

**Question 1****(i)**

$$\begin{aligned}
137 &= 1 * 115 + 22 \\
115 &= 5 * 22 + 5 \\
22 &= 4 * 5 + 2 \\
5 &= 2 * 2 + 1 \\
2 &= 2 * 1 + 0
\end{aligned}$$

Therefore  $\gcd(137, 115) = 1$ .

$$\begin{aligned}
1 &= 5 - 2 * 2 \\
&= 5 - 2 * (22 - 4 * 5) = 9 * 5 - 2 * 22 \\
&= 9 * (115 - 5 * 22) - 2 * 22 = 9 * 115 - 47 * 22 \\
&= 9 * 115 - 47 * (137 - 115) = 56 * 115 - 47 * 137.
\end{aligned}$$

Therefore the general solution of  $\gcd(137, 115) = 137x + 115y$  is  
 $x = -47 + 115t$  and  $y = 56 - 137t$ .

**(ii)**

Since  $10n + 9 = 1 * (10n + 1) + 8$  then  $\gcd(10n + 1, 10n + 9) = \gcd(10n + 1, 8)$ .

As  $10n + 1$  is odd and  $8$  is a power of  $2$  then  $\gcd(10n + 1, 10n + 9) = 1$ .

**(iii)**

Let  $P(n)$  be the proposition that the given formula is true for  $n$ .

As  $P(1)$  is  $1 = (1 * 2 * 3)/6 = 1$  then  $P(1)$  is true and we have the basis for induction.

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

$$\begin{aligned}
&1 + 3 + 6 + 10 + \dots + \frac{k(k+1)}{2} + \frac{(k+1)(k+2)}{2} \\
&= \frac{k(k+1)(k+2)}{6} + \frac{(k+1)(k+2)}{2} \quad (\text{using the induction hypothesis}) \\
&= \frac{(k+1)(k+2)}{6} (k+3).
\end{aligned}$$

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)**

Assume there are a finite number of primes  $p_1, p_2, \dots, p_n$  and let  $N = p_1 p_2 \dots p_n + 1$ . Since  $N$  is not divisible by any of the  $n$  primes then either  $N$  is prime or it is divisible by a prime not in the list. In either case the list is not complete. Therefore there are infinitely many primes.

**(ii)**

Each of the  $N$  consecutive numbers  $(N + 1)! + n$ , where  $2 \leq n \leq N + 1$ , is composite as it is divisible by  $n$ . Therefore the statement is true.

**(iii)**

If  $n$  is not prime then all three numbers are not prime so we can assume that  $n$  is prime.

Therefore, as  $n$  is prime and  $n \geq 4$  it can be written as either  $3m + 1$  or  $3m + 2$ , where  $m \geq 1$ .

If  $n = 3m + 1$  then  $4n - 1 = 12m + 3 = 3(4m + 1)$ . So  $4n - 1$  is composite as  $m \geq 1$ .

If  $n = 3m + 2$  then  $4(4n - 1) - 1 = 4(12m + 7) - 1 = 48m + 27 = 3(16m + 9)$ . So  $4(4n - 1) - 1$  is composite.

Therefore the statement is true.

**Question 3****(i)**

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

(a) As  $10n + 3 \equiv 3 \pmod{4}$  then the least positive residue modulo 4 of  $10n + 3$  is 3.

(b) As  $10n + 3 \equiv 13 \pmod{15}$  then the least positive residue modulo 15 of  $10n + 3$  is 13.

**(ii)**

Since  $a \equiv b \pmod{n}$  then by the definition of congruence  $a - b = tn$ , for some integer  $t$ .

So  $a^2 = (b + tn)^2 = b^2 + n(2bt + t^2n)$ .

Since  $a^2 - b^2 = n(2bt + t^2n)$  then by the definition of congruence  $a^2 \equiv b^2 \pmod{n}$ .

**(iii)**

$$5x \equiv 8 \pmod{11} \Leftrightarrow 45x \equiv x \equiv 72 \equiv 6 \pmod{11}$$

As 4, 7, and 11 are relatively prime in pairs then we can use the Chinese Remainder theorem.  
Therefore the equations

$$x \equiv 3 \pmod{4}, \quad x \equiv 3 \pmod{7}, \quad \text{and } x \equiv 6 \pmod{11}$$

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)**

As 19 is a prime then by FLT,  $4^{18} \equiv 7^{18} \equiv 1 \pmod{19}$ .

Therefore  $4^{40} + 7^{40} = (4^{18})^2 4^4 + (7^{18})^2 7^4 \equiv (-3)^2 + (-8)^2 \equiv 9 + 7 \equiv 16 \pmod{19}$ .

**(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 1<sup>st</sup> few digits of  $3/19$ .

$$3 = 0 * 19 + 3$$

$$30 = 1 * 19 + 11$$

$$110 = 5 * 19 + 15$$

Since the recurring decimal of  $3/19$  is the same as that of  $1/19$  except that it starts at a different point then  $3/19 = 0.\langle 157894736842105263 \rangle$ .

[[As it says write down, to get the starting point, you could multiply 0526.. by 3 to get 15... ]]

**Question 5****(i)(a)**

$$68 = 2^2 * 17.$$

As  $\sigma$  is multiplicative then

$$\sigma(68) = \sigma(2^2)\sigma(17) = \frac{2^3 - 1}{2 - 1} * 18 = 7 * 18 = 126 < 2 * 68.$$

Therefore 68 is not abundant.

**(i)(b)**

$$168 = 4 * 42 = 2^3 * 3 * 7.$$

As  $\sigma$  is multiplicative then

$$\sigma(168) = \sigma(2^3)\sigma(3)\sigma(7) = \frac{2^4 - 1}{2 - 1} * 4 * 8 = 15 * 32 = 480 > 2 * 168.$$

Therefore 168 is abundant.

**(i)(c)**

If  $p = 2$  then  $\sigma(4p^2) = \sigma(2^4) = 2^5 - 1 = 31 < 2 * 16$ . Therefore  $\sigma(4p^2)$  is not abundant when  $p = 2$ .

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

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

As  $p \leq 7$ , a prime, and  $p \neq 2$  then  $4p^2$  is abundant when  $p = 3, 5, \text{ or } 7$ .

**(ii)**

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

Since  $2p - 1$  is an odd prime and  $\phi$  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)**

The discriminant of the equation is  $(-7)^2 - 4 * 1 * 9 = 49 - 36 = 13$ .

As 29 is an odd prime and  $\gcd(13, 29) = 1$  then the quadratic congruence has solutions if 13 is a quadratic residue of 29.

$$\begin{aligned} (13/29) &= (-16/29) && \text{Th. 2.1(a). } -16 \equiv 13 \pmod{29} \\ &= (-1/29) (4^2/29) && \text{Th. 2.1(c)} \\ &= 1 * 1 = 1 && \text{Th. 2.1(b), Th. 2.1(e) as } 29 \equiv 1 \pmod{4}. \end{aligned}$$

Therefore the congruence does have solutions.  $[[x \equiv 13 \text{ or } 23 \pmod{29}]]$

**(ii)**

$$\begin{aligned} (127/167) &= (-1) (167/127) && \text{LQR. } 167 \equiv 127 \equiv 3 \pmod{4} \\ &= - (40/127) && \text{Th. 2.1(a). } 40 \equiv 167 \pmod{127} \\ &= - (2^2/127) (2/127) (5/127) && \text{Th. 2.1(c)} \\ &= - 1 * 1 * (5/127) && \text{Th. 2.1(b), Th. 3.2 as } 127 \equiv 7 \pmod{8} \\ &= - (127/5) && \text{LQR. } 5 \equiv 1 \pmod{4} \\ &= - (2/5) && \text{Th. 2.1(a). } 127 \equiv 2 \pmod{5} \\ &= - (-1) = 1 && \text{Th. 3.2. } [[36^2 \equiv 127 \pmod{167}]] \end{aligned}$$

**(iii)** 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  $p \equiv 1, 2 \text{ or } 4 \pmod{7}$ ,  $p \neq 7$  (1)

If  $p \equiv 1 \pmod{4}$  LQR gives  $(7/p) = (p/7) = 1$ , (2)

Combining (1) & (2):

$$p \equiv 1 \pmod{7} \text{ \& } p \equiv 1 \pmod{4} \Rightarrow p \equiv 1 \pmod{28}$$

$$p \equiv 2 \pmod{7} \text{ \& } p \equiv 1 \pmod{4} \Rightarrow p \equiv 9 \pmod{28}$$

$$p \equiv 4 \pmod{7} \text{ \& } p \equiv 1 \pmod{4} \Rightarrow p \equiv 25 \pmod{28}$$

Also if  $p \equiv 3 \pmod{4}$  (3)

By LQR  $(7/p) = (-1) (p/7) = 1 \Rightarrow (p/7) = -1 \Rightarrow p \equiv 3, 5 \text{ or } 6 \pmod{7}$  (4)

Combining (3) & (4)

$$p \equiv 3 \pmod{7} \text{ \& } p \equiv 3 \pmod{4} \Rightarrow p \equiv 3 \pmod{28}$$

$$p \equiv 5 \pmod{7} \text{ \& } p \equiv 3 \pmod{4} \Rightarrow p \equiv 19 \pmod{28}$$

$$p \equiv 6 \pmod{7} \text{ \& } p \equiv 3 \pmod{4} \Rightarrow p \equiv 27 \pmod{28}$$

Therefore  $p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$  with  $p$  an odd prime:  $p \neq 7$ . [4 Marks]

**Question 7****(i)(a)**

$$C_1 = \frac{1}{1} = 1; C_2 = \frac{1*1+1}{1} = 2; C_3 = \frac{3*2+1}{3*1+1} = \frac{7}{4}; C_4 = \frac{3*7+2}{3*4+1} = \frac{23}{13};$$

$$C_5 = \frac{5*23+7}{5*13+4} = \frac{122}{69}; C_6 = \frac{5*122+23}{5*69+13} = \frac{633}{358}.$$

**(i)(a)**

By Corollary to Theorem 4.1  $|x - C_3| > \frac{1}{2*4*13} = \frac{1}{104}$ . Therefore  $C_3$  is not sufficiently accurate.

By Corollary to Theorem 4.1  $|x - C_4| < \frac{1}{13*69} < \frac{1}{500}$ .

Hence  $C_4$  is the 1<sup>st</sup> convergent accurate to  $x$  within  $1/500$ .

**(ii)**

Let  $x = [\langle 2, 2, 1 \rangle] = [2, 2, 1, x]$ .

The convergents of  $[2, 2, 1, x]$  are

$$C_1 = \frac{2}{1}; C_2 = \frac{2*2+1}{2} = \frac{5}{2}; C_3 = \frac{1*5+2}{1*2+1} = \frac{7}{3}; C_4 = \frac{x*7+5}{x*3+2} = \frac{7x+5}{3x+2} = x.$$

.

So  $3x^2 - 5x - 5 = 0$  and this has the positive solution  $x = \frac{5 + \sqrt{25 + 60}}{6} = \frac{5 + \sqrt{85}}{6}$ .

This gives  $[3, \langle 2, 2, 1 \rangle] = 3 + \frac{6}{5 + \sqrt{85}} = 3 + \frac{6(5 - \sqrt{85})}{25 - 85} = 3 + \frac{\sqrt{85} - 5}{10} = \frac{5}{2} + \frac{\sqrt{85}}{10}$ .

**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).

As the 2nd and 3rd elements are odd then we must have  $2mn = 44$ .

As  $mn = 22 = 2 * 11$  then  $m = 22, n = 1$ , and  $m = 11, n = 2$  are the only possibilities.

Therefore there are only 2 primitive Pythagorean triples where the even number is 44 and these are  $(44, 483, 485)$  and  $(44, 117, 125)$ .

**(ii)**

$240 = 3 * 8 * 10 = 2^4 * 3 * 5$ . Since a factor of the form  $4k + 3$  occurs to an odd power then 360 cannot be expressed as the sum of 2 squares (Th. 4.3).

$260 = 2 * 13 * 10 = 2^2 * 5 * 13$ . Since no factor of the form  $4k + 3$  occurs to an odd power then 260 can be expressed as the sum of 2 squares (Th. 4.3).

$280 = 4 * 7 * 10 = 2^3 * 5 * 7$ . Since a factor of the form  $4k + 3$  occurs to an odd power then 280 cannot be expressed as the sum of 2 squares (Th. 4.3).

$$260 = 26 * 10 = (5^2 + 1^2) * (3^2 + 1^2) = (5 * 3 + 1 * 1)^2 + (5 * 1 - 1 * 3)^2 = 16^2 + 2^2.$$

**(iii)**

Assume that  $x = x_1, y = y_1$  is a solution in positive integers.

Therefore  $x_1^3 = 3y_1^3$ .

Since  $3 \mid 3y_1^3$  then  $3 \mid x_1^3$  and so  $x_1$  is also divisible by 3. Therefore we can write  $x_1 = 3x_2$  where  $x_2$  is a positive integer.

Therefore  $27x_2^3 = 3y_1^3$ . Dividing by 3 gives  $9x_2^3 = y_1^3$ .

Since  $3 \mid 9x_2^3$  then  $3 \mid y_1^3$  and so  $y_1$  is also divisible by 3. Therefore we can write  $y_1 = 3y_2$  where  $y_2$  is a positive integer.

Therefore  $9x_2^3 = 27y_2^3$ . Dividing by 9 gives  $x_2^3 = 3y_2^3$ .

Therefore  $x = x_2, y = y_2$  is also a solution of  $x^3 = 3y^3$  with  $x_2 < x_1$  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**