Question 1

(i) (4 marks)

253 = 1 * 187 + 66
187 = 2 * 66 + 55
66 = 1 * 55 + 11
55 = 5 * 11 + 0

Therefore gcd(187, 253) = 11. [[253 = 23 * 11, 187 = 17 * 11]]

gcd(187, 253) = 11 = 66 – 55
= 66 – (187 – 2 * 66) = 3 * 66 – 187
= 3 * (253 - 187) – 187 = 3 * 253 - 4 * 187.

So x = -4, and y = 3 is a solution of gcd (187, 253) = 11 = 187x + 253y.
Dividing by 11 gives 17x + 23y = 1.
Therefore, by Unit 1, Th. 5.1, the general solution of gcd (187, 253) = 187x + 253y is
x = -4 + 23k and y = 3 - 17k, where k is an integer.

(ii) (3 marks)

Using the result gcd(qb+r, b) = gcd(b, r) then, as 12n + 3 = 3 * (4n + 3) - 6, we have
gcd(12n + 3, 4n + 3) = gcd(4n + 3, -6).
So possible values for gcd(12n + 3, 4n + 3) are the divisors of 6.
As 4n + 3 is odd the gcd cannot be even. So possible values of gcd(12n + 3, 4n + 3) are 1 and 3.

As 3 | 12n + 3 then gcd(12n + 3, 4n + 3) = 3 if and only if 3 | 4n + 3.
So gcd(12n + 3, 4n + 3) = 3 if 3 | n and it equals 1 otherwise.

(iii) (4 marks)

Let P(n) be the proposition $3 + 6 + 10 + ... + ½ (n + 1)(n + 2) = \frac{1}{6}[(n + 1)(n + 2)(n + 3) - 6]$.

P(1) is $3 = \frac{1}{6} * [(1 + 1)(1 + 2)(1 + 3) - 6] = \frac{1}{6} * (24 – 6) = 3$. As P(1) is true then we have the basis for induction.

Assume P(k) is true for some positive integer k.
$3 + 6 + 10 + ... + ½ (k + 1)(k + 2) + ½ [(k + 1) + 1][(k + 1) + 2]$
$= \frac{1}{6}[(k + 1)(k + 2)(k + 3) - 6] + ½ (k + 2)(k + 3)$ (using the induction hypothesis)
$= \frac{1}{6}\{(k + 2)(k + 3)[(k + 1) + 3] – 6\}$
$= \frac{1}{6}\{[(k + 1) + 1][(k + 1) + 2][(k + 1) + 3] – 6\}$

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 (11 marks)

(i)

If m is even then 17m + 2 is also even, and so 2 is a divisor. As 2 is of the form 17m + 2 then in these cases the number has a divisor of the same form.

When m = 1 or 3 then 17m + 2 is 19 or 53. These are both prime numbers of the form 17m + 2.

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

Therefore the statement is **false**.

(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) (3 marks)

Since $n \equiv 4 \pmod 6$ then $n = 6k + 4$ for some integer k.
Therefore $10n + 3 = 10(6k + 4) + 3 = 60k + 43$.

(i)(a) $10n + 3 = 60k + 43 \equiv 3 \pmod 4$. So 3 is the least positive residue mod 4.

(i)(b) $10n + 3 = 60k + 43 \equiv 13 \pmod{15}$. So 13 is the least positive residue mod 15.

(ii) (3 marks)

Since $a \equiv b \pmod n$ then, by the definition of congruence, $a - b = sn$, for some integer s.
So $a^2 = (b + sn)^2 = b^2 + n(2bs + s^2n)$.
Since $a^2 - b^2 = n(2bs + s^2n)$, and $2bs + s^2n$ is an integer then, by the definition of congruence,
$a^2 \equiv b^2 \pmod n$.

(iii) (5 marks)

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

$3x + 4 \equiv 6 \pmod 7 \Leftrightarrow 3x \equiv 2 \pmod 7 \Leftrightarrow 15x \equiv 10 \pmod 7 \Leftrightarrow x \equiv 3 \pmod 7$.
$7x \equiv 9 \pmod{11} \Leftrightarrow -21x \equiv -27 \pmod{11} \Leftrightarrow x \equiv 6 \pmod{11}$.

As 4, 7, and 11 are relatively prime in pairs then we can use the Chinese Remainder theorem.
Therefore the equations
$x \equiv 3 \pmod 4$, $x \equiv 3 \pmod 7$, and $x \equiv 6 \pmod{11}$
have a unique solution modulo $4 * 7 * 11 = 28 * 11 = 308$.

Integers which satisfy the congruence $x \equiv 6 \pmod{11}$ are 6, 17, ... Steps of 11
Integers which also satisfy the congruence $x \equiv 3 \pmod 7$ are 17, 94, 171, ... Steps of 77
Integers which also satisfy the congruence $x \equiv 3 \pmod 4$ are 171, ...

Therefore the least positive integer which satisfies the linear congruences is 171.

[[As $x \equiv 3$ modulo 4 and 7 we could immediately deduce $x \equiv 3 \pmod{28}$. It does not seem to help here.]]

Question 4

(i) (4 marks)

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) (3 marks)

As 19 is a prime and gcd (35, 19) = 1 then by FLT, $35^{18} \equiv 1 \pmod{19}$.

Therefore $35^{42} = (35^{18})^2\, 35^6 \equiv (1)^2 (-3)^6 \equiv 81 * 9 \equiv 5 * 9 \equiv 7 \pmod{19}$.

[[$35^{42} \equiv (-3)^{42} \equiv 9 * 81^{10} \equiv 9 * 5^{10} \equiv 9 * 25^5 \equiv 9 * 6^5 \equiv 54 * 36^2 \equiv -3 * (-2)^2 \equiv -12 \equiv 7 \pmod{19}$]]

(ii)(b) (4 marks)

130 = 2 * 5 * 13.

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

$a^2 \equiv a \pmod 2$. Therefore $a^{25} \equiv a \pmod 2$.
$a^5 \equiv a \pmod 5$. 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
$a^{25} \equiv a \pmod{130}$.

Question 5

(i)(a) (2 marks)

165 = 3 * 5 * 11. As σ is multiplicative then
$\sigma(165) = \sigma(3)\,\sigma(5)\,\sigma(11) = 4 * 6 * 12 = 2 * 144 < 2 * 165$.
Therefore 165 is not abundant.

$112 = 4 * 28 = 2^4 * 7$. As σ is multiplicative then
$\sigma(112) = \sigma(2^4)\,\sigma(7) = (2^5 - 1) * 8 = 2 * 128 > 2 * 112$.
Therefore 112 is abundant.

(i)(b) (5 marks)

As p is an odd prime then $\sigma(4p^2) = \sigma(2^2)\,\sigma(p^2) = \left(2^3 - 1\right)\frac{p^3 - 1}{p - 1} = 7\left(p^2 + p + 1\right)$.

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

As p is an odd prime then $4p^2$ is abundant when p = 3, 5, or 7.

(ii) (4 marks)

Since $p > 3$ is prime, and ϕ is multiplicative then
$\phi(6p) = \phi(2)\phi(3)\,\phi(p) = 1 * 2 * (p - 1) = 2(p - 1)$.

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 $\phi(6p) = \phi(4p - 2)$.

Question 6

(i) (3 marks)

The quadratic congruence has solutions if $5^2 - 4 * 7 * 1 = -3$ 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.
$= -1.$

Therefore the congruence does not have solutions.

(ii) (3 marks)

$(167/193) = (360/193)$ Th. 2.1(a), $167 \equiv 360 \pmod{193}$.
$= (6^2/193)(2/193)(5/193)$ Th. 2.1(c).
$= 1 * 1 * (193/5)$ Th. 2.1(b), 3.2, and 4.2.
$= (3/5)$ Th. 2.1(a), $193 \equiv 3 \pmod 5$.
$= -1.$ Th. 4.4.

(iii) (5 marks) Solution by Linda Brown

$(p/7) = 1 \Leftrightarrow p$ is a quadratic residue of $7 \Leftrightarrow X^2 \equiv p \pmod 7$ has solutions
The quadratic residues mod 7 are 1, 2 and 4 ($1^2 \equiv 1 \equiv 6^2$, $2^2 \equiv 4 \equiv 5^2$, $3^2 \equiv 2 \equiv 4^2$)
So $p \equiv 1, 2$ or $4 \pmod 7$, $p \neq 7$ (1)

If $p \equiv 1 \pmod 4$ LQR gives $(7/p) = (p/7) = 1$, (2)
Combining (1) & (2):
$p \equiv 1 \pmod 7$ & $p \equiv 1 \pmod 4$ $\Rightarrow p \equiv 1 \pmod{28}$
$p \equiv 2 \pmod 7$ & $p \equiv 1 \pmod 4$ $\Rightarrow p \equiv 9 \pmod{28}$
$p \equiv 4 \pmod 7$ & $p \equiv 1 \pmod 4$ $\Rightarrow p \equiv 25 \pmod{28}$

Also if $p \equiv 3 \pmod 4$ (3)
By LQR $(7/p) = (-1)(p/7) = 1 \Rightarrow (p/7) = -1 \Rightarrow p \equiv 3, 5$ or $6 \pmod 7$ (4)
Combining (3) & (4)
$p \equiv 3 \pmod 7$ & $p \equiv 3 \pmod 4$ $\Rightarrow p \equiv 3 \pmod{28}$
$p \equiv 5 \pmod 7$ & $p \equiv 3 \pmod 4$ $\Rightarrow p \equiv 19 \pmod{28}$
$p \equiv 6 \pmod 7$ & $p \equiv 3 \pmod 4$ $\Rightarrow p \equiv 27 \pmod{28}$

Therefore $p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$ with p an odd prime: $p \neq 7$.

Question 7

(i) (2 marks)

157 = 3 * 43 + 28
43 = 1 * 28 + 15
28 = 1 * 15 + 13
15 = 1 * 13 + 2
13 = 6 * 2 + 1
2 = 2 * 1 + 0

Therefore 157/43 = [3, 1, 1, 1, 6, 2]
= [3, 1, 1, 1, 6, 1, 1], using Second continued fraction identity.

(ii) (9 marks)

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 of y = [1, <2, 1, 2>] are

$$C_1 = \frac{1}{1};\ C_2 = \frac{2*1+1}{2} = \frac{3}{2};\ C_3 = \frac{1*3+1}{1*2+1} = \frac{4}{3};\ C_4 = \frac{2*4+3}{2*3+2} = \frac{11}{8};$$
$$C_5 = \frac{2*11+4}{2*8+3} = \frac{26}{19};\ C_6 = \frac{1*26+11}{1*19+8} = \frac{37}{27};\ C_7 = \frac{2*37+26}{2*27+19} = \frac{100}{73}.$$

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

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

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

[[C_4 is about 1/197 away from the true value, and C_5 about 1/665.]]

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).

As the 2nd and 3rd sides are odd then we must have $2mn = 24$. As $mn = 12$ then the only possible values of opposite parity with $m > n$ are

$m = 12$ and $n = 1$, or $m = 4$ and $n = 3$.

Therefore the only possible primitive Pythagorean triples are (24, 143, 145) and (24, 7, 25).

(ii) (3 marks)

$245 = 5 * 49 = 5 * 7^2$.

Since no factor of the form $4k + 3$ occurs to an odd power then 245 can be expressed as the sum of 2 squares (Unit 8, Th. 4.3).

$245 = 5 * 7^2 = (2^2 + 1^2) * 7^2 = 14^2 + 7^2$.

$496 = 4 * 124 = 16 * 31 = 2^4 * 31$.

Since the factor 31 is of the form $4k + 3$ and it occurs to an odd power then 496 cannot be expressed as the sum of 2 squares (Th. 4.3).

(ii) (4 marks)

Assume there is a solution $x = x_1$, $y = y_1$, and $z = z_1$.

Therefore $4x_1^3 - 2y_1^3 = z_1^3$. As the two of the terms in the equation are divisible by 2 then the 3rd term must also be divisible by 2. Since $2 \mid z_1^3$ then $2 \mid z_1$. Therefore $z_1 = 2 z_2$ where z_2 is an integer.

Hence $2x_1^3 - y_1^3 = 4 z_2^3$. Similarly $2 \mid y_1$ and so $y_1 = 2 y_2$ where y_2 is an integer.

Hence $x_1^3 - 4y_2^3 = 2 z_2^3$. Similarly $2 \mid x_1$ and so $x_1 = 2 x_2$ where x_2 is an integer.

Hence $4x_2^3 - 2y_2^3 = z_2^3$. As we have found another solution with $x_2 < x_1$, $y_2 < y_1$, and $z_2 < z_1$ then the descent step is complete. Hence the method of infinite descent shows can be no solutions in the positive integers.

END OF NUMBER THEORY SOLUTIONS