Question 1

(i)

$170 = 1 * 98 + 72$ **OR** $170 = 2 * 98 - 26$
$98 = 1 * 72 + 26$ $98 = 4 * 26 - 6$
$72 = 2 * 26 + 20$ $26 = 4 * 6 + 2$
$26 = 1 * 20 + 6$ $6 = 3 * 2 + 0$
$20 = 3 * 6 + 2$
$6 = 3 * 2 + 0$

Therefore gcd(98, 170) = gcd (170, 98) = 2.
[[$170 = 2 * 85 = 2 * 5 * 17$, $98 = 2 * 49 = 2 * 7^2$]]

gcd(98, 170) = 2
= 20 - 3 * 6
= 20 - 3 * (26 - 20) = 4 * 20 - 3 * 26
= 4 * (72 - 2 * 26) - 3 * 26 = 4 * 72 - 11 * 26
= 4 * 72 - 11 * (98 - 72) = 15 * 72 - 11 * 98
= 15 * (170 - 98) – 11 * 98 = 15 * 170 - 26 * 98.

OR
= 26 - 4 * 6
= 26 - 4 (4 * 26 - 98) = 4 * 98 - 15 * 26
= 4 * 98 - 15(2* 98 - 170) = 15 * 170 - 26 * 98

Therefore the general solution of gcd (98, 170) = 98x + 170y is

$$x = -26 + \frac{170}{\gcd(98,170)}t = -26 + 85t \text{ and } y = 15 - \frac{98}{\gcd(98,170)}t = 15 - 49t, \text{ where } t \in \mathbb{Z}.$$

(ii)

Using the result gcd(qb+r, b) = gcd(b, r) then, as m = 10n + 6, we have gcd(m, n) = gcd(n, 6).
As n has remainder 1 when divided by 6 then $n = 6\alpha + 1$ where α is a non-negative integer.
So gcd(n, 6) = gcd(6, 1) = 1.
Therefore gcd(m, n) = 1.

(iii)

Let P(n) be the proposition that $2 * 10^n + 4$ is divisible by 12 for $n \geq 1$.

P(1) is $2 * 10 + 4 = 24$ is divisible by 12. Therefore P(1) is true and we have the basis for induction.

Assume P(k) is true for some positive integer $k \geq 1$.

$2 * 10^{k+1} + 4 = 10 (2 * 10^k + 4) - 36$.

Since, by the induction hypothesis, $2 * 10^k + 4$ is divisible by 12 and $12 \mid 36$ then
$12 \mid 2 * 10^{k+1} + 4$.

Therefore if P(k), for $k \geq 1$, is true then P(k + 1) is true. This completes the induction step.
The result then follows from the Principle of Mathematical Induction**.**

Question 2

(i)

Assume there are a finite number, n, of primes of the form 4k - 1.
We can write these as p_i where i = 1 to n.

Let $M = 4\, p_1\, p_2 \ldots p_n - 1$.

Since M is of the form 4k - 1 then, by our assumption, it is not a prime. As it is an odd number then all of its factors must be of the form 4k - 1 or 4k +1.

M is not divisible by any of the primes p_i, where i = 1 to n, as the remainder is -1.
Therefore all of the prime factors of M must be of the form 4k + 1.

Since $(4k_1 + 1)(4k_2 + 1) = 4(4k_1k_2 + k_1 + k_2) + 1$
then the product of any 2 numbers of the form 4k + 1 is also of the form 4k + 1.
Therefore the product of any number of factors of the form 4k +1 is also of this form.
So all of the factors of M cannot be of the form 4k + 1.

Since our assumption the there are a finite number of primes of the form 4k -1 has lead to a contradiction then the assumption must be false.

Therefore there are infinitely many primes of the form 4k -1.

(ii)

If p is a prime other than 3 then it can be written in the form 3m + 1 or 3m + 2, where m is a non-negative integer.

If p is of the form 3m + 1 then 4p - 1 = 4(3m + 1) - 1 = 3(4m + 1). As m > 1 then 4p - 1 is not prime.

If p is of the form 3m + 2 then 4p + 1 = 4(3m + 2) + 1 = 3(4m + 3). As $m \geq 0$ then 4p + 1 is not prime.

Therefore, for any prime $p \neq 3$, it is impossible for both 4p -1 and 4p + 1 to be prime.

Question 3

(i)

(a)

As $a \equiv b \pmod{n}$ then, by the definition of congruence, $a = b + \alpha n$ for some integer α.
Similarly, if $c \equiv d \pmod{n}$ then $c = d + \beta n$ for some integer β.
Therefore $a + c = b + d + (\alpha + \beta)n$.
So $a + c \equiv b + d \pmod{n}$.

(b)

As $ka \equiv b \pmod{n}$ then $ka = b + \alpha n$ for some integer α.
As $kc \equiv d \pmod{n}$ then $kc = d + \beta n$ for some integer β.

Therefore $ad = a(kc - \beta n) = (ka)c - a\beta n = (b + \alpha n)c - a\beta n = bc + (\alpha c - a\beta)n$.
So $ad \equiv bc \pmod{n}$.

(ii)

As 5, 7, and 11 are relatively prime in pairs then we can use the Chinese Remainder theorem.
Therefore the equations have a unique solution modulo $5 * 7 * 11 = 35 * 11 = 385$.

As 5 and 7 are mutually prime and
$x \equiv 3 \pmod{5}$ and $x \equiv 3 \pmod{7}$
then $x \equiv 3 \pmod{5 * 7} \equiv 3 \pmod{35}$, by Corollary to Unit 3, Theorem 1.3.

Integers which satisfy the congruence $x \equiv 3 \pmod{35}$ are
3, 38, 73, 108, 143, 178, ...

The first of these integers which satisfies the congruence $x \equiv 2 \pmod{11}$ is 178.

Therefore the least positive integer which satisfies the linear congruences is 178.

Question 4

(i)

When p = 2 then (2 - 1)! ≡ 1 ≡ -1 (mod 2)

Let p ≥ 3 be a prime.
If a is one of the least positive residues then the equation ax ≡ 1 (mod p)
has a unique solution. [[Unit 3, Th. 3.2(b)]]

If $x \equiv a \pmod p$ then $a^2 - 1 \equiv 0 \pmod p$.
By Lagrange's theorem there are a maximum of 2 solutions for a when p is a prime.
Since 1 and p -1 are solutions then these are the only solutions.

Therefore the remaining p - 3 least positive residues (2, 3, ..., p -2) must have an inverse which is congruent to another residue in the list. Since the remaining p -3 values can be put into (p - 3)/2 pairs which are inverses of each other we have

$$\begin{aligned} & 1 * [\, 2 * 3 * \ldots * (p-2)\,] * (p-1) \\ & \equiv 1 * 1^{(p-3)/2} * (p-1) \\ & \equiv (p-1) \equiv -1 \pmod p. \end{aligned}$$

Therefore $(p - 1)! \equiv -1 \pmod p$ if p is a prime.

[[You might prefer the proof in the unit.]]

(ii)(a)

As 17 is a prime and gcd (5, 17) = 1 then by FLT, $5^{16} \equiv 1 \pmod{17}$.
As 17 is a prime and gcd (3, 17) = 1 then by FLT, $3^{16} \equiv 1 \pmod{17}$.

$$\begin{aligned} 5^{100} - 3^{100} &= (5^{16})^6\, 5^4 - (3^{16})^6\, 3^4 \\ &\equiv 5^4 - 3^4 \equiv (5^2 - 3^2)(5^2 + 3^2) \pmod{17} \\ &\equiv 0 \pmod{17} \text{ as } 5^2 + 3^2 = 34 \end{aligned}$$

So $17 \mid 5^{100} - 3^{100}$.

(ii)(b)

105 = 5 * 21 = 3 * 5 * 7.

Using the alternative formulation of Fermat's Little Theorem we have

$a^3 \equiv a \pmod 3$. Therefore $a^{13} \equiv (a^3)^4\, a \equiv a^4\, a \equiv a^3\, a^2 \equiv a^3 \equiv a \pmod 3$.
$a^5 \equiv a \pmod 5$. Therefore $a^{13} \equiv (a^5)^2\, a^3 \equiv a^5 \equiv a \pmod 5$.
$a^7 \equiv a \pmod{13}$. Therefore $a^{13} \equiv a^7\, a^6 \equiv a^7 \equiv a \pmod{13}$.

Therefore using the Corollary to Unit 3, Theorem 1.3 twice, we have

$a^{13} \equiv a \pmod{105}$.

Question 5

(i)(a)

Since p is a prime then $2^p - 1$ is an odd number. Therefore 2^{p-1} and $2^p - 1$ are mutually prime.
As σ is a multiplicative function then

$$\sigma(m) = \sigma(2^{p-1})\,\sigma(2^p - 1).$$

$\sigma(2^{p-1}) = 1 + 2 + \ldots 2^{p-1} = 2^p - 1.$

As m is perfect then

$$\sigma(m) = (2^p - 1)\,\sigma(2^p - 1) = 2m = 2^p (2^p - 1).$$

So $\sigma(2^p - 1) = 2^p$.

Since $\sigma(2^p - 1) = 1 + (2^p - 1)$ + any other divisors of $2^p - 1$
$= 2^p$ + any other divisors.

As $\sigma(2^p - 1) = 2^p$ then there cannot be any other divisors. Therefore $2^p - 1$ is prime.

(ii) (a)

$\sigma(6) = 1 + 2 + 3 + 6 = 12.$
$\sigma(\sigma(6)) = \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$

$\sigma(16) = \sigma(2^4) = 2^5 - 1 = 31.$
$\sigma(\sigma(16)) = \sigma(31) = 1 + 31 = 32.$

(ii) (b)

Let $n = 2^{p-1}$.
$\sigma(n) = \sigma(2^{p-1}) = 2^p - 1.$

If $2^p - 1$ is prime then

$$\sigma(\sigma(n)) = \sigma(2^p - 1) = 1 + (2^p - 1) = 2^p = 2n.$$

Therefore if $2^p - 1$ is prime then 2^{p-1} is superperfect.

[[This confirms our result in part (ii)(a) for 16.]]

Question 6

All the theorems referenced are in Unit 6.

(i)

The discriminant of the equation is $(-7)^2 - 4 * 3 * 3 = 49 - 36 = 13$.

As 31 is an odd prime and gcd (13, 31) = 1 then the quadratic congruence has solutions if 13 is a quadratic residue of 31.

(13/31)	= (31/13)	LQR, $13 \equiv 1 \pmod 4$
	= (18/13)	Th. 2.1(a)
	= (2/13) * $(3^2/13)$	Th. 2.1(c)
	= -1 * 1	Th 2.1(b), Th. 3.2, $13 \equiv 5 \pmod 8$.

As 13 is a quadratic non-residue of 31 then the given equation has no solutions.

(ii)

(76/103)	= $(2^2/103)$ (19/103)	Th. 2.1(c)
	= 1 * - (103/19)	Th. 2.1(b). LQR $103 \equiv 19 \equiv 3 \pmod 4$.
	= - (8/19)	Th. 2.1(a)
	= - (2/19) $(2^2/19)$	Th. 2.1(c)
	= - (-1) 1	Th 2.1(b). Th. 3.2. $19 \equiv 3 \pmod 8$
	= 1	

[[$(\pm 30)^2 \equiv 76 \pmod{103}$]]

(iii)

When a = 2 and p = 8k + 7 the set S in Gauss' Lemma is S = {2, 4, 6, ..., 8k + 6}
As all these numbers are less than 8k + 7 then the numbers in S are all least positive residues modulo 8k + 7.

The numbers which exceed p/2 are
4k + 4, …, 8k + 6.

There are $\frac{(8k+6)-(4k+4)}{2}+1 = 2k+2$.

Since $(-1)^{2k+2} = 1$ then, by Gauss' Lemma,
2 is a quadratic residue of any prime of the form 8k + 7.

Question 7

(i)

Applying the Euclidean algorithm

96 = 1 * 67 + 29
67 = 2 * 29 + 9
29 = 3 * 9 + 2
9 = 4 * 2 + 1 = gcd (96, 67)
2 = 2 * 1 + 0

Therefore a continued simple fraction for 96/67 is [1, 2, 3, 4, 2].

k =	**1**	**2**	**3**	**4**	**5**
a_k	1	2	3	4	2
p_k	1	3	10	43	96
q_k	1	2	7	30	67

Using Unit 7, Th. 1.3a with k = 5 we have

$p_5 q_4 - p_4 q_5 = 96 * 30 - 43 * 67 = (-1)^5 = -1$.

So 96 (-30) - 67 * (-43) = 1.
As gcd(96, 67) = 1 then the general solution of 96x - 67y = 1 is

x = -30 + 67t, y = -43 + 96t, where t is an integer.

Putting t = 1 gives the positive solutions x = 37, y = 53.

[[96*37 = (100 - 4) * 37 = 3700 - 148 = 3552.
67 * 53 = 67 * (50 + 3) = 3350 + 201 = 3551.]]

(ii)

Let x = [<2, 1>] = [2, 1, x].

The convergents of [2, 1, x] are

$$C_1 = \frac{2}{1};\ C_2 = \frac{2*1+1}{1} = \frac{3}{1};\ C_3 = \frac{x*3+2}{x*1+1} = \frac{3x+2}{x+1} = x.$$

.

So $x^2 - 2x - 2 = 0$ and this has the positive solution $x = \frac{2+\sqrt{4+8}}{2} = 1+\sqrt{3}$.

The convergents of [3, 2, <2, 1>] = [3, 2, x] are

$$C_1 = \frac{3}{1};\ C_2 = \frac{3*2+1}{2} = \frac{7}{2};$$

$$C_3 = \frac{x*7+3}{x*2+1} = \frac{10+7\sqrt{3}}{3+2\sqrt{3}} = \frac{10+7\sqrt{3}}{3+2\sqrt{3}}\frac{3-2\sqrt{3}}{3-2\sqrt{3}} = \frac{(30-42)+\sqrt{3}}{9-12} = \frac{12-\sqrt{3}}{3} = [3, 2, <2, 1>]..$$

Question 8

(i)

$$\sqrt{8} = 2 + (\sqrt{8} - 2) = 2 + (\sqrt{8} - 2)\frac{(\sqrt{8} + 2)}{(\sqrt{8} + 2)} = 2 + \frac{8 - 4}{(\sqrt{8} + 2)} = 2 + \frac{1}{(\sqrt{2} + 1)/2}.$$

$$\frac{\sqrt{2} + 1}{2} = 1 + \frac{(\sqrt{2} - 1)}{2} = 1 + \frac{(\sqrt{2} - 1)}{2}\frac{(\sqrt{2} + 1)}{(\sqrt{2} + 1)} = 1 + \frac{1}{2(\sqrt{2} + 1)}.$$

$$2\sqrt{2} + 2 = 4 + (2\sqrt{2} - 2) = 4 + (2\sqrt{2} - 2)\frac{(2\sqrt{2} + 2)}{(2\sqrt{2} + 2)} = 4 + \frac{4}{(2\sqrt{2} + 2)} = 4 + \frac{1}{(\sqrt{2} + 1)/2}.$$

As $\frac{\sqrt{2} + 1}{2}$ has occurred previously then the last two lines will be repeated indefinitely.

So $\sqrt{8}$ = [2, <1, 4>].

By Unit 8, Theorem 1.1, if x= a, y = b are solutions of $x^2 - 8y^2 = 1$ then
a/b is a convergent of $\sqrt{8}$.

As the continued fraction of $\sqrt{8}$ has cycle length 2 then, by Unit 8, Th. 1.2,
$p_{2r}^2 - 8q_{2r}^2 = (-1)^{2r} = 1$; r = 1, 2, 3, …

k =	**1**	**2**	**3**	**4**	**5**	**6**
a_k	2	1	4	1	4	1
p_k	2	3	14	17	82	99
q_k	1	1	5	6	29	35

So 3 positive solutions of the Diophantine equation are
x = 3, y = 1; x = 17, y = 6; x = 99, y = 35.

(ii)

$720 = 10 * 72 = 2 * 5 * 9 * 8 = 2^4 * 3^2 * 5$.
Since no factor of the form 4k + 3 occurs to an odd power then 720 can be expressed as the sum of 2 squares (Unit 8, Th. 4.3).

$720 = 5 * (2^2 * 3)^2 = (2^2 + 1^2) * 12^2 = 24^2 + 12^2$.

$726 = 2 * 363 = 2 * 3 * 121 = 2 * 3 * 11^2$.
Since a factor of the form 4k + 3 occurs to an odd power then 726 cannot be expressed as the sum of 2 squares (Th. 4.3).

(iii)

Assume that $x = x_1$, $y = y_1$, $z = z_1$ is a solution in positive integers of the equation.
Then $x_1^3 - 3y_1^3 = 9 z_1^3$. (A)

As 3 divides the second and third terms then $3 \mid x_1^3$.
Therefore $3 \mid x_1$ and there is an integer x_2 such that $x_1 = 3 x_2$.
Substituting this in equation (A) and dividing by 3 gives
$9x_2^3 - y_1^3 = 3 z_1^3$. (B)

As 3 divides the first and third terms then $3 \mid y_1^3$.
Therefore $3 \mid y_1$ and there is an integer y_2 such that $y_1 = 3 y_2$.
Substituting this in equation (B) and dividing by 3 gives
$3x_2^3 - 9y_2^3 = z_1^3$. (C)

As 3 divides the first and second terms then $3 \mid z_1^3$.
Therefore $3 \mid z_1$ and there is an integer z_2 such that $z_1 = 3 z_2$.
Substituting this in equation (C) and dividing by 3 gives
$x_2^3 - 3y_2^3 = 9z_2^3$. (D)

Therefore $x = x_2$, $y = y_2$, $z = z_2$ is also a solution of $x_1^3 - 3y_1^3 = 9 z_1^3$ in positive integers with $x_2 < x_1$.

As the descent step has been established then by the method of infinite descent there can be no solution in positive integers.

END OF PART 1 SOLUTIONS