[[Comments are written like this.
Please send me (dave@wildd.freeserve.co.uk) details of any errors you find or suggestions for improvements.]]

Question 1

(i) (4 marks)

230 = 2 * 103 + 24
103 = 4 * 24 + 7
24 = 3 * 7 + 3
7 = 2 * 3 + 1
3 = 3 * 1 + 0

Therefore as gcd(230, 103) = 1 then 230 and 103 are relatively prime.

1 = 7 – 2 * 3
= 7 - 2 * (24 - 3 * 7) = 7 * 7 - 2 * 24
= 7 * (103 - 4 * 24) – 2 * 24 = 7 * 103 - 30 * 24
= 7 * 103 - 30 * (230 - 2 * 103) = 67 * 103 - 30 * 230.

Therefore 103x - 230y = 1 when x = 67 and y = 30.

(ii) (4 marks)

Let P(n) be the proposition
$1 + 5 + 12 + 22 + ... + ½ n(3n -1) = ½ n^2 (n + 1)$.

P(1) is $1 = ½ * 1^2 * (1 + 1)$.
As P(1) is true then we have the basis for induction.

Assume P(k) is true for some positive integer k.

$1 + 5 + 12 + 22 + ... + ½ k(3k -1) + ½ (k + 1)[3(k + 1) -1]$
$= ½ k^2 (k + 1) + ½ (k + 1)(3k + 2)$ (using the induction hypothesis)
$= ½ (k + 1) (k^2 + 3k +2) = ½ (k + 1)^2 (k +2)$.

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**.**

(iii) (3 marks)

gcd(a, b) = 1 ⇒ gcd(a, -b) = 1 ⇒ gcd(a, a - b) = 1.
Therefore if c | a -b then gcd(a, c) = 1.

[[Alternatively. Since gcd(a,b) = 1 then we can write 1 = αa - βb = (α - β)a + β(a - b), where α and β are integers. As c | a - b then we can write 1 = ma + nc for some integers m and n. As 1 can be expressed in this form then gcd (a, c) = 1.]]

Question 2 (11 marks)

(i)

False. $87 = 29 * 3 = 17 * 5 + 2$. The prime divisors 29 and 3 are not of the form $17m + 2$.

As 2 is of the form $17m + 2$ then we only need to consider odd values of m.

(ii)

Any prime greater than 3 can be expressed in the form
$12k + 1, 12k + 5, 12k + 7, 12k + 11$.

$1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$. Therefore if $p > 3$ is a prime then p^2 is of the form $12k + 1$.

Therefore the statement is **true**.

(iii)

Any twin primes greater than 3 must either be of the form
$12m + 5, 12m + 7$
or $12m + 11, 12(m + 1) + 1$.

In both cases the sum of the primes is divisible by 12. Therefore the statement is **true**.

Question 3

(i) (1 mark)

Since $n \equiv 5 \pmod{10}$ then $n = 10k + 5$ for some integer k.
Therefore $6n + 1 = 6(10k + 5) + 1 = 60k + 31$.

As $6n + 1 \equiv 7 \pmod{12}$ then the least positive residue modulo 12 of $6n + 1$ is 7.

(ii) (4 marks)

Let $0 \le i, j \le n - 1$.

If $c + ia \equiv c + ja \pmod{n}$ then $ia \equiv ja \pmod{n}$.
Since $\gcd(a, n) = 1$ then a can be cancelled to give $i \equiv j \pmod{n}$.

Therefore none of the values $c, c + a, c + 2a, \ldots , c + (n - 1)a$ are congruent modulo n. As there are n of these values then they form a complete set of residues modulo n.

(iii) (6 marks)

By the Chinese Remainder theorem these equations have a unique solution modulo $3*4*13 = 156$.

Integers which satisfy the congruence $x \equiv 7 \pmod{13}$ are 7, 20, 33, ...
Integers which also satisfy the congruence $x \equiv 1 \pmod{4}$ are 33, 85, 137, ...
Integers which also satisfy the congruence $x \equiv 2 \pmod{3}$ are 137, ...

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

Question 4

(i) (3 marks)

By 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)

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

By 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 equation has a unique solution 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

(i) (5 marks)

If $2^p - 1$ is prime

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

$$\begin{aligned}\sigma(2^{p-1}(2^p - 1)) &= \sigma(2^{p-1})\,\sigma(2^p - 1) && \text{as } \sigma \text{ multiplicative}\\ &= (2^p - 1)\,2^p\\ &= 2\,\{2^{p-1}(2^p - 1)\}\end{aligned}$$

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

$$\begin{aligned}\sigma(2^{p-1}(2^p - 1)) &= \sigma(2^{p-1})\,\sigma(2^p - 1) && \text{Since } \sigma \text{ is a multiplicative function}\\ &= (2^p - 1)\,\sigma(2^p - 1)\\ &= 2^p\,(2^p - 1) && \text{as } 2^{p-1}(2^p - 1) \text{ is perfect}\end{aligned}$$

This means that $\sigma(2^p - 1) = 2^p$.
As 1 and $2^p - 1$ are factors of $2^p - 1$ then $\sigma(2^p - 1) \le 1 + (2^p - 1) = 2^p$. As the equality only holds when $2^p - 1$ is prime 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) (2 marks)

$110 = 11 * 5 * 2$.
$\sigma(110) = \sigma(11)\,\sigma(5)\,\sigma(2) = 12 * 6 * 3 = 72 * 3 = 216$.

$112 = 4 * 28 = 2^4 * 7$.
$\sigma(112) = \sigma(2^4)\,\sigma(7) = (2^5 - 1) * 8 = 31 * 8 = 248$.

Therefore only 112 is abundant.

(ii)(b) (4 marks)

If $n = 4p^2$ where p is an odd prime then

$$\sigma(n) = \sigma(2^2)\,\sigma(p^2) = (2^3 - 1)\,(1 + p + p^2).$$

If $4p^2$ is abundant then $7(1 + p + p^2) > 8p^2$. So $p^2 < 7(p + 1)$ or $p < 7 + \frac{7}{p}$.

Therefore $4p^2$ is abundant only for the odd primes 3, 5, or 7.

Question 6

(i) (3 marks)

The quadratic congruence has solutions if

$5^2 - 4 * 2 * 4 = 25 - 32 = -7$

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) (4 marks)

(62/139)	= (2/139)(31/139)	Th. 2.1(c)
	= (-1) * -(139/31)	Th. 3.2 and LQR. $139 \equiv 31 \equiv 3 \pmod 4$
	= (15/31)	Th. 2.1(a). $139 \equiv 15 \pmod{31}$
	= (-16/31)	Th. 2.1(a). $15 \equiv -16 \pmod{31}$
	$= (-1/31)(4^2/31)$	Th. 2.1(c).
	= -1 * 1	Th. 2.1(e) and Th. 2.1(b)
	= -1	

(iii) (4 marks)

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

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

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) (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].

(ii) (7 marks)

Let α = [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 $x = \dfrac{2+\sqrt{4+8}}{2} = 1+\sqrt{3}$.

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

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

α = [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 $\dfrac{1}{2q_k q_{k+1}} < \left|\alpha - \dfrac{p_k}{q_k}\right| < \dfrac{1}{q_k q_{k+1}}$, 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)

Since the cycle length of $\sqrt{11}$ is 2 then every even convergent gives a solution of the Diophantine equation (Th. 1.2).

Convergents of [3, <3, 6>] are $C_1 = 3/1$; $C_2 = 10/3$; $C_3 = 63/19$; $C_4 = 199/60$.

Therefore 2 positive solutions are x = 10, y = 3; and x = 199, y = 60.

$199^2 = (200 - 1)^2 = 40{,}000 - 400 + 1 = 39{,}601$. $11 * 60^2 = 11 * 3600 = 39{,}600$.

(ii) (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).

As the 2nd and 3rd sides are odd then we must have 2mn = 12.
As mn = 6 then m = 6, n = 1, and m = 3, n = 2 are the only possibilities.

Therefore the only primitive Pythagorean triples are (12, 35, 37) and (12, 5, 13).

Since (4, 3, 5) is a primitive Pythagorean triple then (16, 12, 20) is a non-primitive Pythagorean triple with 12 as a side.

(iii) (3 marks)

Assume that $x = x_1$, $y = y_1$, $z = z_1$ is a solution in positive integers.
Therefore $x_1^3 + 9y_1^3 = 3z_1^3$

Since the other 2 terms in the equation are divisible by 3 then x_1^3 is also divisible by 3. Therefore we can write $x_1 = 3x_2$ where x_2 is a positive integer.
Therefore $27x_2^3 + 9y_1^3 = 3z_1^3$. Dividing by 3 gives $9x_2^3 + 3y_1^3 = z_1^3$.

Similarly z_1^3 is also divisible by 3. Therefore we can write $z_1 = 3z_2$ where z_2 is a positive integer.
Hence $9x_2^3 + 3y_1^3 = 27z_2^3$. Dividing by 3 gives $3x_2^3 + y_1^3 = 9z_2^3$.

Similarly y_1^3 is also divisible by 3. Therefore we can write $y_1 = 3y_2$ where y_2 is a positive integer.
So $3x_2^3 + 27y_2^3 = 9z_2^3$. Dividing by 3 gives $x_2^3 + 9y_2^3 = 3z_2^3$.

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

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