Question 1

(i)

899 = 1 * 493 + 406
493 = 1 * 406 + 87
406 = 4 * 87 + 58
87 = 1 * 58 + 29
58 = 2 * 29 + 0

Therefore gcd(899, 493) = 29. [[899 = 31 * 29, 493 = 17 * 29]]

gcd(899, 493) = 29
= 87 – 58
= 87 – (406 – 4 * 87) = 5 * 87 – 406
= 5 * (493 - 406) – 406 = 5 * 493 - 6 * 406
= 5 * 493 – 6 * (899 – 493) = 11 * 493 – 6 * 899.

So x = -6, and y = 11 is a solution of gcd (899, 493) = 29 = 899x + 493y.
Dividing by 29 gives 31x + 17y = 1.
Therefore, by Unit 1, Th. 5.1, the general solution of gcd (899, 493) = 899x + 493y is
x = -6 + 17k and y = 11 - 31k, where k is an integer.

(ii)

Using the result gcd(qb+r, b) = gcd(b, r) then, as 8n + 5 = (8n – 1) + 6, we have
gcd(8n -1, 8n + 5) = gcd(8n + 5, 8n - 1) = gcd(8n - 1, 6).
So possible values for gcd(8n – 1, 8n + 5) are 1, 2, 3, or 6.
As 8n – 1 is odd the gcd cannot be even so gcd(8n – 1, 8n + 5) is 1 or 3.

When n = 1, gcd(8n – 1, 8n + 5) = gcd(7, 13) = 1.
When n = 2, gcd(8n – 1, 8n + 5) = gcd(15, 21) = 3.
Therefore both 1 and 3 are possible.

(iii)
Let P(n) be the proposition $9 + 31 + 65 + ... + (6n^2 + 4n - 1) = n (n + 2) (2n + 1)$.

P(1) is $9 = 1 (1 + 2)(2 * 1 + 1) = 9$. As P(1) is true then we have the basis for induction.

Assume P(k) is true for some positive integer k.
$9 + 31 + 65 + ... + (6k^2 + 4k – 1) + [6(k + 1)^2 + 4(k + 1) – 1] =$
$= k (k + 2) (2k + 1) + [6k^2 + 16k + 9]$ (using the induction hypothesis)
[[Our target is $(k + 1) ((k + 1) + 2) (2(k + 1) + 1) = (k + 1)(k +3)(2k + 3)$]]
$= 2k^3 + 5k^2 + 2k + [6k^2 + 16k + 9] = 2k^3 + 11k^2 + 18k + 9$
$= (k + 1) (2k^2 + 9k + 9) = (k + 1)(k +3)(2k + 3) = (k + 1) ((k + 1) + 2) (2(k + 1) + 1)$.

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

Assume there are a finite number of primes of the form 3k + 2, where k is a non-negative integer. Let these primes be $p_1, p_2, \ldots, p_r$.

Let $N = (p_1 p_2 \ldots p_r)^2 + 1$.

If p is of the form 3k + 2 then $p \equiv 2 \pmod 3$ and $p^2 \equiv 1 \pmod 3$.
Therefore $N \equiv 1^r + 1 \equiv 2 \pmod 3$. Therefore N is of the form 3k + 2, where k is a non-negative integer.

As N is greater than any of the primes of the form 3k + 2 then it cannot be a prime.

As N is not divisible by 3 then all of its prime factors must be of the form 3k + 1 or 3k+2.

Dividing N by a prime of the form 3k + 2 leaves a remainder of 1 so none of the prime factors can be of this form. Therefore all of the prime factors must be of the form 3k + 1.

If all the prime factors of the form $3k + 1 \equiv 1 \pmod 3$ then multiplying them together results in a number equal to 1 (mod 3). Since $N \equiv 2 \pmod 3$ then all the factors cannot be of the form 3k + 1.

Since the assumption there are a finite number of primes of the form 3k + 2 has lead to a contradiction then the assumption is incorrect. Therefore there are an infinite number of primes of the form 3k + 2.

Question 3

(i) (2 marks)

Since $n \equiv 3 \pmod 8$ then $n = 8k + 3$ for some integer k.
Therefore $5n + 3 = 5(8k + 3) + 3 = 40k + 18$.

(i)(a) $5n + 3 = 40k + 18 \equiv 2 \pmod 4$. So 2 is the least positive residue mod 4.

(i)(b) $5n + 3 = 40k + 18 \equiv 18 \pmod{20}$. So 18 is the least positive residue mod 20.

(ii) (4 marks) [[Same as 2007 Qu. 3 (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 $ac - bd = n(bt + sd + stn)$ and $bt + sd + stn$ is an integer then, by the definition of congruence,

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

(iii) (5 marks)

[[Get all congruences in to the form $x \equiv a \pmod p$ so we can use the Chinese Remainder theorem]]

$2x \equiv 7 \pmod 5 \Leftrightarrow 6x \equiv 21 \pmod 5 \Leftrightarrow x \equiv 1 \pmod 5$.
[[We now have the equations given in 2007 Qu. 3 (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

$$15, 32, 49, 66, 83, 100, 117, 134, 151, \ldots \quad [[\ 151 = 10 * 15 + 1\ ]]$$

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

Question 4

[[This question is identical to 2004 Qu. 4.]]

(i) (3 marks)

As 37 is a prime and gcd(10, 37) = 1 then, by the FLT, $10^{36} \equiv 1 \pmod{37}$.
Therefore $10^{75} \equiv (10^{36})^2 * 10^3 \equiv 1^2 * 100 * 10 \equiv -11 * 10 \equiv -110 \equiv 1 \pmod{37}$.

Therefore the least positive residue is 1.

(ii)(a) (4 marks)

$12x \equiv 1 \pmod{37}$
$\Rightarrow 36x \equiv 3 \pmod{37}$
$\Rightarrow -x \equiv 3 \pmod{37}$
$\Rightarrow x \equiv 34 \pmod{37}$

As 37 is a prime and gcd(12, 37) = 1 then, by the FLT, $12^{36} \equiv 1 \pmod{37}$.
Therefore as $12 * 12^{35} \equiv 1 \pmod{37}$ then $12^{35} \pmod{37}$ is also a solution of $12x \equiv 1 \pmod{37}$. As this congruence has a unique solution (Unit 3 Th. 3.2(b)) then 34 is equal to the least positive residue of $12^{35} \pmod{37}$.

(ii)(b) (4 marks)

$12^2x \equiv 144x \equiv 33x \equiv 1 \pmod{37}$ has a solution congruent to $12^{34} \pmod{37}$.

$12^2x \equiv 1 \pmod{37}$
$\Rightarrow (36)^2x \equiv 3^2 \pmod{37}$
$\Rightarrow (-1)^2x \equiv 9 \pmod{37}$
$\Rightarrow x \equiv 9 \pmod{37}$

Therefore 9 is equal to the least positive residue of $12^{34} \pmod{37}$.

Question 5

[[Same as 2007 Qu. 5 except 150 instead of 140 in part (i).]]

(i)

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 $150 = 6 * 25 = 2 * 3 * 5^2$ then $\sigma(150) = \sigma(2)\ \sigma(3)\ \sigma(5^2) = 3 * 4 * \frac{5^3 - 1}{5 - 1} = 12 * 31$.
As 150 is not divisible by 31 then 150 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)

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

If n is 3-perfect then $32(2^{r+1} - 1) = 3n = 2^r * 3^2 * 7$.
As $(2^{r+1} - 1)$ is odd 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) (3 marks)

The quadratic congruence has solutions if $(-7)^2 - 4 * 1 * 9 = 49 - 36 = 13$ is a quadratic residue of 29.

$(13/29) = (-16/29)$	Th. 2.1(a), $13 \equiv -16 \pmod{29}$
$= (-1/29)(4^2/29)$	Th. 2.1(c).
$= 1 * 1 = 1$	Th. 2.1(e), and Th. 2.1(b). $29 \equiv 1 \pmod 4$

Therefore the congruence does have solutions.

[[$x^2 - 7x + 9 \equiv x^2 + 22x + 9 \equiv (x + 11)^2 - 112 \equiv (x + 11)^2 - 25 \equiv 0 \pmod{29}$.
So $x = +5 - 11 = -6$ or $x = -5 - 11 = -16$ are solutions.]]

(ii) (4 marks)

$(227/239) = (-12/239)$	Th. 2.1(a), $227 \equiv -12 \pmod{239}$
$= (-1/239)\,(2^2/239)(3/239)$	Th. 2.1(c).
$= -1 * 1 * 1$	Th. 2.1(e), 2.1(b), 4.4. $239 \equiv 3 \pmod 4$, $239 \equiv -1 \pmod{12}$.
$= -1$	

(iii) (4 marks) [[Same as 2007 Qu. 6 (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
$4k + 4, \ldots, 8k + 4$.

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

Since $(-1)^{2k+1} = -1$ then, by Gauss' Lemma,
2 is a quadratic non-residue of any prime of the form $8k + 5$.

Question 7

(i) (2 marks)

173 = 4 * 39 + 17
39 = 2 * 17 + 5
17 = 3 * 5 + 2
5 = 2 * 2 + 1
2 = 2 * 1 + 0

Therefore 173/39 = [4, 2, 3, 2, 2]
= [4, 2, 3, 2, 1, 1], using Second continued fraction identity.

(ii) (4 marks) [[Same as 2007 Qu 7(ii).]]

Using Theorem 1.2 and Corollary 1.2 we have

$p_1 = 1$; $q_1 = 1$;
$p_2 = 1 * 2 + 1 = 3$; $q_2 = 2$;
$p_3 = 3 * 3 + 1 = 10$; $q_3 = 3 * 2 + 1 = 7$;
$p_4 = 4 * 10 + 3 = 43$; $q_4 = 4 * 7 + 2 = 30$,

and so the first 4 convergents are $C_1 = 1/1 = 1$; $C_2 = 3/2$; $C_3 = 10/7$; and $C_4 = 43/30$.

$q_5 = 5 * 30 + 7 = 157$. Therefore, using the Corollary to Theorem 2.1, we have

$| x - C_4 | < 1/ (q_4 q_5) = 1 / (30 * 157) = 1/ 4710$.

Linda Brown has pointed out that we do not need to calculate q_5 if we use Theorem 1.4.
$| x - C_4 | \leq 1/ (2q_3 q_4) = 1/ 420$.

(ii) (5 marks)

Let $\alpha = [2, 2, x]$ where $x = [<3>] = [3, x]$.
The convergents of [3, x] are 3/1, (3x + 1)/x = x.
So $x^2 - 3x - 1 = 0$ and this has the positive solution $x = \frac{3+\sqrt{3^2+4*1*1}}{2} = \frac{3+\sqrt{13}}{2}$.

The convergents of [2, 2, x] are 2/1, 5/2, (5x + 2)/(2x + 1) = α.

This gives $[2,2,\langle 3\rangle] = \frac{10x+4}{4x+2} = \frac{19+5\sqrt{13}}{8+2\sqrt{13}} = \frac{(19+5\sqrt{13})(8-2\sqrt{13})}{64-52}$

$= \frac{(152-130)+(40-38)\sqrt{13}}{12} = \frac{11+\sqrt{13}}{6}$

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 30
As the 2nd and 3rd sides are odd then we must have $2mn = 30$. As $mn = 15$ then it is not possible to choose m and n of opposite parity. Therefore there are no primitive Pythagorean triples with a side of 30.

(i)(b) Side 32
Similarly we must have $2mn = 32$.
As $mn = 16$ then the only possible values of opposite parity are $m = 16$ and $n = 1$.
Therefore the only possible primitive Pythagorean triple is (32, 255, 257).

(ii) (3 marks) [[2009 Qu. 8 (ii) used 610 and 620 = 1240/2.]]

$610 = 2 * 5 * 61$.
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
$610 = 5 * 122 = (2^2 + 1^2) * (11^2 + 1^2) = (2*11 + 1*1)^2 + (2*1 - 1*11)^2 = 23^2 + 9^2$.
[[The other solution is $13^2 + 21^2$.]]

$1240 = 2 * 5 * 4 * 31$.
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) (4 marks)

$$\sqrt{3} = \frac{m}{n} = \frac{m}{n}\frac{m-n}{m-n} = \frac{m^2 - mn}{n(m-n)} = \frac{3n^2 - mn}{n(m-n)} = \frac{3n - m}{m-n} \quad .$$

Since $1 < \sqrt{3} < 2$ and n is positive then $n < \sqrt{3}n = m < 2n$. So $0 < m - n < n$.

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

Therefore $\sqrt{3}$ is irrational.

END OF NUMBER THEORY SOLUTIONS