Question 1

(i)

253 = 1 * 209 + 44
209 = 4 * 44 + 33 [[or 209 = 5 * 44 - 11; 44 = 4 * 11 + 0]]
44 = 1 * 33 + 11
33 = 3 * 11 + 0

Therefore gcd (253, 209) = 11. [[253 = 23 * 11, 209 = 19 * 11]]

11 = 44 – 33
= 44 - (209 - 4 * 44) = 5 * 44 - 209
= 5 * (253- 209) – 209 = 5 * 253 - 6 * 209.

Therefore the general solution of gcd (253, 209) = 253x + 209y is

$$x = 5 + \frac{209}{\gcd(253, 209)}t = 5 + 19t \text{ and } y = -6 - \frac{253}{\gcd(253, 209)}t = -6 - 23t$$, where $t \in \mathbb{Z}$.

(ii)

24n + 3 = 3 (8n + 1).

gcd (8n + 1, 8n - 1) = gcd (8n + 1, 2). Since 8n + 1 is odd then gcd (8n + 1, 8n - 1) =1.

Therefore gcd (8n -1, 24n + 3) = gcd (8n - 1, 3(8n + 1)) = gcd (8n - 1, 3).
So gcd (8n -1, 24n + 3) = 1 or 3.

gcd (8n -1, 24n + 3) = 3 when 8n - 1 $\equiv$ 0 (mod 3). So n $\equiv$ 2 (mod 3).

(iii)

Let P(n) be the proposition that 10^n - 4 is divisible by 12.

As P(2) is 10^2 - 4 = 96 is divisible by 12 then P(2) is true and we have the basis for induction.

Assume P(k) is true for some positive integer k $\geq$ 2.

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

Since, by the induction hypothesis, 10^k - 4 is divisible by 12 then 12 | 10^{k+1} - 4.

Therefore if P(k), for k $\geq$ 2, 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)

When $n = 6$ then $12n + 5 = 77 = 7 * 11$. Neither 7 nor 11 is of the form $12m + 5$.

Therefore the statement is false.

(ii)

Without loss of generality we can assume that $p < q$.

As p and q are odd primes then $p = 2m + 1$ and $q = 2m + 3$ for some integer m.
As $p + q = 4m + 4$ then $4 \mid p + q$.

If p is a prime other than 3 then it can be written in the form $3m + 1$ or $3m + 2$.
The smallest twin prime cannot be of the form $3m + 1$ as $3 \mid p + 2$.
So $p = 3m + 2$ and $q = 3m + 4$ for some integer m.
As $p + q = 6m + 6$ then $3 \mid p + q$.

As 3 and 4 are relatively prime then $12 \mid p + q$.

Therefore the statement is true.

(iii)

If $p = 3$ then $q = 13$ and $r = 53$. These are both prime.

If p is prime and not equal to 3 then it can be written in the form $3n + 1$ or $3n + 2$.

If $p = 3n + 1$ then $q = 12n + 5$ and $r = 48n + 21$. As r is divisible by 3 then q and r are not both prime.

If $p = 3n + 2$ then $q = 12n + 9$. As q is divisible by 3 then q and r are not both prime.

Therefore the statement is true.

Question 3

(i)

(a) As $4n + 3 \equiv 3 \pmod 4$ then the least positive residue modulo 4 of $4n + 3$ is 3.

(b) Since $n \equiv 5 \pmod 8$ then $n = 8k + 5$ for some integer k.
Therefore $4n + 3 = 4(8k + 5) + 3 = 32k + 23$.
As $32n + 23 \equiv 7 \pmod{16}$ then the least positive residue modulo 16 of $4n + 3$ is 7.

(ii)

Since $a \equiv b \pmod n$ then, by the definition of congruence, $a - b = sn$, for some integer s.
Similarly as $c \equiv d \pmod n$ then $c - d = tn$, for some integer t.

Therefore $ac = (b + sn)(d + tn) = bd + n(bt + sd + stn)$.
Since $ac - bd = n(bt + sd + stn)$ then, by the definition of congruence,

$$ac \equiv bd \pmod n.$$

(iii)

$3x - 11 \equiv 0 \pmod{17} \Leftrightarrow 18x \equiv 66 \pmod{17} \Leftrightarrow x \equiv 15 \pmod{17}$.

As 3, 5, and 17 are relatively prime in pairs then we can use the Chinese Remainder theorem.
Therefore the equations

$$x \equiv 1 \pmod 3, \quad x \equiv 1 \pmod 5, \text{ and } x \equiv 15 \pmod{17}$$

have a unique solution modulo $3 * 5 * 17 = 3 * 85 = 255$.

As $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$ and 3 and 5 are relatively prime then, by the Corollary to Theorem 1.3, we have

$$x \equiv 1 \pmod{15}.$$

Integers which satisfy the congruence $x \equiv 15 \pmod{17}$ are

15, 32, 49, 66, 83, 100, 117, 134, 151, ...

Therefore the least positive integer which satisfies the linear congruences is 151.

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

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

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 (36, 17) = 1 then by FLT, $36^{16} \equiv 1 \pmod{17}$.

Therefore $36^{36} = (36^{16})^2 \, 36^4 \equiv (1)^2 \, 2^4 \equiv 16 \pmod{17}$.

[[$36^{36} \equiv 2^{36} \equiv (2^4)^9 \equiv (-1)^9 \equiv -1 \pmod{17}$]]

(ii)(b)

195 = 5 * 39 = 3 * 5 * 13.

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

$a^3 \equiv a \pmod 3$. Therefore $a^{25} \equiv (a^3)^8 \, a \equiv a^8 \, a \equiv (a^3)^3 \equiv a^3 \equiv a \pmod 3$.
$a^5 \equiv a \pmod 5$. Therefore $a^{25} \equiv (a^5)^5 \equiv a^5 \equiv a \pmod 5$.
$a^{13} \equiv a \pmod{13}$. Therefore $a^{25} \equiv a^{13} \, a^{12} \equiv a^{13} \equiv a \pmod{13}$.

Therefore using the Corollary to Unit 3, Theorem 1.3 twice, we have
$a^{25} \equiv a \pmod{195}$.

Question 5

(i)(a)

As 120 = 8 * 15 = 2^3 * 3 * 5 then $\sigma(120) = \sigma(2^3)\,\sigma(3)\,\sigma(5) = \frac{2^4-1}{2-1} * 4 * 6 = 360 = 3 * 120$.
Therefore 120 is 3-perfect.

As 140 = 14 * 10 = 2^2 * 5 * 7 then $\sigma(140) = \sigma(2^2)\,\sigma(5)\,\sigma(7) = \frac{2^3-1}{2-1} * 6 * 8 = 7 * 6 * 8$.
As $\sigma(140)$ is not divisible by 5 then 140 is not 3-perfect.

(ii)

As $p \geq 3$ then $\sigma(n) = \sigma(2^r)\,\sigma(p) = \frac{2^{r+1}-1}{2-1}(p+1) = 2^{r+1}p + 2^{r+1} - p - 1$.

If $\sigma(n) = 3n$ then $2^{r+1}p + 2^{r+1} - p - 1 = 3 * 2^r * p$.
As 3 * 2^r p = (2 + 1) * 2^r p = 2^{r+1} p + 2^r p then
$2^r p = 2^{r+1} - p - 1$.

Rearranging the equation gives $2^r(p-2) = -(p+1)$.
Since p > 2 then the left-hand side of the equation is positive whereas the other side is negative.
Since our assumption has lead to a contradiction then the assumption that there is a 3-perfect number of the given form must be incorrect.

(iii)

$\sigma(n) = \sigma(2^r)\,\sigma(3)\,\sigma(7) = \frac{2^{r+1}-1}{2-1} * 4 * 8 = 32\left(2^{r+1}-1\right)$.

If n is 3-perfect then 32 (2^{r+1} - 1) = 3n = 2^r * 3^2 * 7.
We must have r = 5 to get the same power of 2 on both sides of the equation.

When r = 5 the equation holds as 32 * 63 = 2^5 * 9 * 7. Therefore n is 3-perfect in this case.

Hence n = 32 * 21 = 32 (20 + 1) = 640 + 32 = 672 is the only 3-perfect number of this form.

Question 6

(i)

The discriminant of the equation is $5^2 - 4 * 7 * 1 = -3$.

As 23 is an odd prime and gcd (-3, 23) = 1 then the quadratic congruence has solutions if -3 is a quadratic residue of 23.

(-3/23)	= (-1/23) (3/23)	Th. 2.1(c)
	= -1 * 1	Th. 2.1(e) and Th. 4.4
	= -1	

As -3 is a quadratic non-residue of 23 then the equation has no solutions.

(ii)

(163/193)	= (193/163)	LQR. $193 \equiv 1 \pmod 4$
	= (30/163)	Th. 2.1(a). $30 \equiv 193 \pmod{163}$
	= (2/163) (3/163) (5/163)	Th. 2.1(c)
	= (- 1) * (-1) * (5/163)	Th. 3.2, $163 \equiv 3 \pmod 8$; Th. 4.4, $163 \equiv 7 \pmod{12}$
	= (163/5)	LQR. $5 \equiv 1 \pmod 4$
	= (3/5)	Th 2.1(a). $163 \equiv 3 \pmod 5$
	= - 1	Th. 4.4.

(iii)

When a = 2 and p = 8k + 5 the set S in Gauss' Lemma is S = {2, 4, 6, ..., 8k + 4}
As all these numbers are less than 8k + 5 then the numbers in S are all least positive residues modulo 8k + 5.

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

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

Since $(-1)^{2k+1} = -1$ then, by Gauss' Lemma,
2 is a not a quadratic residue of any prime of the form 8k + 5.

Question 7

(i)

$$\begin{aligned} 83 &= 2 * 30 + 23 \\ 30 &= 1 * 23 + 7 \\ 23 &= 3 * 7 + 2 \\ 7 &= 3 * 2 + 1 \\ 2 &= 2 * 1 + 0 \end{aligned}$$

Therefore $83/30 = [2, 1, 3, 3, 2]$.

Using the second continued fraction identity we also have

$$83/30 = [2, 1, 3, 3, 2] = [2, 1, 3, 3, 1 + 1/1] = [2, 1, 3, 3, 1, 1].$$

(ii)

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

The convergents of $[2, 1, 2, x]$ are

$$C_1 = \frac{2}{1};\ C_2 = \frac{2*1+1}{1} = \frac{3}{1};\ C_3 = \frac{2*3+2}{2*1+1} = \frac{8}{3};\ C_4 = \frac{x*8+3}{x*3+1} = \frac{8x+3}{3x+1} = x.$$

.

So $3x^2 - 7x - 3 = 0$ and this has the positive solution $x = \frac{7+\sqrt{49+36}}{6} = \frac{7+\sqrt{85}}{6}$.

So $\left[1, \langle 2,1,2 \rangle\right] = 1 + \frac{6}{7+\sqrt{85}} = 1 + \frac{6\left(7-\sqrt{85}\right)}{49-85} = 1 + \frac{\sqrt{85}-7}{6} = \frac{\sqrt{85}-1}{6}$.

The first seven convergents are

$$C_1 = \frac{1}{1};\ C_2 = \frac{2*1+1}{2} = \frac{3}{2};\ C_3 = \frac{1*3+1}{1*2+1} = \frac{4}{3};\ C_4 = \frac{2*4+3}{2*3+2} = \frac{11}{8};$$

$$C_5 = \frac{2*11+4}{2*8+3} = \frac{26}{19};\ C_6 = \frac{1*26+11}{1*19+8} = \frac{37}{27};\ C_7 = \frac{2*37+26}{2*27+19} = \frac{100}{73}.$$

(i)(a)

By Corollary to Theorem 4.1, $|x - C_4| > \frac{1}{2*8*19} = \frac{1}{16*19} > \frac{1}{25*20} = \frac{1}{500}$. Therefore C_4 is not sufficiently accurate.

By Corollary to Theorem 4.1, $|x - C_5| < \frac{1}{19*27} = \frac{1}{(20-1)*27} = \frac{1}{540-27} < \frac{1}{500}$.

Hence C_5 is the 1st convergent accurate to the given periodic continued fraction within 1/500.

Question 8

(i)

284 = 4 * 71. Since a factor of the form 4k + 3 occurs to an odd power then 284 cannot be expressed as the sum of 2 squares (Th. 4.3). As 284 is of the form 4^n (8m + 7) where m and n are positive integers then it cannot be expressed as the sum of 3 squares (Th. 4.4).

286 = 2 * 143 = 2 * 11 * 13. Since a factor of the form 4k + 3 occurs to an odd power then 286 cannot be expressed as the sum of 2 squares (Th. 4.3). As 286 is not of the form 4^n (8m + 7) where m and n are positive integers then it can be expressed as the sum of 3 squares (Th. 4.4).

288 = 4 * 72 = 32 * 9 = $2^5 * 3^2$. Since no factor of the form 4k + 3 occurs to an odd power then 288 can be expressed as the sum of 2 squares (Th. 4.3). Including the term 0^2 means it can also be expressed as the sum of 3 squares.

288 = 32 * 3^2 = ($4^2 + 4^2$) * 3^2 = $12^2 + 12^2$. [[or by inspection 288 = 144 + 144 = …]]

(ii)

$$\sqrt{8} = \frac{m}{n} = \frac{m}{n}\frac{3n-m}{3n-m} = \frac{1}{3n-m}\left(3m - \frac{m^2}{n}\right) = \frac{1}{3n-m}\left(3m - \frac{m^2}{n^2}n\right) = \frac{3m-8n}{3n-m}.$$

Since $2 < \sqrt{8} < 3$ then 2n < m < 3n.
So 3n - m > 0 and, as 2n - m < 0 then, 3n - m < n.

Since 0 < 3n - m < n then the numerator and denominator of (3m - 8n) / (3n -m) are both positive and are smaller integers than the corresponding values in m/n.

Therefore the descent step has been established.

Hence by the method of infinite descent it is not possible to write $\sqrt{8}$ in the given form.

Therefore $\sqrt{8}$ is irrational.

END OF PART 1 SOLUTIONS