2002 Question 1

(i) Let $P(n)$ be the statement "$1+\dots+\frac{1}{2}n(3n-1)=\frac{1}{2}n^2(n+1)$"

For $n=1$, LHS $=1=$ RHS, so $P(1)$ is true.

Suppose $P(k)$ is true. For $n=k+1$

$$\begin{aligned} LHS &= 1+\dots+\tfrac{1}{2}k(3k-1)+\tfrac{1}{2}(k+1)(3(k+1)-1) \\ &= \tfrac{1}{2}k^2(k+1)+\tfrac{1}{2}(k+1)(3k+2) \\ &= \tfrac{1}{2}(k+1)^2(k+2) = RHS \end{aligned}$$

Thus $P(k) \Rightarrow P(k+1)$. By Induction $P(n)$ true for $n \geq 1$.

(ii)

$$\begin{aligned} 211 &= 1.160+51 \\ 160 &= 3.51+7 \\ 51 &= 7.7+2 \\ 7 &= 3.2+1 \end{aligned}$$

So $\gcd(211, 161)=1$

$$\begin{aligned} 1 &= 7-3.2 = 7-3(51-7.7) \\ &= 22.7-3.51 = 22(160-3.51)-3.51 \\ &= 22.160-69.51 \\ &= 22(160)-69(211-160) \\ &= 91.160-69.211 \end{aligned}$$

A solution is $x=-69$, $y=-91$

General solution $x=-69+160k$, $y=-91+211k$ $(k \in \mathbb{Z})$

A positive solution $\underline{x=91,\ y=120.}$

(iii) $n = 12k+3$, so $m=36k+13$.

If $d \mid m$ and $d \mid n$, then $d \mid (m-3n)$, ie $d \mid 4$.

But $d \mid n$, so $d \mid ((12k+3)-3k.4)$ ie $d \mid 3$

$d \mid 3$, $d \mid 4$ so $d = \pm 1$

i.e. only positive common divisor is 1, so $\gcd(m,n)=1$.

Question 2

(i) False. 4 has no prime divisor of form $3k+1$.

(ii) True. Let $N = 3k-1$, so $N \equiv -1 \pmod 3$

Clearly $3 \nmid N$, so each prime divisor p has $p \equiv 1$ or $p \equiv -1 \pmod 3$

If all have $p \equiv 1 \pmod 3$, then $N \equiv 1 \pmod 3$

Since $N \equiv -1 \pmod 3$, N has divisor $3k-1$.

(iii) False. $\gcd(1,3) = 1$, but $\gcd(4,10) = 2$.

(iv) [Bookwork]

(*) Suppose that the result is false.

Let complete list of "$3k-1$" primes be $p_1, \dots, p_n$

Let $N = 3p_1 \cdots p_n - 1$.

By (ii) N has a prime divisor p of form $3k-1$.

But then, as list complete $p = p_i$, some i

Now $p_i \nmid N$ ($N \equiv -1 \pmod{p_i}$).

We have a contradiction to *

Hence result is true.

Question 3

(i) $n = 6k+2$, $12n+7 = 72k+31$.

a) $72n+31 = 8(9k+3)+7$, so $12n+7 \equiv \underline{7 \pmod 8}$

b) $72n+31 = 9(8k+3)+4$, so $12n+7 \equiv \underline{4} \pmod 9$

(ii) $19x \equiv 9 \pmod{61}$

$3.19 \equiv -4 \pmod{61}$

$-4x \equiv 27 \pmod{61}$

$-4x \equiv 88 \pmod{61}$

$\underline{x \equiv -22 \equiv 39} \pmod{61}$

(iii) $x \equiv 3 \pmod{13}$ has solutions $3, 16, 29, 42$

mod 5 $\quad 3 \quad 1 \quad 4 \quad 2$.

So solution of $\left.\begin{array}{l} x \equiv 3 \pmod{13} \\ x \equiv 2 \pmod 5 \end{array}\right\}$ is $x \equiv 42 \pmod{65}$.

Solutions	42	107	172
Modulo 3	0	2	1

Solution $x \equiv 172 \pmod{195}$

Least positive solution is $\underline{172}$.

Question 4

(i) (Bookwork.)

Result is true for $p = 2$.

Suppose p is an odd prime.

For $a \in \{1, .., p-1\}$ $\exists a'$ in $\{1, .., p-1\}$ with $aa' \equiv 1 \pmod p$

$a \equiv a' \Leftrightarrow a^2 \equiv 1 \Leftrightarrow a \equiv \pm 1 \pmod p$ ie $a = 1, p-1$

Thus $(p-1)! = 1 \times 2 \times .. \times p-1 \equiv 1.(\underbrace{...}_{\text{pairs } a, a'})p-1 \pmod{p-1}$

ie $(p-1)! \equiv -1 \pmod p$

(ii) FLT If $p \nmid a$, $a^{p-1} \equiv 1 \pmod p$.

(a) $40^{6} \equiv 1 \pmod 7$, so

$40^{65} \equiv (40^6)^{10} . 40^5 \equiv 40^5 \equiv 5^5 \pmod 7$

$\equiv 25.125 \equiv 4.6 \equiv 24 \equiv 3 \pmod 7$.

ie remainder is 3.

(b) $195 = 3.5.13$.

If $3 \nmid a$, then $a^2 \equiv 1 \pmod 3$, so $a^{24} \equiv 1^8 \equiv 1 \pmod 3$

Then $a^{25} - a \equiv (a^{24} - 1)a \equiv 0 \pmod 3$

If $3 \mid a$, then $(a^{24} - 1)a \equiv 0 \pmod 3$

ie for all a, $(a^{24} - 1)a \equiv 0 \pmod 3$

Similarly $(a^{24} - 1)a \equiv 0 \pmod 5$

$(a^{24} - 1)a \equiv 0 \pmod{13}$

Hence $a^{25} - a \equiv 0 \pmod{195}$

ie $a^{25} \equiv a \pmod{195}$

Question 5

(i) $\sigma(m) = \sigma(2^{p-1})\,\sigma(2^p - 1)$ $\qquad$ $\sigma(2^{p-1}) = 2^p - 1$

$= (2^p - 1).\,2^p$ $\qquad$ $\sigma(2^p - 1) = 2^p$ if $2^p - 1$ prime

$= 2m$ _ so m perfect.

(ii) (a) If n prime, $\sigma(n) = n + 1$,

$\sigma(n) - n = 1 \not\equiv 0 \pmod 3$

ie when n prime, $\sigma(n) - n$ not divisible by 3.

(b) If $n = p^2$, p prime, $\sigma(n) = p^2 + p + 1$. Then

$\sigma(n) - n) = p + 1 \equiv 0 \pmod 3 \iff p \equiv 2 \pmod 3$.

(c) If $n = pq$; p, q distinct primes, $\sigma(n) = pq + p + q + 1$.

$\sigma(n) - n = p + q + 1 \equiv 0 \pmod 3$

$\iff p + q \equiv 2 \pmod 3$

The condition satisfied if $p = 3$ $q \equiv 2 \pmod 3$

or $p \equiv 2 \pmod 3$, $q = 3$

or $p \equiv q \equiv 1 \pmod 3$.

Question 6

(i) Disenminant = "b^2-4ac" = -23. Solutions $\Leftrightarrow \left(\frac{-23}{17}\right)=1$

$$\left(\frac{-23}{17}\right) = \left(\frac{11}{17}\right) \qquad -23 \equiv 11 \pmod{17}$$

$$= +\left(\frac{17}{11}\right) \qquad 17 \equiv 1 \pmod 4$$

$$= \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$$

$$= (-1)\left(-\frac{11}{3}\right) = \qquad 11 \equiv 3 \pmod 8,\ 11 \equiv 3 \equiv 3 \pmod 4$$

$$= \left(\frac{2}{3}\right) = -1 \qquad 3 \equiv 3 \pmod 8$$

ie <u>no</u> solutions.

(ii) $$\left(\frac{-37}{59}\right) = \left(\frac{22}{59}\right) = \left(\frac{2}{59}\right)\left(\frac{11}{59}\right) \qquad -37 \equiv 22 \pmod{59}$$

$$= (-1)\left(-\left(\frac{59}{11}\right)\right) \qquad 59 \equiv 11 \equiv 3 \pmod 4$$

$$= \left(\frac{59}{11}\right) = \left(\frac{4}{11}\right) = 1$$

ie $\underline{(-37/59) = 1}$

(iii) $\left(\frac{2}{p}\right) = (-1)^K$, where K is the number of integers

$$\{2.1, 2.2, \dots, 2.\,4k+2\}$$

Congruent to $Q > \frac{p}{2}$ modulo p.

Numbers are already reduced modulo p

$2j > \frac{8k+5}{2} \Leftrightarrow j > 2k+1$

Hence $K = 2k+1$, so $\left(\frac{2}{p}\right) = -1$, as required.

Question 7

(i) $172 = 2.79 + 14$

$79 = 5.14 + 9$

$14 = 1.9 + 5$

$9 = 1.5 + 4$

$5 = 1.4 + 1$

$4 = 4.1 + 0$

p_k	1	2	11	13	24	37	172
a_k		2	5	1	1	1	4
q_k	0	1	5	6	11	17	79

so $17.172 - 37.79 = 1$

A solution is $\underline{x = 17,\ y = 37}$.

(ii) Let $x = [\langle 3,2\rangle]$, so $x = [\langle 3,2\rangle, x]$

ie $x = 3 + \dfrac{1}{2+\frac{1}{x}} = 3 + \dfrac{x}{2x+1} = \dfrac{7x+3}{2x+1}$.

Then $2x^2 - 6x - 3 = 0$

Solution $x = \dfrac{6+\sqrt{60}}{4} = \dfrac{3+\sqrt{15}}{2}$ (*) (other root <0)

Then $[2,3,\langle 3,2\rangle] = 2 + \dfrac{1}{3+\frac{1}{x}}$.

$= 2 + \dfrac{x}{3x+1} = \dfrac{7x+2}{3x+1}$

Given number is $\underline{\dfrac{25+7\sqrt{15}}{11+3\sqrt{15}}}$ (*)

(Can be tidied up to $\dfrac{20-\sqrt{15}}{7}$)

Question 8

(i) "Even member $= 2mn$, $m > n$, m, n of opposite parity"

$20 = 2mn \iff 10 = mn$, ie $m = 10, n = 1$ or $m = 5, n = 2$

Solutions "$(2mn, m^2 - n^2, m^2 + n^2)$"

ie. $(20, 99, 101)$
$(20, 21, 29)$

$22 = 2mn \iff 11 = mn$, but m, n can't have opposite parity

ie no solutions.

(ii) $360 = 2^3 . 3^2 . 5$ no "$4k+3$" factor: solutions

$364 = 2^2 . 7 . 13$ has prime factor $7 \equiv 3 \pmod 4$
for which $7^2 \nmid 364$
ie no solutions.

$\underline{360} = 36.10 = 6^2 (3^2 + 1^2) = \underline{(18)^2 + 6^2}$.

(iii) Suppose $\sqrt{8} = m/n$. so $m = \sqrt{8}\,n$

Then $\dfrac{8n - 2m}{m - 2n} = \dfrac{(8 - 2\sqrt{8})n}{(\sqrt{8} - 2)n} = \sqrt{8} \cdot \dfrac{\sqrt{8} - 2}{\sqrt{8} - 2} = \sqrt{8}$

Now $2 < \sqrt{8} < 3$

So $2n < m < 3n$, ie $0 < m - 2n < n$

Thus, if $\sqrt{8} = \dfrac{m}{n}$, $\sqrt{8} = \dfrac{8n - 2m}{m - 2n}$

with integers $8n - 2m$, $m - 2n$ & $m - 2n < n$

ie we have $\sqrt{8} = \dfrac{m'}{n'}$ with $0 < n' < n$

By infinite descent, we cannot have a sequence of decreasing positive integers

$\sqrt{8} = m/n$ is impossible.