NUMBER THEORY 1996

Question 1

(i) The statement is true for $n=1$, as $\frac{1}{6}.1.2.3=1$.
Suppose that the statement is true for $n=k$.
Then

$$1+6+\cdots+k(2k-1)=\frac{1}{6}k(k+1)(4k-1)$$

so that

$$\begin{aligned}1+6+\cdots+k(2k-1)+(k+1)(2k+1)&=\frac{1}{6}k(k+1)(4k-1)+(k+1)(2k+1)\\&=\frac{1}{6}(k+1)(4k^2-k+12k+6)\\&=\frac{1}{6}(k+1)(4k^2+11k+6)\\&=\frac{1}{6}(k+1)(k+2)(4k+3).\end{aligned}$$

Thus if the statement is true for $n=k$ then it is true for $n=k+1$. It follows from the Principle of Induction that the statement is true for all positive integers n.

(ii) $$\begin{aligned}238&=2.140-42\\140&=3.42+14\\42&=3.14\end{aligned}$$

Thus $\gcd(238,140)=14$.

(iii) As $\gcd(51,36)=3$, the linear Diophantine equation has a solution if and only if c is a multiple of 3. Thus we must solve the equation $51x-36y=3$, that is $17x-12y=1$.
Applying the Euclidean algorithm gives

$$\begin{aligned}17&=12+5\\12&=2.5+2\\5&=2.2+1.\end{aligned}$$

Thus

$$\begin{aligned}1&=5-2.2=5-2.(12-2.5)=5.5-2.12\\&=5.(17-12)-2.12=5.17-7.12.\end{aligned}$$

A particular solution is $x=5$, $y=7$ and the general solution is

$$x=5+12t,\quad y=7+17t,\quad t\in\mathbb{Z}.$$

Question 2.

(i) Suppose, to obtain a contradiction, that there are finitely many primes of the form $4k+3$, say $p_1, p_2, \ldots, p_n$. Consider the integer

$$N=4(p_1\cdots p_n)-1=4((p_1\cdots p_n)-1)+3.$$

Since N is odd, every prime divisor of N is of the form $4k+1$ or $4k+3$. If every prime divisor of N were of the form $4k+1$, then N would be of the form $4k+1$; but this is not the case, so N has a prime divisor q of the form $4k+3$. By hypothesis $q=p_j$ for some j. Then $q\mid N$ and $q\mid(p_1\cdots p_n)$ so that

$$q \mid 4(p_1 \cdots p_n) - N,$$

that is $q \mid 1$. This is a contradiction. Therefore there are infinitely many primes of the form $4k+3$.

(ii) Note that $a_8 = 68$, $a_9 = 85$ and $\gcd(68, 85) = 17$. Now let $d_n = \gcd(a_n, a_{n+1})$. Then $d_n \mid n^2+4$ and $d_n \mid (n+1)^2+4$ so that $d_n \mid 2n+1$. Therefore

$$d_n \mid 2(n^2+4) - n(2n+1),$$

that is $d_n \mid 8-n$. Next,

$$d_n \mid 2n+1 + 2(8-n),$$

that is $d_n \mid 17$. Thus for each n, $d_n = 1$ or $d_n = 17$.

Question 3

(i)(a) FALSE. Counterexample: $1 \equiv 3 \pmod 2$ but $1 \not\equiv 3 \pmod 4$.

(b) FALSE. Counterexample: $2.1 \equiv 2.2 \pmod 2$ but $1 \not\equiv 2 \pmod 2$.

(c) TRUE. If $da \equiv db \pmod m$ then $da - db = km$ for some integer k so that $a - b = k\left(\frac{m}{d}\right)$, that is $a \equiv b \pmod{\frac{m}{d}}$.

(d) TRUE. If $a \equiv db \pmod m$ then $a = db + rm$ for some integer r, so that $a = d\left(b + r\left(\frac{m}{d}\right)\right)$, that is $d \mid a$ so $a \equiv 0 \pmod d$.

(ii) $x \equiv 8 \pmod{11} \Rightarrow x = 8, 19, \ldots$

and

$x \equiv 4 \pmod 5 \Rightarrow \quad x = 19, 74, 129, \ldots$

and

$x \equiv 0 \pmod 3 \Rightarrow \quad x = 129, \ldots$

Thus the smallest integer which satisfies the three congruences simultaneously is 129.

Question 4

(i) Consider the set

$$\{a, 2a, \ldots, (p-1)a\}$$

of $p-1$ numbers. None of these is congruent to 0 modulo p, for if $ra \equiv 0 \pmod p$ where r is an integer, then, by Euclid's Lemma, $r \equiv 0 \pmod p$ since $a \not\equiv 0 \pmod p$ so that $r \notin \{1, 2, \ldots, p-1\}$. Moreover no two members of the set are congruent modulo p, for if $ra \equiv sa \pmod p$ where $1 \leq r, s \leq p-1$ then $r \equiv s \pmod p$ since $a \not\equiv 0 \pmod p$ so that $r = s$. It follows that the members of the set are congruent modulo p, in some order, to the numbers in the set $\{1, 2, \ldots, p-1\}$. Therefore

$$a.(2a).\ldots.((p-1)a) \equiv 1.2.\ldots.(p-1) \pmod p,$$

that is

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod p.$$

Since $(p-1)! \not\equiv 0 \pmod p$ it follows that

$$a^{p-1} \equiv 1 \pmod p.$$

(ii) (a) As the decimal representation of $\frac{1}{17}$ has cycle of length 16, it follows that the order of 10 modulo 17 is 16.

(b) $(10^8)^2 \equiv 1 \pmod{17}$ but $10^8 \not\equiv 1 \pmod{17}$ so the order of 10 modulo 17 is 16. Therefore $10^8 \equiv -1 \pmod{17}$.

(c) $130 = 7.17 + 11$
$110 = 6.17 + 8$

Thus the decimal representation of $\frac{13}{17}$ begins 0.76. But the cycle of $\frac{13}{17}$ is that of $\frac{1}{17}$ with a different starting point, so

$$\frac{13}{17} = \cdot\langle 7647058823529411 \rangle .$$

Question 5

(i) Let p be a prime. Then $\sigma(p) = p+1$ so that $2p + \sigma(p) = 3p+1$ which is not divisible by 3.

(ii) Suppose that $n = p^2$ where p is an odd prime and that $2n + \sigma(n)$ is divisible by 3. Then $3p^2 + p + 1 \equiv 0 \pmod 3$ so that $p \equiv 2 \pmod 3$. Therefore $p \equiv 2 \pmod 6$ or $p \equiv 5 \pmod 6$. But an odd prime cannot be congruent to 2 modulo 6 so that $p \equiv 5 \pmod 6$.

(iii) Suppose that $n = 2p^r$ where p is an odd prime and that $2n + \sigma(n)$ is divisible by 3. Since $\sigma(2p^r) = \sigma(2)\sigma(p^r) = 3\sigma(p^r)$ it follows that $3 | 2p^r$ and this is the case if and only if $p = 3$.

(iv) Suppose that $n = pq$ where p, q are distinct odd primes and that $2n + \sigma(n)$ is divisible by 3. Since $\sigma(pq) = \sigma(p)\sigma(q) = (p+1)(q+1) = pq + p + q + 1$, it follows that $p+q+1$ is divisible by 3. There are 3 cases: (i) $p = 3$, $q \equiv 2 \pmod 3$; (ii) $q = 3$, $p \equiv 2 \pmod 3$; (iii) $p \equiv q \equiv 1 \pmod 3$.

Question 6

(i) The discriminant is $7^2 - 4.5 = 29$. Now

$$\begin{aligned}
(29/43) &= (43/29) && \text{LQR} \\
&= (14/29) && 2.1(a) \\
&= (2/29)(7/29) && 2.1(c) \\
&= -(7/29) && 3.2 \\
&= -(29/7) && \text{LQR} \\
&= -(1/7) && 2.1(a) \\
&= -1 && 2.1(b)
\end{aligned}$$

Thus 29 is not a quadratic residue of 43 and the congruence has no solutions.

(ii)
$$\begin{aligned}
(86/103) &= (2/103)(43/103) && 2.1(c) \\
&= (43/103) && 3.2 \\
&= -(103/43) && \text{LQR} \\
&= -(17/43) && 2.1(a) \\
&= -(43/17) && \text{LQR} \\
&= -(9/17) && 2.1(a) \\
&= -1 && 2.1(b).
\end{aligned}$$

(iii) Suppose that $8k+5$ is prime. To apply the Gauss Lemma, we must count the number of members of the set

$$\{2, 4, \ldots, 8k+4\}$$

which exceed $\frac{8k+5}{2}$. The set contains $4k+2$ members, the first $2k+1$ do not exceed $4k+2$ whilst the remainder are greater than $4k+3$. Thus $2k+1$ members exceed $\frac{8k+5}{2}$. By the Gauss Lemma

$$(2/8k+5) = (-1)^{2k+1} = -1.$$

Thus 2 is a quadratic non-residue of each prime p such that $p \equiv 5 \pmod 8$.

Question 7

(i) $35 = \underline{2}.13 + 9$
$13 = \underline{1}.9 + 4$
$9 = \underline{2}.4 + 1$
$4 = \underline{4}.1$.

Therefore

$$\frac{35}{13} = [2,1,2,4] = [2,1,2,3,1].$$

(ii) The proof is by induction. Let $[a_1, a_2, \ldots]$ be the ICF. Then

$$p_1 = a_1, \quad p_2 = a_1 a_2 + 1, \quad q_1 = 1, \quad q_2 = a_2$$

so that

$$p_2 q_1 - p_1 q_2 = (a_1 a_2 + 1) - a_1 a_2 = 1 = (-1)^2.$$

Thus the formula holds for $k=2$. Suppose that the formula holds for $k=m$. Since

$$p_{m+1} = a_{m+1} p_m + p_{m-1}, \quad q_{m+1} = a_{m+1} q_m + q_{m-1}$$

we see that

$$\begin{aligned} &p_{m+1} q_m - p_m q_{m+1} \\ &= (a_{m+1} p_m + p_{m-1}) q_m - p_m (a_{m+1} q_m + q_{m-1}) \\ &= p_{m-1} q_m - p_m q_{m-1} = -(p_m q_{m-1} - p_{m-1} q_m) \\ &= (-1)(-1)^m = (-1)^{m+1}. \end{aligned}$$

Thus if the formula holds for $k=m$, it holds for $k=m+1$. By the Principle of Induction, the formula holds for all integers k such that $k \geq 2$.

(iii) Put $x = [\langle 2,3 \rangle]$ so that

$$x = [2,3,x] = 2 + \frac{1}{3+\frac{1}{x}} = 2 + \frac{x}{3x+1}$$
$$= \frac{7x+2}{3x+1}.$$

Therefore $(3x+1)x = 7x+2$ so that

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

Since $x > 0$,

$$x = \frac{6+\sqrt{60}}{6} = \frac{3+\sqrt{15}}{3}.$$

Hence

$$\alpha = [1, \langle 2,3 \rangle] = [1, x] = 1 + \frac{1}{x} = \frac{x+1}{x}$$
$$= \frac{6+\sqrt{15}}{3+\sqrt{15}} = \frac{3\sqrt{15}-3}{6} = \frac{1}{2}(\sqrt{15}-1).$$

The convergents of α are given by the table

1	2	3	4	5	6
1	3	10	23	79	181
1	2	3	2	3	2
1	2	7	16	55	126

Now

$$\left|\alpha - \frac{23}{16}\right| < \frac{1}{16.55} < \frac{1}{500}$$

and

$$\left|\alpha - \frac{10}{7}\right| > \frac{1}{2.7.16} > \frac{1}{500}.$$

Thus C_4 is the first convergent of α which is sufficiently accurate.

Question 8

(i) Using the continued fraction algorithm

$$x_1 = \sqrt{12} = 3 + \sqrt{12} - 3 \qquad a_1 = 3$$

$$x_2 = \frac{1}{\sqrt{12}-3} = \frac{\sqrt{12}+3}{3} = 2 + \frac{\sqrt{12}-3}{3} \qquad a_2 = 2$$

$$x_3 = \frac{3}{\sqrt{12}-3} = \sqrt{12}+3 = 6 + (\sqrt{12}-3) \qquad a_3 = 6$$

$$x_4 = \frac{1}{\sqrt{12}-3} = x_2.$$

Therefore $\sqrt{12} = [3, \langle 2, 6\rangle]$.

The first two solutions of the Pell's equation are determined by the 2nd and 4th convergents of $\sqrt{12}$. To obtain the convergents, we use the table.

1	2	3	4
3	7	45	97
3	2	6	2
1	2	13	28

So the first two solutions of $x^2 - 12y^2 = 1$ are $(x, y) = (7, 2)$ and $(x, y) = (97, 28)$.

(ii) As 560 is divisible by 7 with exponent 1 and 570 is divisible by 19 with exponent 1 and 7, 19 are congruent to 3 modulo 4 neither 560 nor 570 can be expressed as the sum of two squares.

On the other hand,

$$\begin{aligned} 580 &= 2^2.5.29 = 2^2(2^2+1^2)(5^2+2^2) \\ &= 24^2 + 2^2 \\ &= 18^2 + 16^2. \end{aligned}$$

NUMBER THEORY 1997

Question 1

(i) $253 = 2.161 - 69$

$161 = 2.69 + 23$

$69 = 3.23$

Thus $\gcd(161, 253) = 23 = 161 - 2.69$

$= 161 - 2(2.161 - 253)$

$= (-3).161 + 2.253$;

therefore $x = -3$, $y = 2$.

(ii) Since $F_1 = 1$ and $F_3 = 2$, $F_5 = 5$, so that $2F_3 - F_5 + 2 = 1$, the statement is true for $n = 1$.

Suppose that the statement is true for $n = k$.

Then

$$F_1 + 2F_2 + \cdots + kF_k = (k+1)F_{k+2} - F_{k+4} + 2.$$

Thus

$$F_1 + 2F_2 + \cdots + kF_k + (k+1)F_{k+1}$$
$$= (k+1)(F_{k+1} + F_{k+2}) - F_{k+4} + 2$$
$$= (k+1)F_{k+3} - F_{k+4} + 2.$$

But $F_{k+4} = F_{k+5} - F_{k+3}$ so that

$$F_1 + 2F_2 + \cdots + kF_k + (k+1)F_{k+1}$$
$$= (k+1)F_{k+3} - (F_{k+5} - F_{k+3}) + 2$$
$$= (k+2)F_{k+3} - F_{k+5} + 2.$$

So the statement is true for $n = k+1$. As the statement is true for $n = 1$ and, for each integer $k \geq 1$, is true for $n = k+1$ if it is true for $n = k$, the statement is true for all positive integers n, by the Principle of Mathematical Induction.

(iii) Since $\gcd(a,b) = 1$, there exist integers m, n such that $ma + nb = 1$ and since $a \mid bc$, there exists an integer k such that $bc = ka$. Thus

$$c = (ma + nb)c = mac + nka$$
$$= (mc + nk)a.$$

Therefore $a \mid c$.

Question 2

(i) FALSE: $6.4 + 1 = 25 = 5^2$.

(ii) TRUE: As $3 \nmid 6k+5$ and $6k+5$ is odd, every prime divisor of $6k+5$ is congruent to 1 or 5 modulo 6. But the product of integers congruent to 1 modulo 6 is congruent to 1 modulo 6. Since $6k+5 \equiv 5 \pmod 6$ it must have at least one prime divisor congruent to 5 modulo 6.

(iii) FALSE: $\gcd(4,9) = 1$ but $\gcd(6.4+1, 6.9+1) = \gcd(25, 55) = 5$.

(iv) TRUE. Suppose that there are only finitely many primes of the form $6k+5$, say

$p_1, \cdots, p_n$ and consider

$$N = 6(p_1 \cdots p_n) - 1 = 6((p_1 \cdots p_n) - 1) + 5.$$

Since N is congruent to 5 modulo 6, it must, by (ii), have a prime divisor p which is congruent to 5 modulo 6. But then, by hypothesis $p = p_j$ for some j. Thus $p \mid N$ and $p \mid 6(p_1 \cdots p_n)$ so that $p \mid 1$, which is absurd. This contradiction shows that there are infinitely many primes congruent to 5 modulo 6.

Question 3

(i) Suppose that $na \equiv nb \pmod{mn}$. Then there exists an integer k such that $na - nb = kmn$. Thus $a - b = km$ so that $a \equiv b \pmod{m}$.

From $48x \equiv 12 \pmod{150}$ we obtain $8x \equiv 2 \pmod{25}$ and

$$8x \equiv 2 \pmod{25} \iff -x \equiv 6 \pmod{25}$$
$$\iff x \equiv 19 \pmod{25}.$$

(ii) Since

$$x^3 - 2x - 4 = (x-1)(x^2+x-1) - 5,$$

it follows that modulo 5

$$\begin{aligned} x^3 - 2x - 4 &\equiv (x-1)(x^2+x-1) \\ &\equiv (x-1)(x^2-4x+4) \\ &\equiv (x-1)(x-2)^2. \end{aligned}$$

Thus the solution is $x \equiv 1 \pmod 5$ or $x \equiv 2 \pmod 5$.

[Alternatively: solve by inspection.]

(iii) $x \equiv 2 \pmod{11}$ and $x \equiv 2 \pmod 5$

$$\iff x \equiv 2 \pmod{55}.$$

$x \equiv 2 \pmod{55} \Rightarrow x = 2, 57, 112$ and $112 \equiv 1 \pmod 3$.

Thus 112 is the smallest positive integer which satisfies the congruences simultaneously.

Question 4

(i) By FLT, $3^{12} \equiv 1 \pmod{13}$ and $2^{12} \equiv 1 \pmod{13}$. Therefore

$$3^{100} = (3^{12})^8 3^4 \equiv 3^4 \equiv (-4)(-4) \equiv 3 \pmod{13}$$

and

$$2^{100} = (2^{12})^8 2^4 \equiv 2^4 \equiv 3 \pmod{13}.$$

Thus $3^{100} \equiv 2^{100} \pmod{13}$; that is, $13 \mid (3^{100} - 2^{100})$.

(ii) By Wilson's Theorem, $16! \equiv -1 \pmod{17}$; that is $17 \mid (16! + 1)$. Each prime less than 17 divides $16!$ and so cannot divide $16! + 1$. Therefore 17 is the smallest prime divisor of $16! + 1$.

(iii) Note first, using FLT, that

$$24^{24} \equiv 3^{24} \equiv (3^6)^4 \equiv 1 \pmod 7$$
$$24^{24} \equiv 2^{24} \equiv (2^{10})^2 2^4 \equiv 16 \equiv 5 \pmod{11}.$$

Thus 24^{24} is a simultaneous solution of the congruences

$$x \equiv 1 \pmod 7, \quad x \equiv 5 \pmod{11}.$$

If $x \equiv 5 \pmod{11}$ then $x = 5, 16, 27, 38, 49, 60, 71, \ldots$ and $71 \equiv 1 \pmod 7$. Since the congruence have a unique solution modulo 77, $24^{24} \equiv 71 \pmod{77}$ and so ~~77~~ 71 is the smallest positive remainder when 24^{24} is divided by 77.

Question 5

(i) A positive integer n is perfect if $\sigma(n) = 2n$. Suppose $k \geq 2$ is an integer and $2^k - 1$ is prime. Then $\sigma(2^k - 1) = 2^k$. Since 2^{k-1} and $2^k - 1$ are relatively prime

$$\sigma(2^{k-1}(2^k-1)) = \sigma(2^{k-1})\sigma(2^k-1) = (2^k-1)2^k$$
$$= 2 \cdot 2^{k-1}(2^k-1).$$

Hence $2^{k-1}(2^k-1)$ is perfect.

(ii) (a) If n is a prime

$$n + 2\varphi(n) = n + 2(n-1) = 3n - 2$$

so $n + 2\varphi(n)$ is not divisible by 3.

(b) Let $n = p^2$ where p is a prime. Then

$$n + 2\varphi(n) = p^2 + 2\varphi(p^2) = p^2 + 2(p^2 - p)$$
$$= 3p^2 - 2p.$$

Thus $n + 2\varphi(n) \equiv -2p \equiv p \pmod 3$. Thus $n + 2\varphi(n) \equiv 0 \pmod 3$ if and only if

$p \equiv 0 \pmod 3$; that is, if and only if $p = 3$.

(c) Let $n = pq$ where $p > 3$ and $q > 3$ are distinct primes. Then

$$n + 2\varphi(n) = pq + 2(p-1)(q-1)$$
$$= 3pq - 2p - 2q + 2.$$

If $n + 2\varphi(n) \equiv 0 \pmod 3$ then $2(p+q) \equiv 2 \pmod 3$ and so $p + q \equiv 1 \pmod 3$. Since $p > 3$ and $q > 3$ we must have $p \equiv q \equiv 2 \pmod 3$.

Question 6

(i) The discriminant is $36 + 24 = 60$ so solutions exist if and only if $(60/47) = 1$. Now

$$\begin{aligned}(60/47) &= (13/47) && 2.1(a)\\ &= (47/13) && \text{LQR}\\ &= (8/13) && 2.1(a)\\ &= (4/13)(2/13) && 2.1(c)\\ &= (2/13) && 2.1(b)\\ &= -1 && 3.2.\end{aligned}$$

Thus the congruence has no solution.

(ii)
$$\begin{aligned}(-39/67) &= (28/67) && 2.1(a)\\ &= (4/67)(7/67) && 2.1(c)\\ &= (7/67) && 2.1(b)\\ &= -(67/7) && \text{LQR}\\ &= -(4/7) && 2.1(a)\\ &= -1 && 2.1(b)\end{aligned}$$

(iii) By LQR

$$(3/p) = \begin{cases} (p/3) & \text{if } p \equiv 1 \pmod 4 \\ -(p/3) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Also

$$(p/3) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Thus $(3/p) = 1$ if and only if either $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$, that is $p \equiv 1 \pmod{12}$, or $p \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$, that is $p \equiv 11 \equiv -1 \pmod{12}$.

Thus $(3/p) = 1$ if $p \equiv \pm 1 \pmod{12}$ and $(3/p) = -1$ otherwise, that is $p \equiv \pm 5 \pmod{12}$.

Question 7

(i)
$$\begin{aligned} 57 &= 1.32 + 25 \\ 32 &= 1.25 + 7 \\ 25 &= 3.7 + 4 \\ 7 &= 1.4 + 3 \\ 4 &= 1.3 + 1 \\ 3 &= 3.1 \end{aligned}$$

Thus $\frac{57}{32} = [1, 1, 3, 1, 1, 3]$

The convergents can be found from the table

1	2	3	4	5	6
1	2	7	9	16	57
1	1	3	1	1	3
1	1	4	5	9	32.

It follows that

$$57.9 - 32.16 = 1$$

so that $x = 9$, $y = 16$ is one solution of the Diophantine equation. It is the solution in which y takes its smallest positive value, since values of y in solutions differ by multiples of 57.

(ii) Put $x = [\langle 1, 2 \rangle]$. Then

$$x = [1, 2, x] = 1 + \frac{1}{2 + \frac{1}{x}} = 1 + \frac{x}{2x+1} = \frac{3x+1}{2x+1}.$$

Thus $x(2x+1) = 3x+1$, so

$$2x^2 - 2x - 1 = 0.$$

Since $x > 0$, $\quad x = \frac{2 + \sqrt{12}}{4} = \frac{1+\sqrt{3}}{2}$.

Now

$$\alpha = [0, 1, x] = \frac{1}{1 + \frac{1}{x}} = \frac{x}{x+1} = \frac{1+\sqrt{3}}{3+\sqrt{3}} = \frac{(1+\sqrt{3})(3-\sqrt{3})}{6} = \frac{\sqrt{3}}{3}.$$

The convergents can be found from the table

1	2	3	4	5	6
0	1	1	3	4	11
0	1	1	2	1	2
1	1	2	5	7	19.

Thus $C_1 = 0$, $C_2 = 1$, $C_3 = \frac{1}{2}$, $C_4 = \frac{3}{5}$, $C_5 = \frac{4}{7}$, $C_6 = \frac{11}{19}$.

Now
$$|\alpha - C_5| < \frac{1}{7.19} < \frac{1}{100}$$

and
$$|\alpha - C_4| > \frac{1}{2.5.7} > \frac{1}{100}.$$

Thus C_5 is the first convergent with the required accuracy.

Question 8

(i) Since the period of the continued fraction is 2, solutions are determined by the even convergents. The convergents can be found from the table

	3	10	63	199
3	3	6	3	
1	3	19	60	

Solutions are $(10, 3)$ and $(199, 60)$.

(ii) Since $(3, 4, 5)$ is a primitive Pythagorean triple, $(12, 16, 20)$ is a non-primitive triple with the required property. To find the required primitive triple, we need positive integers m, n which are relatively prime and of opposite parity such that $mn = 10$. Taking $m = 5, n = 2$ gives the triple $(20, 21, 29)$.

(iii) Suppose (x, y, z) is a solution in positive integers. Then

$$x^3 - 4y^3 = 2z^3.$$

Thus x^3 is even and so x is even, say $x = 2x_1$. Then

$$8x_1^3 - 4y^3 = 2z^3$$

so

$$z^3 = 4x_1^3 - 2y^3$$

and hence z is even, say $z = 2z_1$. Then

$$8z_1^3 = 4x_1^3 - 2y^3$$

so that

$$y^3 = 2x_1^3 - 4z_1^3$$

and hence y is even, say $y = 2y_1$. Then

$$8y_1^3 = 2x_1^3 - 4z_1^3$$

so that

$$x_1^3 - 4y_1^3 = 2z_1^3;$$

that is, (x_1, y_1, z_1) is a solution. Thus if (x, y, z) is a positive solution, then $(\frac{x}{2}, \frac{y}{2}, \frac{z}{2})$ is a positive solution. As infinite descent through positive integers is impossible, the equation has no positive solution.

NUMBER THEORY 1998.

Question 1

(i) $126 = 1.87 + 39$

$87 = 2.39 + 9$

$39 = 4.9 + 3$

$9 = 3.3$.

Thus

$$\begin{aligned} \gcd(87, 126) = 3 &= 39 - 4.9 \\ &= 39 - 4(87 - 2.39) \\ &= 9(126 - 87) - 4.87 \\ &= 87(-13) - 126(-9). \end{aligned}$$

So a particular solution of the Diophantine equation is $x = -13$, $y = -9$. A solution with x and y both positive is

$$x = -13 + \frac{126}{3} = 29, \quad y = -9 + \frac{87}{3} = 20.$$

(ii) As $1 = \frac{1}{2}.1^2.(1+1)$, the formula holds for $n = 1$. Suppose that it holds for $n = k$. Then

$$1 + 5 + \cdots + \tfrac{1}{2}k(3k-1) = \tfrac{1}{2}k^2(k+1)$$

so that

$$\begin{aligned} 1 + 5 + \cdots + \tfrac{1}{2}k(3k-1) + \tfrac{1}{2}(k+1)(3k+2) &= \tfrac{1}{2}k^2(k+1) + \tfrac{1}{2}(k+1)(3k+2) \\ &= \tfrac{1}{2}(k+1)(k^2 + 3k + 2) \\ &= \tfrac{1}{2}(k+1)^2(k+2). \end{aligned}$$

Thus if the formula holds for $n = k$, then it holds for $n = k+1$. By the Principle of Induction, the formula holds for all positive integers n.

(iii) Let $d = \gcd(m, n)$. As $m = 7n + 4$, $d \mid 4$ so that $d = 1, 2$ or 4. But $n = 4k + 3$ for some integer k so that n is odd. Thus $d = 1$.

Question 2

(i) For each $i = 1, \ldots, r$, $p_i \equiv 2 \pmod 3$ so that $p_i^2 \equiv 1 \pmod 3$. Thus

$$(p_1 \cdots p_r)^2 = p_1^2 \cdots p_r^2 \equiv 1 \pmod 3.$$

(ii) A number of the form $3k+2$ is not divisible by 3. Thus each of its prime divisors is congruent to 1 or 2 modulo 3. If all the prime divisors were congruent to 1 modulo 3, then $3k+2$ would be congruent to 1 modulo 3, which is not the case. So $3k+2$ has at least one prime divisor congruent to 2 modulo 3.

(iii) Suppose that the number of primes of the form $3k+2$ is finite and that $p_1, \ldots, p_r$ is a complete list of such primes. Then $N = (p_1 \cdots p_r)^2 + 1$ is of the form $3k+2$ by part (i). Hence from part (ii), it has a prime divisor of the same form; that is $p_j \mid N$ for some j. Then $p_j \mid N$ and $p_j \mid (p_1 \cdots p_r)^2$ so that $p_j \mid 1$ which is a contradiction. Hence there are infinitely many primes of the form $3k+2$.

Question 3

(i) As $n \equiv 4 \pmod 6$, there is an integer k such that $n = 6k+4$ so that

$$12n+5 = 72k + 53.$$

Therefore

$$12n+5 \equiv 53 \equiv 5 \pmod 8$$

and

$$12n+5 \equiv 53 \equiv 8 \pmod 9.$$

(ii) There are p numbers in the list, so it is enough to show that no two distinct numbers are congruent modulo p. Suppose that

$$2 + ra \equiv 2 + sa \pmod p$$

where $0 \leq r < s < p$. Then $ra \equiv sa \pmod p$. But $\gcd(a, p) = 1$, so that $r \equiv s \pmod p$ which is a contradiction. So the list forms a complete set of residues modulo p.

(iii) Firstly

$$3x \equiv 5 \pmod{11} \iff x \equiv 20 \equiv 9 \pmod{11}.$$

Next,

$$x \equiv 9 \pmod{11} \Rightarrow x = 9, 20, 31, 42, \ldots$$

and $42 \equiv 2 \pmod 5$.

Finally,

$x \equiv 9 \pmod{11}$ and $x \equiv 2 \pmod 5 \Rightarrow x = 42, 97, \ldots$

and $97 \equiv 1 \pmod 3$.

Thus the smallest positive integer satisfying the congruences simultaneously is $\underline{97}$.

Question 4

(i)(a) By FLT, $5^{12} \equiv 1 \pmod{13}$ so that

$$5^{50} = (5^{12})^4 5^2 \equiv 25 \equiv -1 \pmod{13}.$$

Also $3^{12} \equiv 1 \pmod{13}$ so that

$$3^{30} = (3^{12})^2 3^6 \equiv 3^6 \equiv 27 \cdot 27 \equiv 1 \pmod{13}.$$

Thus $5^{50} + 3^{30} \equiv 0 \pmod{13}$ so the remainder when $5^{50} + 3^{30}$ is divided by 13 is 0.

(b) As $p \equiv 0 \pmod p$, $p^{q-1} \equiv 0 \pmod p$.

By FLT, $q^{p-1} \equiv 1 \pmod p$. Thus

$$p^{q-1} + q^{p-1} \equiv 1 \pmod p.$$

Similarly

$$p^{q-1} + q^{p-1} \equiv 1 \pmod q.$$

As p and q are distinct primes

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

by Theorem 1.3.

(ii)(a) As the cycle is of length 18, the order of 10 modulo 19 is 18.

(b) $10^{18} \equiv 1 \pmod{19}$ so that $(10^9)^2 \equiv 1 \pmod{19}$.

Hence $10^9 \equiv 1 \pmod{19}$ or $10^9 \equiv -1 \pmod{19}$.

We cannot have $10^9 \equiv 1 \pmod{19}$ for then the order of 10 modulo 19 would be a divisor of 9. Hence $10^9 \equiv -1 \pmod{19}$.

(c) The recurring decimal of $12/19$ has the same cycle as that of $1/19$ with a different starting point.

As

$$120 = 6.19 + 6$$
$$60 = 3.19 + 3,$$

the cycle starts with $\cdot 63\ldots$, so

$$\frac{12}{19} = 0.\langle 631578947368421052\rangle.$$

Question 5

(i) (a) $\sigma(74) = \sigma(2)\sigma(37) = 3.38 = 114 < 2.74$ so 74 is not abundant.

(b) $\sigma(174) = \sigma(2.3.29) = \sigma(2)\sigma(3)\sigma(29)$
$= 3.4.30 = 360 > 2.174$
so 174 is abundant.

(c) If $p \neq 2$, $p \neq 5$,
$$\sigma(10p) = \sigma(2)\sigma(5)\sigma(p) = 18(p+1)$$
and $18(p+1) > 20p$ if and only if $2p < 18$; that is, $p = 3$ or $p = 7$.

Also
$$\sigma(20) = \sigma(2^2)\sigma(5) = 42 > 2.20$$
so 20 is abundant, and
$$\sigma(50) = \sigma(2)\sigma(5^2) = 93 < 2.50$$
so 50 is not abundant.

Thus the prime numbers p for which $10p$ is abundant are 2, 3 and 7.

(ii) We have
$$\varphi(4p) = \varphi(4)\varphi(p) = 2(p-1),$$
$$\varphi(4p-2) = \varphi(2)\varphi(2p-1) = 2p-2;$$
that is, $\varphi(4p) = \varphi(4p-2)$.

Question 6

(i) The discriminant is $5^2 - 4.2.4 = -7$. The congruence has solutions if and only if -7 is a quadratic residue of 37. Now

$$(-7/37) = (30/37) \qquad 2.1(a)$$
$$= (2/37)(3/37)(5/37) \qquad 2.1(c).$$

By 3.2, $(2/37) = -1$ and by 4.4, $(3/37) = 1$.

By LQR
$$(5/37) = (37/5) = (2/5) = -1.$$

Thus $(-7/37) = 1$ and so the congruence has solutions.

(ii) $(67/107) = -(107/67)$ LQR
$= -(40/67)$ 2.1 (a)
$= -(2/67)(5/67)$ 2.1.(b)(c)
$= (5/67)$ 3.2

And
$$(5/67) = (67/5) = (2/5) = -1.$$

Thus $(67/107) = -1$.

(iii) As
$$(6/p) = (2/p)(3/p),$$
$(6/p) = 1$ if and only if either $(2/p) = 1$ and $(3/p) = 1$ or $(2/p) = -1$ and $(3/p) = -1$.

For $(2/p) = 1$ and $(3/p) = 1$ we have
$$p \equiv 1, 7 \pmod 8 \text{ and } p \equiv 1, 11 \pmod{12};$$
that is, $p \equiv 1, 23 \pmod{24}$.

For $(2/p) = -1$ and $(3/p) = -1$ we have

$p \equiv 3, 5 \pmod 8$ and $p \equiv 5, 7 \pmod{12}$;

that is, $p \equiv 5, 19 \pmod{24}$.

Thus $(6/p) = 1$ if and only if p is congruent to 1, 5, 19 or 23 modulo 24.

Question 7

(i) $39 = \underline{2} \cdot 14 + 11$

$14 = \underline{1} \cdot 11 + 3$

$11 = \underline{3} \cdot 3 + 2$

$3 = \underline{1} \cdot 2 + 1$

$2 = \underline{2} \cdot 1$

Thus

$$\frac{39}{14} = [2, 1, 3, 1, 2] = [2, 1, 3, 1, 1, 1].$$

(ii) Put $x = \langle 3, 1 \rangle$. Then

$$x = [3, 1, x] = 3 + \frac{1}{1 + \frac{1}{x}} = 3 + \frac{x}{x+1} = \frac{4x+3}{x+1}.$$

Hence $x^2 - 3x - 3 = 0$ so that, as $x > 0$,

$$x = \frac{3 + \sqrt{21}}{2}.$$

Thus

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

$$= \frac{2(4 + \sqrt{21})}{3 + \sqrt{21}} = \frac{2(4 + \sqrt{21})(\sqrt{21} - 3)}{12}$$

$$= \frac{\sqrt{21} + 9}{6}.$$

(iii) $x_1 = \frac{\sqrt{5}}{2} = 1 + \frac{\sqrt{5} - 2}{2}$

$x_2 = \frac{2}{\sqrt{5} - 2} = 2\sqrt{5} + 4 = 8 + (2\sqrt{5} - 4)$

$x_3 = \frac{1}{2\sqrt{5} - 4} = \frac{2\sqrt{5} + 4}{4} = 2 + \frac{\sqrt{5} - 2}{2}$

$x_4 = \frac{2}{\sqrt{5} - 2} = x_2$.

Thus

$$\frac{\sqrt{5}}{2} = [1, \langle 8, 2 \rangle].$$

Question 8

(i)(a) We should require $2mn = 14$, that is $mn = 7$ with m and n of opposite parity. Thus there are no primitive Pythagorean triples with even member 14.

(b) $2mn = 16$, that is $mn = 8$, has one solution with $m > n$ and m and n of opposite parity, namely $m = 8$, $n = 1$. The required primitive Pythagorean triple is $(16, 63, 65)$.

(ii) As $31 \mid 620$ and $31^2 \nmid 620$, 620 cannot be written as the sum of two squares.

$$610 = 2 \cdot 5 \cdot 61 = (6^2 + 5^2)(3^2 + 1^2)$$

$$= 23^2 + 9^2 = 21^2 + 13^2.$$

(iii) Suppose that $\sqrt{7} = \frac{m}{n}$ where m and n are positive integers. Then

$$\frac{7n - 2m}{m - 2n} = \frac{7 - 2\sqrt{7}}{\sqrt{7} - 2} = \frac{(7 - 2\sqrt{7})(\sqrt{7} + 2)}{3} = \frac{3\sqrt{7}}{3}$$

$$= \sqrt{7}.$$

But ~~$\sqrt{7} > 2$ so that $m > 2n$. Hence~~ $2 < \sqrt{7} < 3$ so that $0 < m - 2n < n$. Hence

the assumption that $\sqrt{7}$ can be written as the quotient of two positive integers gives rise to an expression of $\sqrt{7}$ as a quotient of positive integers with smaller denominator. Since there cannot be an infinite strictly decreasing sequence of positive integers, $\sqrt{7}$ cannot be so expressed; that is, $\sqrt{7}$ is irrational.