Question 1

(i)

$161 = 1 * 98 + 63$ **OR** $161 = 2 * 98 - 35$
$98 = 1 * 63 + 35$ $98 = 3 * 35 - 7$
$63 = 1 * 35 + 28$ $35 = 5 * 7 + 0$
$35 = 1 * 28 + 7$
$28 = 4 * 7 + 0$

Therefore gcd(98, 161) = gcd (161, 98) = 7.
[[161 = 7 * 23, 98 = 7 * 14]]

gcd(98, 161) = 7
= 35 - 28
= 35 - (63 - 35) = 2 * 35 - 63
= 2 * (98 - 63) - 63 = 2 * 98 - 3 * 63
= 2 * 98 - 3 * (161 - 98) = 5 * 98 - 3 * 161.

OR
= 3 * 35 - 98
= 3 * (2 * 98 - 161) – 98 = 5 * 98 - 3 * 161

So $x_0 = 5$, and $y_0 = -3$ is a solution of gcd (98, 161) = 7 = 98x + 161y.
Dividing by 7 gives 14x + 23y = 1.
Therefore, by Unit 1, Th. 1.5, the general solution of gcd (98, 161) = 7 = 98x + 161y is
x = 5 + 23k and y = -3 – 14k, where k is an integer.

(ii)

Using the result gcd(qb+r, b) = gcd(b, r) then, as m = 9n + 4, we have gcd(m, n) = gcd(n, 4).
As n has remainder 3 when divided by 4 then $n = 4\alpha + 3$ where α is a non-negative integer.
So gcd(n, 4) = gcd(4, 3) = 1.
Therefore gcd(m, n) = 1.

(iii)

Let P(n) be the proposition $1 + 5 + 12 + 22 + ... + \frac{1}{2} n(3n -1) = \frac{1}{2} n^2 (n + 1)$.

P(1) is $1 = \frac{1}{2} * 1^2 * (1 + 1)$. As P(1) is true then we have the basis for induction.

Assume P(k) is true for some positive integer k.
$1 + 5 + 12 + 22 + ... + \frac{1}{2} k(3k -1) + \frac{1}{2} (k + 1)[3(k + 1) -1]$
$= \frac{1}{2} k^2 (k + 1) + \frac{1}{2} (k + 1)(3k + 2)$ (using the induction hypothesis)
$= \frac{1}{2} (k + 1) (k^2 + 3k +2)$
$= \frac{1}{2} (k + 1)^2 (k +2)$.

Therefore if P(k) 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)

4 is of the form 3k + 1 but 4 = 2 * 2, and 2 is not of this form.
The statement is **false**.

(ii) *[[Need this result in part(iv) so it must be true]].*

By the Division Algorithm every number has one of the forms 3k, 3k + 1, or 3k - 1.

The only prime of the form 3k is 3. 3 does not divide a positive integer of the form 3k – 1.

Therefore if a number of the form 3k – 1 does not have a prime divisor of the same form then it can be written as $p_1 p_2 \ldots p_n$ where the primes p_i are all of the form 3k + 1.

However as $p_1 p_2 \ldots p_n \equiv 1^n \equiv 1 \pmod 3$ then it is not of the form 3k – 1.

Therefore a number of the form 3k – 1 must have a prime factor of the same form so the statement is **true**.

(iii)

If m = n = 1, then gcd(m, n) = 1 and gcd(3m + 1, 3n + 1) = gcd(4, 4) = 4.
Therefore the statement is **false**.

(iv) *[[Since gcd(3, -1) = 1 then Dirichlet's theorem tells us there are an infinite number.]]*

The statement is **true**.

Assume there are a finite number of primes of the form 3k - 1 and these are $p_1, p_2, \ldots, p_n$.

Let $N = 3(p_1p_2...p_n) - 1$. Since this is of the form 3k - 1 then, by part (ii) it must have a prime factor of the form 3k – 1. Assume this prime is p_i $(1 \le i \le n)$.

Since p_i divides N and $3(p_1p_2...p_n)$ then it divides $N - 3(p_1p_2...p_n) = 1$.

Since p_i does not divide 1 then the assumption that there are a finite number of primes of the form 3k - 1 must be false. Therefore there are an infinite number of primes of this form.

Question 3

(i)

Since $n \equiv 5 \pmod 8$ then $n = 8k + 5$ for some integer k.
Therefore $6n + 3 = 6(8k + 5) + 3 = 48k + 33$.

(a) As $6n + 3 \equiv 1 \pmod 8$ then the least positive residue modulo 8 is 1.

(b) As $6n + 3 \equiv 9 \pmod{12}$ then the least positive residue modulo 12 is 9.

(ii)

$r\,a \equiv r\,b \pmod{r\,n} \Leftrightarrow r\,a = r\,b + \alpha\, r\,n$, for some integer α
$\Leftrightarrow a = b + \alpha\, n$
$\Leftrightarrow a \equiv b \pmod n$, since $n > 0$.

[[I am not sure why they have added the condition $n \geq 2$ rather than $n > 0$. If $n = 1$ then we have $r\,a \equiv r\,b \pmod r \Leftrightarrow a \equiv b \pmod 1$. Both sides are always true.]]

(iii)

$2x \equiv 1 \pmod 7 \Leftrightarrow 8x \equiv x \equiv 4 \pmod 7$
$6x \equiv 8 \pmod{11} \Leftrightarrow 12x \equiv x \equiv 16 \equiv 5 \pmod{11}$
$x \equiv 2 \pmod 3 \Leftrightarrow x \equiv 5 \pmod 3$

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

$x \equiv 5 \pmod 3$, $x \equiv 4 \pmod 7$, and $x \equiv 5 \pmod{11}$

have a unique solution modulo $3 * 7 * 11 = 21 * 11 = 231$.

As $x \equiv 5 \pmod 3$, $x \equiv 5 \pmod{11}$ and 3 and 11 are relatively prime then, by the Corollary to Theorem 1.3, we have

$x \equiv 5 \pmod{33}$.

Integers which satisfy the congruence $x \equiv 5 \pmod{33}$ are

5, 38, 71, 104, 137, ...

The first integer which also equals 4 modulo 7 is 137.

Therefore the least positive integer which satisfies the linear congruences is 137.

Question 4

(i)

As gcd(7, 17) = 1 and gcd(3, 17) then by FLT, $7^{16} \equiv 3^{16} \equiv 1 \pmod{17}$.

Therefore $7^{20} + 3^{20} \equiv 7^4 + 3^4 \equiv 49^2 + 81 \equiv (-2)^2 - 4 \equiv 0 \pmod{17}$.

Hence $7^{20} + 3^{20}$ is divisible by 17.

(ii)

If p is a prime less than 19 then p divides 18!. Therefore p does not divide 18! + 1 since there is a remainder of 1.

Since 19 is a prime then by Wilson's Theorem $(19 - 1)! = 18! \equiv -1 \pmod{19}$.
As $18! + 1 \equiv -1 + 1 \equiv 0 \pmod{19}$ then 18! + 1 is divisible by 19.

Therefore 19 is the smallest prime divisor of 18! + 1.

(iii)

(iii)(a)

As 23 is a prime, then by Theorem 2.2, the length of the cycle in decimal of 1/23 is equal to the order of 10 (modulo 23). Therefore $10^{22} \equiv 1 \pmod{23}$ and 22 is the smallest power of 10 for which this is true.

$10^{22} \equiv (10^{11})^2 \equiv 1 \pmod{23}$. Since 10^{11} cannot be congruent to 1 modulo 23 then
$10^{11} \equiv -1 \pmod{23}$.

(iii)(b)

5/23 has the same cycle as 1/23 but starting at a different point.

As 5 * 043... = 21... then the cycle starts at 21. Therefore the recurring decimal of 5/23 is
0.<217391304347826086956 5>.

Question 5

(i)(a)

If $2^p - 1$ is prime

Since $2^p - 1$ is prime then $\gcd(2^p - 1, 2^{p-1}) = 1$ and $\sigma(2^p - 1) = 1 + 2^p - 1 = 2^p$.

$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\,\sigma(2^p - 1)$ as σ multiplicative
$= (2^p - 1)\,2^p$
$= 2\,\{2^{p-1}(2^p - 1)\}$
A number n is perfect if $\sigma(n) = 2n$. Therefore $2^{p-1}(2^p - 1)$ is perfect if $2^p - 1$ is prime.

If $2^{p-1}(2^p - 1)$ is perfect

As $2^p - 1$ is odd then $\gcd(2^{p-1}, 2^p - 1) = 1$.
$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\,\sigma(2^p - 1)$ Since σ is a multiplicative function
$= (2^p - 1)\,\sigma(2^p - 1)$
$= 2^p\,(2^p - 1)$ as $2^{p-1}(2^p - 1)$ is perfect

This means that $\sigma(2^p - 1) = 2^p$.
As 1 and $2^p - 1$ are factors of $2^p - 1$ then $\sigma(2^p - 1) \geq 1 + (2^p - 1) = 2^p$. As the equality only holds when there are no other factors then $2^p - 1$ is prime.

Therefore $2^{p-1}(2^p - 1)$ is perfect if and only if 2^{p-1} is prime.

(ii)(a)

If $n = p$, where p is a prime, then $\sigma(n) = 1 + p$ and $n + 2\sigma(n) = 2 + 3p \equiv 2 \pmod 3$.
Therefore n cannot be prime if $n + 2\sigma(n)$ is divisible by 3.

(ii)(b)

Assume $n = p^2$, where p is a prime, has the property.
As $\sigma(n) = 1 + p + p^2$ then $n + 2\sigma(n) = 2 + 2p + 3p^2$.
As this is divisible by 3 then $2(1 + p) \equiv 0 \pmod 3$.
Therefore $p \equiv 2 \pmod 3$.

(ii)(c)

If $p = 2$ then $n = 2p = 4$. $\sigma(n) = 1 + 2 + 4 = 7$ and $n + 2\sigma(n) = 18 \equiv 0 \pmod 3$.

If $p \neq 2$ then $\sigma(n) = \sigma(2p) = 1 + 2 + p + 2p = 3(1 + p)$ and $n + 2\sigma(n) = 2p + 6(1 + p)$.
If $n + 2\sigma(n)$ is divisible by 3 then 2p is divisible by 3. Therefore $p = 3$.

Therefore the possible primes for which $n = 2p$ is possible are 2 and 3.

Question 6

(i)

The quadratic congruence has solutions if the discriminant
$5^2 - 4 * 2 * 4 = 25 - 32 = -7$
is a quadratic residue of 31.

$(-7/31) = (24/31)$		Th. 2.1(a). $-7 \equiv 24 \pmod{31}$
$= (2^2/31)(2/31)(3/31)$		Th . 2.1(c)
$= 1 * 1 * (-1)$		Th. 2.1(b), Th. 3.2 and Th. 4.4.
$= -1$		

Therefore the congruence does not have any solutions.

(ii)

$(62/139) = (2/139)(31/139)$	Th. 2.1(c)
$= (-1) * - (139/31)$	Th. 3.2 and LQR. $139 \equiv 31 \equiv 3 \pmod{4}$
$= (-16/31)$	Th. 2.1(a). $139 \equiv -16 \pmod{31}$
$= (-1/31)\ (4^2/31)$	Th. 2.1(c).
$= -1 * 1$	Th. 2.1(e) and Th. 2.1(b)
$= -1$	

(iii)

As $p > 3$ then it is of the form $4k + 1$ or $4k + 3$.

$(3/p) = (p/3)$	if $p \equiv 1 \pmod{4}$. LQR
$= - (p/3)$	if $p \equiv 3 \pmod{4}$. LQR.

As $p > 3$ then it is of the form $3k + 1$ or $3k + 2$.

$(p/3) = (1/3) = 1$	if $p \equiv 1 \pmod{3}$.
$= (2/3) = -1$	if $p \equiv 2 \pmod{3}$.

By the Division Algorithm an odd prime greater than 3 must be of the form
$12k + 1$, $12k + 5$, $12k + 7$, $12k + 11$.

p (mod 12)	p (mod 4)	p (mod 3)	(3/p)
1	1	1	$= (p/3) = (1/3) = 1$
5	1	2	$= (p/3) = (2/3) = -1$
$7 \equiv -5$	3	1	$= - (p/3) = - (1/3) = -1$
$11 \equiv -1$	3	2	$= - (p/3) = - (2/3) = (-1)^2 = 1$

Therefore the given result holds.

Question 7

(i)

Applying the Euclidean algorithm

57 = 1 * 32 + 25
32 = 1 * 25 + 7
25 = 3 * 7 + 4
7 = 1 * 4 + 3
4 = 1 * 3 + 1 = gcd (96, 67)
3 = 3 * 1 + 0

Therefore a continued simple fraction for 57/32 is [1, 1, 3, 1, 1, 3].

k =	**1**	**2**	**3**	**4**	**5**	**6**
p_k	1	2	7	9	16	57
a_k	1	1	3	1	1	3
q_k	1	1	4	5	9	32

Using Unit 7, Th. 1.3a with k = 6 we have $p_6 q_5 - p_5 q_6 = 57 * 9 - 16 * 32 = (-1)^6 = 1$.

As gcd(57, 32) = 1 then, using Unit 1 Theorem 5.1, the general solution of $57x - 32y = 1$ is
x = 9 + 32k, y = 16 + 57k, where k is an integer.
Putting t = 0 gives the least positive value of y and the solution x = 9, y = 16.

(ii)

Let $x = [<1, 2>] = [1, 2, x] = 1 + \cfrac{1}{2 + \frac{1}{x}} = 1 + \dfrac{x}{2x+1} = \dfrac{3x+1}{2x+1}$.

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

$$[0,1,<1,2>] = [0,1,x] = 0 + \cfrac{1}{1 + \frac{1}{x}} = \frac{x}{x+1} = \frac{1+\sqrt{3}}{3+\sqrt{3}} = \frac{1+\sqrt{3}}{3+\sqrt{3}}\frac{3-\sqrt{3}}{3-\sqrt{3}} = \frac{2\sqrt{3}}{9-3} = \frac{\sqrt{3}}{3}$$

For [0, 1, <1, 2>] we have

k =	**1**	**2**	**3**	**4**	**5**	**6**
p_k	0	1	1	3	4	11
a_k	0	1	1	2	1	2
q_k	1	1	2	5	7	19
C_k	0	1	1/2	3/5	4/7	11/19

By Corollary to Theorem 4.1, $|x - C_4| > \dfrac{1}{2q_4q_5} = \dfrac{1}{2*5*7}\dfrac{1}{70} > \dfrac{1}{100}$. Therefore C_4 is not sufficiently accurate.

By Corollary to Theorem 4.1, $|x - C_5| < \dfrac{1}{q_5q_6} = \dfrac{1}{7*19} = \dfrac{1}{133} < \dfrac{1}{100}$.

So C_5 is the 1st convergent accurate to the given periodic continued fraction within 0.01.

Question 8

(i)

A primitive Pythagorean triple is of the form $(2mn, m^2 - n^2, m^2 + n^2)$, where m and n are positive integers, $m > n$, $\gcd(m, n) = 1$, and m and n have opposite parity (Th. 2.1).

(i)(a) Side 14
As the 2nd and 3rd sides are odd then we must have $2mn = 14$.
As $mn = 7$ then it is not possible to choose m and n of opposite parity. Therefore there are no primitive Pythagorean triples with a side of 14.

(i)(b) Side 16
Similarly we must have $2mn = 16$. As $mn = 8$ then $m = 8, n = 1$.
Therefore the only possible primitive Pythagorean triple is $(16, 63, 65)$.

(ii)

$610 = 2 * 5 * 61$.
Since no factor of the form $4k + 3$ occurs to an odd power then 610 can be expressed as the sum of 2 squares (Unit 8, Th. 4.3).

Using the Important Identity for two squares we have
$610 = 5 * 122 = (2^2 + 1^2) * (11^2 + 1^2) = (2*11 + 1*1)^2 + (2*1 - 1*11) = 23^2 + 9^2$.
[[The other solution is $13^2 + 21^2$.]]

$620 = 2 * 5 * 2 * 31$.
Since the factor 31 is of the form $4k + 3$ and it occurs to an odd power then 620 cannot be expressed as the sum of 2 squares (Th. 4.3).

(iii)

$$\sqrt{11} = \frac{m}{n} = \frac{m}{n}\frac{m-3n}{m-3n} = \frac{1}{m-3n}\left(\frac{m^2}{n} - 3m\right) = \frac{1}{m-3n}\left(\frac{m^2}{n^2}n - 3m\right) = \frac{11n-3m}{m-3n}.$$

Since $3 < \sqrt{11} = m/n < 4$ and n is positive then $3n < m < 4n$. So $0 < m - 3n < n$.

Since $0 < m - 3n < n$ then the numerator and denominator of $(11n - 3m) / (m - 3n)$ 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 $\sqrt{11}$ in the given form.

Therefore $\sqrt{11}$ is irrational.

END OF PART 1 SOLUTIONS