Question 1

(i)

156 = 1 * 91 + 65
91 = 1 * 65 + 26
65 = 2 * 26 + 13
26 = 2 * 13 + 0

Therefore gcd(91, 156) = gcd (156, 91) = 13.
[[156 = 12 * 13, 91 = 7 * 13]]

gcd(91, 156) = 13
= 65 – 2 * 26
= 65 – 2 * (91 - 65) = 3 * 65 – 2 * 91
= 3 * (156 - 91) – 2 * 91 = 3 * 156 - 5 * 91.

So x = -5, and y = 3 is a solution of gcd (91, 156) = 13 = 91x + 156y.
Dividing by 13 gives 7x + 12y = 1.
Therefore, by Unit 1, Th. 1.5, the general solution of gcd (91, 156) = 13 = 91x + 156y is
x = -5 + 12k and y = 3 - 7k, where k is an integer.

(ii)

Using the result gcd(qb+r, b) = gcd(b, r) then, as 6n + 3 = (6n – 1) + 4, we have
gcd(6n -1, 6n + 3) = gcd(6n + 3, 6n - 1) = gcd(6n - 1, 4).
Since 6n – 1 is odd and 4 is a power of 2 then gcd(6n - 1, 4) = 1.
Therefore gcd(6n -1, 6n + 3) = 1.

(iii)

Let P(n) be the proposition $1 + 7 + 18 + 34 + \ldots + \tfrac{1}{2} n(5n - 3) = \frac{1}{6} n (n + 1) (5n - 2)$.

P(1) is $1 = \frac{1}{6} * 1 (1 + 1)(5 – 2) = 1$. As P(1) is true then we have the basis for induction.

Assume P(k) is true for some positive integer k.
$1 + 7 + 18 + 34 + \ldots + \tfrac{1}{2} k(5k - 3) + \tfrac{1}{2} (k + 1)[5(k + 1) - 3]$
$= \frac{1}{6} k (k + 1)(5k - 2) + \tfrac{1}{2} (k + 1)(5k + 2)$ (using the induction hypothesis)
$= \frac{1}{6} (k + 1) ((5k^2 - 2k) + (15k + 6)) = \frac{1}{6} (k + 1) (5k^2 + 13k + 6)$
$= \frac{1}{6} (k + 1) (k +2) (5k + 3) = \frac{1}{6} (k + 1) ((k +1) + 1) (5(k + 1) - 2)$.

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)

25 is of the form 6k + 1 but 25 = 5 * 5, and 5 is not of this form.
The statement is **false**.

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

Neither 2 nor 3 is a divisor of a number of the form 6k + 5, where $k \geq 0$

The only primes greater than 3 are of the form 6n + 1 or 6n + 5.

The product of one or more numbers of the form 6n + 1 is also of the form 6n + 1

Therefore a number of the form 6k + 5 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(6m + 1, 6n + 1) = gcd(7, 7) = 7.
Therefore the statement is **false**.

(iv) *[[Since gcd(6, 5) = 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 6k + 5 and these are $p_1, p_2, ..., p_n$.

Let $N = 6(p_1p_2...p_n) - 1$. Since this is of the form 6k + 5 then, by part (ii) it must have a prime factor of the form 6k + 5. Assume this prime is p_i $(1 \leq i \leq n)$.

Since p_i divides N and $6(p_1p_2...p_n)$ then it divides $N - 6(p_1p_2...p_n) = -1$.

Since p_i does not divide -1 then the assumption that there are a finite number of primes of the form 6k + 5 must be false. Therefore there are an infinite number of primes of this form.

Question 3

(i) (2 marks)

Since $n \equiv 3 \pmod{10}$ then $n = 10k + 3$ for some integer k.
Therefore $6n + 1 = 6(10k + 3) + 1 = 60k + 19$.

(i)(a) $6n + 1 = 60k + 19 \equiv 7 \pmod{12}$

(i)(b) $6n + 1 = 60k + 19 \equiv 4 \pmod{15}$

(ii) (3 marks)

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

(iii) (6 marks)

Since $5x \equiv 7 \pmod{19}$ then $4 * 5x = 20x \equiv x \equiv 4 * 7 \equiv 9 \pmod{19}$

By the Chinese remainder theorem the congruences
$x \equiv 1 \pmod{2}$ $x \equiv 6 \pmod{7}$ $x \equiv 9 \pmod{19}$
have a unique solution modulo $2 * 7 * 19 = 266$.

Integers which satisfy the congruence $x \equiv 9 \pmod{19}$ are 9, 28, 47, 66, 85, 104, ...
Integers which also satisfy the congruence $x \equiv 6 \pmod{7}$ are 104, 237, ...
237 also satisfies the congruence $x \equiv 1 \pmod{2}$.

Hence 237 is the unique solution modulo 266.
Therefore the least positive integer which satisfies the congruences is 237.

Question 4

(i)

As gcd(5, 13) = 1 and gcd(3, 13) = 1 then by FLT, $5^{12} \equiv 3^{12} \equiv 1 \pmod{13}$.

Therefore $5^{50} + 3^{30} \equiv 5^2 + 3^6 \equiv -1 + (27)^2 \equiv -1 + 1 \equiv 0 \pmod{17}$.

Hence $5^{50} + 3^{30}$ is divisible by 13.

[[If we didn't have to use the FLT then we would have come to the same conclusion by noting $5^2 = 25 \equiv -1 \pmod{13}$ and $3^3 = 27 \equiv 1 \pmod{13}$.

(ii)(a)
As 19 is a prime then the length of the cycle in a decimal of 1/19 is equal to the order of 10 modulo 19. (Unit 4 Theorem 2.2). As the given cycle length is 18 then the order of 10 modulo 19 is 18.

(ii)(b)

By part (a) $10^{18} \equiv (10^9)^2 \equiv 1 \pmod{19}$. Since 19 is a prime then $x^2 - 1 \pmod{19}$ only has 2 solutions (Lagrange's Theorem) and these are +1 or -1. 10^9 cannot equal +1 since the order of 10 is 18.

Therefore $10^9 \equiv -1 \pmod{19}$.

(ii)(c)

Firstly we find the 1st few digits of 12/19.

$12 = 0 * 19 + 12$
$120 = 6 * 19 + 6$
$60 = 3 * 19 + 3$

Since the recurring decimal of 12/19 is the same as that of 1/19 except that it starts at a different point then 12/19 = 0. <631578947368421052>.

Question 5

(i)(a)

74 = 2 * 37.

As σ is multiplicative then
$\sigma(74) = \sigma(2)\sigma(37) = 3*38 = 114 < 2*74$.
Therefore 74 is not abundant.

(i)(b)

174 = 2 * 87 = 2 * 3 * 29.

As σ is multiplicative then
$\sigma(174) = \sigma(2)\sigma(3)\sigma(29) = 3*4*30 = 360 > 2*174$.
Therefore 174 is abundant.

(i)(c)

If p = 2 then, as σ is multiplicative, $\sigma(10p) = \sigma(20) = \sigma(2^2)\,\sigma(5) = (2^3 - 1)\,6 = 42 > 2 * 20$.

Similarly, if p = 5 then $\sigma(10p) = \sigma(50) = \sigma(2)\,\sigma(5^2) = 3(1 + 5 + 5^2) = 93 < 2 * 50$.

If p is an prime other than 2 or 5 then $\sigma(10p) = \sigma(2)\,\sigma(5)\,\sigma(p) = 3 * 6 * (p + 1)$.
$18p + 18 > 20p$ if $p < 9$. So 10p is abundant when p = 3 or 7.

Therefore 10p is abundant when p = 2, 3, or 7.

[[$\sigma(30) = 3 * 4 * 6 = 72$, and $\sigma(70) = 3 * 6 * 8 = 144$.]]

(ii)

Since p is an odd prime and ϕ is multiplicative then $\phi(4p) = \phi(4)\,\phi(p) = 2(p - 1)$.

Since 2p - 1 is an odd prime and ϕ is multiplicative then
$\phi(4p - 2) = \phi(2)\,\phi(2p - 1) = 1 * (2p - 2) = 2(p - 1)$.

Therefore $\phi(4p) = \phi(4p - 2)$.

Question 6

(i) (4 marks)

The quadratic congruence has solutions if $(-5)^2 - 4 * 2 * 4 = 25 - 32 = -7$ is a quadratic residue of 19.

$(-7/19) = (12/19)$	Th. 2.1(a), $-7 \equiv 12 \pmod{19}$
$= (2^2/19)(3/19)$	Th. 2.1(c).
$= 1 * (-1) = -1$	Th. 2.1(b), and Th. 4.4.

Therefore the congruence does not have solutions.

(ii) (4 marks)

$(86/127) = (2/127)\,(43/127)$	Th. 2.1(c).
$= 1 * \{-(127/43)\}$	Th. 3.2, LQR. $127 \equiv 43 \equiv 3 \pmod{4}$.
$= -(-2/43)$	Th. 2.1(a). $127 \equiv -2 \pmod{43}$.
$= -(-1/43)\,(2/43)$	Th. 2.1(c).
$= -\{-1 * (-1)\} = -1$	Th. 2.1(e). Th. 3.2.

(iii) (4 marks)

If $p = 2$ or $p = 3$ then $(6/p)$ is not defined (See Glossary).

If $p \geq 5$ then

$(6/p) = (2/p)\,(3/p)$ Th. 2.1(c).

If $(6/p) = 1$ then either $(2/p) = (3/p) = 1$, or $(2/p) = (3/p) = -1$.

Case 1. $(2/p) = (3/p) = 1$

If $(2/p) = 1$ then $p \equiv \pm 1 \pmod{8}$. If $(3/p) \equiv 1$ then $p \equiv \pm 1 \pmod{12}$.
As lcm(8, 12) = 24 then we consider values of p modulo 24.
As $p \equiv \pm 1 \pmod{12}$ then possible values are 1, 11, 13, and 23.
Therefore the values which satisfy both equations are 1 and 23 (mod 24).

Case 2. $(2/p) = (3/p) = -1$

If $(2/p) = -1$ then $p \equiv 3$ or 5 (mod 8). If $(3/p) \equiv 1$ then $p \equiv 5$ or 7 (mod 12).
As lcm(8, 12) = 24 then we consider values of p modulo 24.
As 5 or 7 (mod 12) then possible values are 5, 7, 17, and 19.
The values which satisfy both equations are 5 and 19 (mod 24).

Therefore $(6/p) = 1$ when $p \equiv \pm 1 \pmod{24}$ or $p \equiv \pm 5 \pmod{24}$.

Question 7

(i) (4 marks)

82 = 1 * 69 + 13
69 = 5 * 13 + 4
13 = 3 * 4 + 1
4 = 4 * 1 + 0

Therefore 82/69 = [1, 5, 3, 4]
= [1, 5, 3, 3, 1], using Second continued fraction identity.

(ii) (7 marks)

Let $\alpha = [0, 2, x]$ where $x = [<2, 1>] = [2, 1, x]$.

The convergents of [2, 1, x] are 2/1, 3/1, (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 [0, 2, x] are 0/1, 1/2, x/(2x + 1) = α.

This gives $[0,2,\langle 2,1\rangle] = \frac{1+\sqrt{3}}{3+2\sqrt{3}} = \frac{(1+\sqrt{3})(3-2\sqrt{3})}{9-12} = \frac{(3-6)+\sqrt{3}(3-2)}{-3} = \frac{3-\sqrt{3}}{3}$.

$\alpha = [0, 2, 2, 1, 2, 1, 2, 1, <1, 2>]$.
Convergents of α are $C_1 = 0/1$; $C_2 = 1/2$; $C_3 = 2/5$; $C_4 = 3/7$;
$C_5 = 8/19$; $C_6 = 11/26$; $C_7 = 30/71$.

By Corollary to Theorem 4.1 $\frac{1}{2q_k q_{k+1}} < \left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}}$, where $C_k = p_k / q_k$.

When k = 5 we have $|\alpha - C_5| < 1/(19 * 26) < 1/400$.
When k = 4 we have $1/(2*7*19) = 1/(14 * 19) = 1/266 < |\alpha - C_4|$.

Therefore the 5th convergent 8/19 is the 1st convergent within 1/400 of $[0,2, <2, 1>]$

Question 8

(i) (4 marks)

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 20
As the 2nd and 3rd sides are odd then we must have $2mn = 20$.
As $mn = 10$ then it possible values are $m = 10, n = 1$; $m = 5, n = 2$.
Therefore the possible primitive Pythagorean triples are (20, 99, 101) and (20, 21, 29).

(i)(b) Side 22
Similarly we must have $2mn = 22$. As $mn = 11$ then it is not possible to choose m and n of opposite parity. Therefore there are no primitive Pythagorean triples with a side of 22.

(ii) (3 marks)

$360 = 6 * 6 * 10 = 2^3 * 3^2 * 5$. Since no factor of the form $4k + 3$ occurs to an odd power then 360 can be expressed as the sum of 2 squares (Th. 4.3).

$364 = 4 * 91 = 4 * 7 * 13$. Since a factor of the form $4k + 3$ occurs to an odd power then 364 cannot be expressed as the sum of 2 squares (Th. 4.3).

$360 = 36 * 10 = 6^2 * (3^2 + 1^2) = 18^2 + 6^2$.

(iii) (4 marks)

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

Since $2 < \sqrt{8} = m/n < 3$ and n is positive then $2n < m < 3n$. So $0 < m - 2n < n$.

Since $0 < m - 2n < n$ then the numerator and denominator of $(8n - 2m) / (m - 2n)$ 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 NUMBER THEORY SOLUTIONS