Rightarrow 17(7 + 21t) + 21y = 14$ A1

$\Rightarrow 119 + 357t + 21y = 14$

$\Rightarrow 21y = -105 - 357t$ A1

$\Rightarrow y = -5 - 17t$ A1

[14]

24. (a) (i) $a \equiv d \pmod{n}$ and $b \equiv c \pmod{n}$

so $a - d = pn$ and $b - c = qn$, M1A1

$a - d + b - c = pn + qn$

$(a + b) - (c + d) = n(p + q)$ A1

$(a + b) \equiv (c + d) \pmod{n}$ AG

(ii) $\begin{cases} 2x + 5y \equiv 1 \pmod{6} \\ x + y \equiv 5 \pmod{6} \end{cases}$

adding $3x + 6y \equiv 0 \pmod{6}$ M1

$6y \equiv 0 \pmod{6}$ so $3x \equiv 0 \pmod{6}$ R1

$x \equiv 0$ or $x \equiv 2$ or $x \equiv 4 \pmod{6}$ A1A1A1

for $x \equiv 0$, $0 + y \equiv 5 \pmod{6}$ so $y \equiv 5 \pmod{6}$ A1

for $x \equiv 2$, $2 + y \equiv 5 \pmod{6}$ so $y \equiv 3 \pmod{6}$ A1

If $x \equiv 4 \pmod{6}$, $4 + y \equiv 5 \pmod{6}$ so $y \equiv 1 \pmod{6}$ A1

(b) Suppose x is a solution

97 is prime so $x^{97} \equiv x \pmod{97}$ M1

$x^{97} - x \equiv 0 \pmod{97}$ A1

$x^{97} - x + 1 \equiv 1 \neq 0 \pmod{97}$

Hence there are no solutions R1

[14]

25. the mth term of the first sequence $= 2 + 4\,(m - 1)$ (M1)(A1)
the nth term of the second sequence $= 7 + 5\,(n - 1)$ (A1)

EITHER

equating these, M1

$5n = 4m - 4$

$5n = 4(m - 1)$ (A1)

4 and 5 are coprime (M1)

$\Rightarrow 4 \mid n$ so $n = 4s$ or $5 \mid (m - 1)$ so $m = 5s + 1,\ s \in \mathbb{Z}^+$ (A1)A1

thus the common terms are of the form $\{2 + 20s;\ s \in \mathbb{Z}^+\}$ A1

OR

the numbers of both sequences are
2, 6, 10, 14, 18, 22
7, 12, 17, 22 A1
so 22 is common A1
identify the next common number as 42 (M1)A1
the general solution is $\{2 + 20s;\ s \in \mathbb{Z}^+\}$ (M1)A1

[9]

26. (a) the relevant powers of 16 are 16, 256 and 4096
then

$51966 = 12 \times 4096$ remainder 2814 M1A1

$2814 = 10 \times 256$ remainder 254

$254 = 15 \times 16$ remainder 14 A1

the hexadecimal number is CAFE A1

Note: CAFE is produced using a standard notation, accept explained alternative notations.

(b) (i) using the Euclidean Algorithm (M1)

$901 = 612 + 289$ (A1)

$612 = 2 \times 289 + 34$

$289 = 8 \times 34 + 17$

$\gcd(901, 612) = 17$ A1

(ii) working backwards (M1)

$17 = 289 - 8 \times 34$

$= 289 - 8 \times (612 - 2 \times 289)$

$= 17 \times (901 - 612) - 8 \times 612$

$= 17 \times 901 - 25 \times 612$

so $p = 17$, $q = -25$ A1A1

(iii) a particular solution is
$s = 5p = 85$, $t = -5q = 125$ (A1)
the general solution is
$s = 85 + 36\lambda$, $t = 125 + 53\lambda$ M1A1
by inspection the solution satisfying all conditions is
$(\lambda = -2)$, $s = 13$, $t = 19$ A1

(c) (i) the congruence is equivalent to $9x = 3 + 18\lambda$ (A1)
this has no solutions as 9 does not divide the RHS R1

(ii) the congruence is equivalent to $3x = 1 + 5\lambda$, $(3x \equiv 1 (\text{mod} 5))$ A1
one solution is $x = 2$, so the general solution
is $x = 2 + 5n$ $(x \equiv 2 \ (\text{mod } 5))$ M1A1

[19]

27. $x \equiv 1(\text{mod } 3) \Rightarrow x = 3k + 1$ A1
Choose k such that $3k + 1 \equiv 2 \ (\text{mod } 5)$ M1
With Euclid's algorithm or otherwise we find
$k \equiv 7 + 5h$ A1
Choose h such that $22 + 15k \equiv 3 \ (\text{mod } 7)$ M1
With Euclid′s algorithm or otherwise
$k \equiv 2 + 7j$ A1
Hence $x = 22 + 15(2 + 7j) = 52 + 105j$ A1 N3

[6]

28. (a) $N = 3 + 11t$ M1
$3 + 11t \equiv 4(\text{mod } 9)$
$2t \equiv 1 \ (\text{mod } 9)$ (A1)
multiplying by 5, $10t \equiv 5 \ (\text{mod } 9)$ (M1)
$t \equiv 5 \ (\text{mod } 9)$ A1
$t = 5 + 9s$ M1
$N = 3 + 11(5 + 9s)$
$N = 58 + 99s$ A1
$58 + 99s \equiv 0(\text{mod } 7)$
$2 + s \equiv 0(\text{mod } 7)$
$s \equiv 5 \ (\text{mod } 7)$ A1
$s = 5 + 7u$ M1
$N = 58 + 99(5 + 7u)$
$N = 553 + 693u$ A1

Note: Allow solutions that are done by formula or an exhaustive, systematic listing of possibilities.

(b) $u = 3$ or 4
hence $N = 553 + 2079 = 2632$ or $N = 553 + 2772 = 3325$ A1A1

[11]

29. (a) (i) $4^8 = 65536 \equiv 7 \pmod 9$ A1
not valid because 9 is not a prime number R1

Note: The R1 is independent of the A1.

(ii) using Fermat's little theorem M1
$5^6 \equiv 1 \pmod 7$ A1

therefore
$(5^6)^{10} = 5^{60} \equiv 1 \pmod 7$ A1

also, $5^4 = 625$ M1
$\equiv 2 \pmod 7$ A1

therefore
$5^{64} \equiv 1 \times 2 \equiv 2 \pmod 7$ (so $n = 2$) A1

Note: Accept alternative solutions not using Fermat.

(b) **EITHER**

solutions to $x \equiv 3 \pmod 4$ are
3, 7, 11, 15, 19, 23, 27, ... A1

solutions to $3x \equiv 2 \pmod 5$ are
4, 9, 14, 19 ... (M1)A1

so a solution is $x = 19$ A1

using the Chinese remainder theorem (or otherwise) (M1)
the general solution is $x = 19 + 20n$ ($n \in \mathbb{Z}$) A1
(accept 19 (mod 20))

OR

$x = 3 + 4t \Rightarrow 9 + 12t \equiv 2 \pmod 5$ M1A1
$\Rightarrow 2t \equiv 3 \pmod 5$ A1
$\Rightarrow 6t \equiv 9 \pmod 5$
$\Rightarrow t \equiv 4 \pmod 5$ A1
so $t = 4 + 5n$ and $x = 19 + 20n$ ($n \in \mathbb{Z}$) M1A1
(accept 19 (mod 20))

Note: Also accept solutions done by formula.

[14]

30. (a) Multiply through by a^{p-2}.

$a^{p-1}x \equiv a^{p-2}b \pmod p$ M1A1

Since, by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod p$, R1

$x \equiv a^{p-2}b \pmod p$ AG

(b) Using the above result,

$x \equiv 3^3 \times 4 \pmod 5 \equiv 3 \pmod 5$ M1A1

$= 3, 8, 13, 18, 23,\ldots$ (A1)

and $x \equiv 5^5 \times 6 \pmod 7 \equiv 4 \pmod 7$ M1A1

$= 4, 11, 18, 25,\ldots$ (A1)

The general solution is

$x = 18 + 35n$ M1

i.e. $x \equiv 18 \pmod{35}$ A1

[11]

31. let x be the number of guests

$x \equiv 1 \pmod 2$
$x \equiv 1 \pmod 3$
$x \equiv 1 \pmod 4$
$x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 6$
$x \equiv 0 \pmod 7$ congruence (i) (M1)(A2)

the equivalent of the first five lines is

$x \equiv 1(\text{mod}(\text{lcm of } 2, 3, 4, 5, 6)) \equiv 1 \pmod{60}$ A1

$\Rightarrow x = 60t + 1$

from congruence (i) $60t + 1 \equiv 0 \pmod 7$ M1A1

$60t \equiv -1 \pmod 7$
$60t \equiv 6 \pmod 7$
$4t \equiv 6 \pmod 7$
$2t \equiv 3 \pmod 7$ A1

$\Rightarrow t = 7u + 5$ (or equivalent) A1

hence $x = 420u + 300 + 1$ A1

$\Rightarrow x = 420u + 301$

smallest number of guests is 301 A1 N6

Note: Accept alternative correct solutions including exhaustion or formula from Chinese remainder theorem.

[10]