

2002 - Number Theory Solutions

[[Comments are written like this.]]

Question 1

(i) (4 marks)

Let $P(n)$ be the proposition $1 + 5 + 12 + 22 + \dots + \frac{1}{2}n(3n-1) = \frac{1}{2}n^2(n+1)$.

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

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

$$\begin{aligned} & 1 + 5 + 12 + 22 + \dots + \frac{1}{2}k(3k-1) + \frac{1}{2}(k+1)[3(k+1)-1] \\ &= \frac{1}{2}k^2(k+1) + \frac{1}{2}(k+1)(3k+2) \quad (\text{using the induction hypothesis}) \\ &= \frac{1}{2}(k+1)(k^2+3k+2) \\ &= \frac{1}{2}(k+1)^2(k+2). \end{aligned}$$

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.

(ii) (4 marks)

$$\begin{aligned} 211 &= 1 * 160 + 51 \\ 160 &= 3 * 51 + 7 \\ 51 &= 7 * 7 + 2 \\ 7 &= 3 * 2 + 1 \\ 2 &= 2 * 1 + 0 \end{aligned}$$

Therefore $\gcd(211, 160) = 1$.

$$\begin{aligned} 1 &= 7 - 3 * 2 = 7 - 3 * (51 - 7 * 7) = 22 * 7 - 3 * 51 \\ &= 22 * (160 - 3 * 51) - 3 * 51 = 22 * 160 - 69 * 51 \\ &= 22 * 160 - 69 * (211 - 160) = 211 * (-69) - 160 * (-91) \end{aligned}$$

Therefore solutions of $211x - 160y = 1$ are of the form

$$x = -69 + \frac{160}{\gcd(211,160)}t = -69 + 160t, \text{ and } y = -91 + \frac{211}{\gcd(211,160)}t = -91 + 211t,$$

where t is an integer.

Hence $x = -69 + 160 = 91$, and $y = -91 + 211 = 120$ are an appropriate pair of positive integers.

*[[Check. $211 * 91 = 211 * (100 - 9) = 21,100 - 1899 = 19,201$. $160 * 120 = 19200$.]]*

(iii) (3 marks)

Since n has remainder 3 when divided by 12 then n is odd.
As $m = 3n + 4$ then

$$\begin{aligned} \gcd(m, n) &= \gcd(n, 4) && \text{Euclidean Algorithm} \\ &= 1 && \text{as } n \text{ is odd.} \end{aligned}$$

Question 2

(i)

4 is of the form $3k + 1$ but $4 = 2 * 2$, and 2 is not of this form.

The statement is **false**.

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

By the Division Algorithm every number has one of the forms $3k$, $3k + 1$, or $3k - 1$.

The only prime of the form $3k$ is 3. 3 does not divide a positive integer of the form $3k + 1$.

If p_1 and p_2 are primes of the form $3k + 1$ then as

$$p_1 p_2 \equiv 1 * 1 \equiv 1 \pmod{3}$$

then the product of two numbers of this type also has the same form.

Therefore a number of the form $3k - 1$ 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 $\gcd(3m + 1, 3n + 1) = \gcd(4, 4) = 4$.

Therefore the statement is **false**.

(iv) *[[Since $\gcd(3, -1) = 1$ 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 $3k - 1$ and these are p_1, p_2, \dots, p_n .

Let $N = 3(p_1 p_2 \dots p_n) - 1$. Since this is of the form $3k - 1$ then it must have a prime factor of the form $3k - 1$ (part ii). Assume this prime is p_i ($1 \leq i \leq n$).

Since p_i divides N and $3(p_1 p_2 \dots p_n)$ then it divides $N - 3(p_1 p_2 \dots p_n) = 1$.

Since p_i does not divide 1 then the assumption that there are a finite number of primes of the form $3k - 1$ must be false. Therefore there are an infinite number of primes of this form.

Question 3

(i) (2 marks)

Since $n \equiv 2 \pmod{6}$ then $n = 6k + 2$ for some integer k .
Therefore $12n + 7 = 12(6k + 2) + 7 = 72k + 31$.

(i)(a) $12n + 7 = 72k + 31 \equiv 31 \equiv 7 \pmod{8}$

(i)(b) $12n + 7 = 72k + 31 \equiv 31 \equiv 4 \pmod{9}$

(ii) (3 marks)

$$19x \equiv 9 \pmod{61} \Leftrightarrow 57x \equiv -4x \equiv 27 \pmod{61}$$
$$\Leftrightarrow -60x \equiv x \equiv 405 \equiv 39 \pmod{61}.$$

Therefore $x \equiv 39 \pmod{61}$.

*[[Check. $19 * 39 = (20 - 1) * (40 - 1) = 800 - 20 - 40 + 1 = 741 = 610 + 131 = 610 + 122 + 9.]]$*

*[[A solution using the Euclidean Algorithm. $61 = 3 * 19 + 4$, $19 = 4 * 4 + 3$, $4 = 1 * 3 + 1$.
 $1 = 4 - 3 = 4 - (19 - 4 * 4) = 5 * 4 - 19 = 5 * (61 - 3 * 19) - 19 = 5 * 61 - 16 * 19$.
Therefore $19^{-1} \equiv -16 \pmod{61}$ so $x \equiv (-16) * 9 \equiv -144 \equiv 39 \pmod{61}$.]]*

(iii) (6 marks)

By the Chinese remainder theorem the congruences

$$x \equiv 1 \pmod{3} \quad x \equiv 2 \pmod{5} \quad x \equiv 3 \pmod{13}$$

have a unique solution modulo $3 * 5 * 13 = 195$.

Integers which satisfy the congruence $x \equiv 3 \pmod{13}$ are 3, 16, 29, 42, ...

Integers which also satisfy the congruence $x \equiv 2 \pmod{5}$ are 42, 107, 172 ...

172 also satisfies the congruence $x \equiv 1 \pmod{3}$.

Hence 172 is the unique solution modulo 195.

Therefore the least positive integer which satisfies the congruences is 172.

Question 4

(i) (5 marks)

When $p = 2$ then $(2 - 1)! \equiv 1 \equiv -1 \pmod{2}$

Let $p \geq 3$ be a prime.

If a is one of the least positive residues then the equation $ax \equiv 1 \pmod{p}$ has a unique solution. [[Unit 3, Th. 3.2(b)]]

If $ab \equiv 1 \pmod{p}$ then if $a \equiv b \pmod{p}$ then $a^2 - 1 \equiv 0 \pmod{p}$.

By Lagrange's theorem there are a maximum of 2 solutions 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

$$\begin{aligned} & 1 * [2 * 3 * \dots * (p - 2)] * (p - 1) \\ & \equiv 1 * 1^{(p-3)/2} * (p - 1) \\ & \equiv (p - 1) \equiv -1 \pmod{p}. \end{aligned}$$

Therefore $(p - 1)! \equiv -1 \pmod{p}$ if p is a prime.

[[You might prefer the proof in the unit.]]

(ii) (6 marks)

(ii)(a) By FLT $40^6 \equiv 1 \pmod{7}$.

Therefore $40^{65} \equiv 40^{66} * 40^{-1} \equiv (40^6)^{11} * 5^{-1} \equiv 1^{11} * 3 \equiv 3 \pmod{7}$.

(ii)(b) [[Solution by Linda Brown.]]

[[The original incorrect solution used the FLT. This is NOT valid as a is not always relatively prime to 3, 5, and 13]]

$195 = 3 * 5 * 13$.

Alternative form of FLT gives $a^3 \equiv a \pmod{3}$, $a^5 \equiv a \pmod{5}$ and $a^{13} \equiv a \pmod{13}$.

Hence $a^{25} \equiv (a^3)^8 * a \equiv a^8 * a \equiv (a^3)^3 \equiv a^3 \equiv a \pmod{3}$,

$$a^{25} \equiv (a^5)^5 \equiv a^5 \equiv a \pmod{5},$$

and $a^{25} \equiv a^{13} * a^{12} \equiv a * a^{12} \equiv a^{13} \equiv a \pmod{13}$.

Hence by the Corollary to Theorem 1.3, with 3, 5 & 13 prime,

$$a^{25} \equiv a \pmod{195}, \text{ for all integers } a.$$

Question 5

(i) (4 marks)

As $2^p - 1$ is odd then $\gcd(2^{p-1}, 2^p - 1) = 1$.

$$\begin{aligned}\sigma(m) &= \sigma(2^{p-1}(2^p - 1)) \\ &= \sigma(2^{p-1})\sigma(2^p - 1) \\ &= (2^p - 1)2^p \\ &= 2m\end{aligned}$$

As σ is a multiplicative function and $\gcd(2^{p-1}, 2^p - 1) = 1$.
 $\sigma(2^p - 1) = 2^p$ as $2^p - 1$ is prime, $\sigma(2^{p-1}) = (2^p - 1)$ as $p > 1$.

As $\sigma(m) = 2m$ then m is perfect if $2^p - 1$ is prime.

(ii) (7 marks)

(ii)(a) If n is prime then $\sigma(n) = n + 1$.

Therefore $\sigma(n) - n = (n + 1) - n = 1$.

As 1 is not divisible by 3 then n cannot be a prime.

(ii)(b) If $n = p^2$ where p is a prime then $\sigma(n) = 1 + p + p^2$.

$$\begin{aligned}3 \mid \sigma(n) - n &\Rightarrow 3 \mid (1 + p + p^2) - p^2 \\ &\Rightarrow 3 \mid p + 1 \\ &\Rightarrow p \equiv 2 \pmod{3}\end{aligned}$$

(iii)(c)

$$\begin{aligned}\sigma(n) &= \sigma(pq) = \sigma(p)\sigma(q) && \text{since } p \text{ and } q \text{ are distinct primes} \\ &= (1 + p)(1 + q) && \text{as } p \text{ and } q \text{ are prime.} \\ &= 1 + p + q + pq.\end{aligned}$$

$$\begin{aligned}3 \mid \sigma(n) - n &\Rightarrow 3 \mid 1 + p + q \\ &\Rightarrow p + q \equiv 2 \pmod{3}\end{aligned}$$

Therefore $\sigma(n) - n$ is divisible by 3 only if

$p = 3$ and $q \equiv 2 \pmod{3}$, or
 $p \equiv 1 \pmod{3}$ and $q \equiv 1 \pmod{3}$ where $p \neq q$, p and q both prime, or
 $p \equiv 2 \pmod{3}$ and $q = 3$.

*[[Check. $\sigma(6) - 6 = 1 + 2 + 3 = 6$. $\sigma(7 * 13) - 7 * 13 = 1 + 7 + 13 = 21$.]]*

2002 Question 6

(i) (4 marks)

The quadratic congruence has solutions if $5^2 - 4 * 2 * 6 = 25 - 48 = -23$ is a quadratic residue of 17.

$$\begin{aligned}(-23/17) &= (-6/17) && \text{Th. 2.1(a), } -23 \equiv -6 \pmod{17} \\ &= (-1/17)(2/17)(3/17) && \text{Th. 2.1(c).} \\ &= 1 * 1 * (-1) = -1 && \text{Th. 2.1(e), Th. 3.2, and Th. 4.4.}\end{aligned}$$

Therefore the congruence does not have solutions.

(ii) (3 marks)

$$\begin{aligned}(-37/59) &= (22/59) && \text{Th. 2.1(a), } -37 \equiv 22 \pmod{59} \\ &= (2/59)(11/59) && \text{Th. 2.1(c).} \\ &= (-1) \{ -(59/11) \} && \text{Th. 3.2. LQR. } 59 \equiv 11 \equiv 3 \pmod{4}. \\ &= (4/11) && 59 \equiv 4 \pmod{11} \\ &= 1 && \text{Th. 2.1(b).}\end{aligned}$$

[[Alternatively not using the LQR.

$$(-37/59) = (-96/59) = (-1/59)(16/59)(3/59)(2/59) = (-1) * 1 * 1 * (-1) = 1.]]$$

(iii) (4 marks)

When $a = 2$ and $p = 8k + 5$ the set S in Gauss' Lemma is $S = \{2, 4, 6, \dots, 8k + 4\}$

If $2\alpha > p/2$ then $\alpha > p/4 = 2k + 5/4$.

As α is an integer then $\alpha \geq 2k + 2$.

The number of values in the set S where the value exceeds $p/2$ is

$$\{(p - 1)/2 - (2k + 2)\} + 1 = (4k + 2) - (2k + 2) + 1 = 2k + 1.$$

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

[[You might find it easier to find number of values $\leq p/2$ and deduce the number $> p/2$.

If $2\alpha \leq p/2$ then $\alpha \leq p/4 = 2k + 5/4$. As α is an integer then $\alpha \leq 2k + 1$.

The number of values in the set S where the value exceeds $p/2$ is

$$\{(p - 1)/2 - (2k + 1)\} = (4k + 2) - (2k + 1) = 2k + 1.]]$$

Question 7

(i) (5 marks)

$$172 = 2 * 79 + 14$$

$$79 = 5 * 14 + 9$$

$$14 = 1 * 9 + 5$$

$$9 = 1 * 5 + 4$$

$$5 = 1 * 4 + 1$$

$$4 = 4 * 1 + 0$$

Therefore $172/79 = [2, 5, 1, 1, 1, 4]$.

The convergents are $C_1 = 2/1$; $C_2 = 11/5$; $C_3 = 13/6$; $C_4 = 24/11$; $C_5 = 37/17$; $C_6 = 172/79$.

By Theorem 1.3(a) we have $172 * 17 - 37 * 79 = (-1)^6 = 1$.

So one solution of the linear Diophantine equation $172x - 79y = 1$ is
 $x = 17, y = 37$.

*[[Check. $172 * 17 - 79 * 37 = 172 * (20 - 3) - (80 - 1) * 37 = 3440 - 516 - 2960 + 37 = 3477 - 3476.]]$*

(ii) (6 marks)

Let $y = [2, 3, x]$ where $x = [<3, 2>] = [3, 2, x]$.

The convergents of $[3, 2, x]$ are $3/1, 7/2, (7x + 3)/(2x + 1) = x$.

So $2x^2 - 6x - 3 = 0$ and the positive solution is $x = \frac{6 + \sqrt{36 + 24}}{4} = \frac{3 + \sqrt{15}}{2}$.

The convergents of $[2, 3, x]$ are $2/1, 7/3, (7x + 2)/(3x + 1) = (14x + 4)/(6x + 2) = y$.

$$\begin{aligned} [2, 3, <3, 2>] &= y \\ &= \frac{25 + 7\sqrt{15}}{11 + 3\sqrt{15}} = \frac{(25 + 7\sqrt{15})(11 - 3\sqrt{15})}{121 - 135} = \frac{(275 - 315) + \sqrt{15}(-75 + 77)}{-14} = \frac{20 - \sqrt{15}}{7}. \end{aligned}$$

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 its 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)

[[Correction by Peter Monk. 08/10/05]]

$$\sqrt{8} = \sqrt{8} \frac{\sqrt{8} - 2}{\sqrt{8} - 2} = \frac{8 - 2(\frac{m}{n})}{(\frac{m}{n}) - 2} = \frac{8n - 2m}{m - 2n}. \quad \text{[[Probably easier to work right to left.]]$$

Let $\sqrt{8} = m_1/n_1$.

Let $m_2 = 8n_1 - 2m_1$, and $n_2 = m_1 - 2n_1$ then $\sqrt{8} = m_2/n_2$.

Since $2 < \sqrt{8} = m_1/n_1 < 3$ then $2n_1 < m_1 < 3n_1$. Therefore $0 < m_1 - 2n_1 = n_2 < n_1$.

As the denominator is smaller then 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