Solutions to 2MP62 May 1999 examination

1.

(i) From $x-1<[x]\le x$, we deduce that, if $[x]\ge n$ then $x\ge [x]\ge n$. Conversely, if $x\ge n$, then $[x]>x-1$ gives $[x]>n-1$. But $[x]$ is an integer, so $x\ge n$.

Replace x by ay and n by $a[y]$: we have

$$[ay]\ge a[y] \Longleftrightarrow ay\ge a[y].$$

But the second inequality follows immediately from $y\ge [y]$ and $a\ge 0$.

4 marks. *First part from exercise sheet, second part unseen.*

(ii) The number of positive multiples of an integer $k>0$ which are $\le n$ is clearly $[\frac{n}{k}]$. To count the power of p dividing $n!$, since p is prime, it is enough to count the powers of p dividing $1,2,3,\ldots,n$ and add these powers up. Now, the number of multiples of p among $1,2,3,\ldots,n$ is $\left[\frac{n}{p}\right]$. Each multiple of p^2 among $1,2,3,\ldots,n$ gives an additional power of p dividing into $n!$, giving $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]$ so far. Continuing in this way we get that the total power of p is as in the given formula.

Let $50!=2^{a_1}5^{b_1}c_1$ where c_1 is not a multiple of 2 or 5. Then the power of 10 dividing 50! is clearly the smaller of a_1 and b_1. Working out a_1 we get

$$\left[\frac{50}{2}\right]+\left[\frac{50}{4}\right]+\left[\frac{50}{8}\right]+\left[\frac{50}{16}\right]+\left[\frac{50}{32}\right],$$

since all subsequent terms are zero. This gives $a_1=25+12+6+3+1=47$. Working out b_1 we get

$$\left[\frac{50}{5}\right]+\left[\frac{50}{25}\right],$$

since all subsequent terms are zero. This gives $b_1=10+2=12$. So, there are min(47,12) $=12$ zeros at the end of 50!.

Let $25!=2^{a_2}5^{b_2}c_2$ where c_2 is not a multiple of 2 or 5. Working out a_2 we get

$$\left[\frac{25}{2}\right]+\left[\frac{25}{4}\right]+\left[\frac{25}{8}\right]+\left[\frac{25}{16}\right],$$

since all subsequent terms are zero. This gives $a_2=12+6+3+1=22$. Working out b_2 we get

$$\left[\frac{25}{5}\right]+\left[\frac{25}{25}\right],$$

since all subsequent terms are zero. This gives $b_2=5+1=6$. Let $\binom{50}{25}=\frac{50!}{25!25!}=2^{a_3}5^{b_3}c_3$ where c_3 is not a multiple of 2 or 5. Then $a_3=a_1-2a_2=3$ and $b_3=b_1-2b_2=0$. So, there are min(3,0) $=0$ zeros at the end of $\binom{50}{25}$.

10 marks. *First part in lectures, second part similar to exercise sheet question.*

(iii) The typical term in the expression (ii) for the power of p dividing $(ab)!$ is $[(ab)/p^k]$ and by (i) this is $\ge a[b/p^k]$, which is a times the corresponding term in the expression (ii) for the power of p dividing $b!$. This applies to all the terms in the expression so adding them up gives that the power of p dividing $(ab)!$ is $\ge a$ times the power of p dividing $b!$. It now follows that, for all primes p, the prime-power expressions for $(ab)!$, $b!$ and $(b!)^a$ have the form

$$(ab)!=\ldots p^r\ldots,\qquad b!=\ldots p^s\ldots,\qquad (b!)^a=\ldots p^{sa}\ldots,$$

and $r\ge sa$. Hence by prime-power decompositions, $(b)!^a|(ab)!$.

6 marks. *Unseen.*

2. For $n \geq 1$ define $\phi(n)$ to be the number of integers x satisfying $1 \leq x \leq n$ and $(x, n) = 1$. Let $\{x_1, \ldots, x_k\}$ be complete set of distinct residues (mod n) which are coprime to n, so that $k = \phi(n)$. Let $(a, n) = 1$. Then each ax_i is coprime to n (since both of a and x_i are coprime to n) and $ax_i \equiv ax_j \iff x_i \equiv x_j$ (since $(a, n) = 1$) $\iff i = j$. It follows that $ax_1, \ldots, ax_k$ are all distinct (mod n) and are all coprime to n, giving that $\{ax_1, \ldots, ax_k\}$ is the same set (mod n) as $\{x_1, \ldots, x_k\}$. Hence $(ax_1)(ax_2)\ldots(ax_k) \equiv x_1x_2\ldots x_k$, so $a^k(x_1x_2\ldots x_k) \equiv x_1x_2\ldots x_k \pmod{n}$. But $(x_1x_2\ldots x_k, n) = 1$ (since each $(x_i, n) = 1$), and so we can cancel $x_1x_2\ldots x_k$ from both sides to give $a^k \equiv 1$, that is: $a^{\phi(n)} \equiv 1 \pmod{n}$, as required.
6 marks. *Bookwork from lectures.*

(i) Since $(a, b) = 1$ there exist integers s, t satisfying $as + bt = 1$. Multiplying by c gives $(as)c + (bt)c = c$, that is: $a(sc) + (bc)t = c$; the first term of the LHS has a factor of a, and the second term is also divisible by a, by our given assumption that $a|bc$. Hence a also divides the RHS, that is $a|c$, as required. Can alternatively use prime power decompositions.
3 marks. *Example from lectures.*

(ii) Since $a|c$ and $b|c$, write $c = ja, c = kb$. Then $ja = kb$ so $a|kb$. But $(a, b) = 1$, so (using (i)), $a|k$. Writing $k = \ell a$, we have that $c = kb = \ell ab$, and so $ab|c$, as required.
4 marks. *Seen similar on exercise sheet.*

(iii) $x \equiv y \pmod{a}$ and $x \equiv y \pmod{b} \iff a|(x-y)$ and $b|(x-y) \iff ab|(x-y)$ [the forward direction from (ii), the reverse direction from $a|ab$ and $b|ab$] $\iff x \equiv y \pmod{ab}$.
3 marks. *Seen similar in lectures.*

(iv) Since $(a, b) = 1$, we have $b^{\phi(a)} \equiv 1 \pmod{a}$ by Euler's Theorem, and so $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{a}$, since $a^{\phi(b)} \equiv 0^{\phi(b)} \equiv 0 \pmod{a}$. Similarly $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{b}$. Hence $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$, by (iii).
4 marks. *Unseen.*

3.
(i) A *Carmichael number* is any n such that n is composite, and, for every b with $(b, n) = 1$, we have $b^{n-1} \equiv 1 \bmod n$. Let $n = q_1 \ldots q_k$ be as in the question. Then n is composite since $k \geq 2$. Let $(b, n) = 1$. Then $(b, q_i) = 1$ for all i. By Fermat's theorem, $b^{q_i - 1} \equiv 1 \bmod q_i$. But $n - 1 = k_i(q_i - 1)$ say, since we are given that $(q_i - 1)|(n - 1)$. Hence

$$b^{n-1} = \left(b^{q_i-1}\right)^{k_i} \equiv 1 \pmod{q_i}.$$

Since the congruence b^{n-1} holds mod q_i for each i, it holds mod the lcm of the q_i which is their product n since they are pairwise coprime. That is: $b^{n-1} \equiv 1 \pmod{n}$, as required.
6 marks. *Bookwork from lectures.*

(ii) We know any prime $p > 3$ satisfies $p \equiv \pm 1 \pmod{6}$. If $p \equiv -1 \pmod{6}$ then we would have $2p - 1 \equiv -3 \pmod{6}$, which would contradict $2p - 1$ prime. So, we can't have $p \equiv -1 \pmod{6}$, which means we must have $p \equiv 1 \pmod{6}$. Now, $n - 1 = p(2p-1)(3p-2) - 1 = (p-1)(6p^2 - p + 1)$; further, $(6p^2 - p + 1)$ is a multiple of 6 (since $p \equiv 1 \pmod{6}$). Hence, all of $p - 1$, $2(p - 1)$, $3(p - 1)$ are factors of $n - 1$, that is, all of: $p - 1$, $(2p - 1) - 1$, $(3p - 2) - 1$ are factors of $n - 1$. Hence, n is a product of distinct primes, $q_1 = p$, $q_2 = 2p - 1$, $q_3 = 3p - 2$, with $(q_i - 1)|(n - 1)$ for all i, and so n is a Carmichael number by (i).

Checking: $p = 5$ gives $2p - 1 = 9$ nonprime, $p = 7$ gives $2p - 1 = 13$ and $3p - 2 = 19$, both prime. So, $p = 7$ is the smallest $p > 3$ for which $p, 2p - 1, 3p - 2$ are all prime, and so $7 \cdot 13 \cdot 19 = 1729$ is the smallest Carmichael number of this form.

8 marks. *Seen similar on exercise sheet.*

(iii) If $k = 2$ then $n = q_1 q_2$ and so $n - 1 = q_1 q_2 - 1 \equiv q_1 - 1 \pmod{q_2 - 1}$, since $q_2 = (q_2 - 1) + 1 \equiv 0 + 1 \equiv 1 \pmod{q_2 - 1}$. But we are given that $(q_2 - 1)|(n - 1)$ and so $n - 1 \equiv 0 \pmod{q_2 - 1}$. Hence $q_1 - 1 \equiv 0 \pmod{q_2 - 1}$, that is: $(q_2 - 1)|(q_1 - 1)$, giving $q_2 - 1 \leq q_1 - 1$, which contradicts $q_1 < q_2$. This shows that $k = 2$ is impossible in (i), and (ii) gives an example with $k = 3$, so that $k = 3$ is the minimum possible.

6 marks. *Unseen.*

4. Miller's test on n to base b (where n be an odd positive integer and b coprime to n). We use $\langle x \rangle$ to denote the least positive residue of x mod n.

Step 1. Let $k = n - 1$, $\langle b^k \rangle = r$. If $r = 1$ then continue, otherwise n *fails* the test.

While k is even and $r = 1$ then repeat the following.

Step 2. Replace k by $k/2$, and replace r by the new value of $\langle b^k \rangle$.

When k fails to be even or r fails to be 1:

If $r = 1$ or $n - 1$ then n *passes* the test.

If $r \neq 1$ and $r \neq n - 1$ then n *fails* the test.

5 marks. *From lectures.*

If $n = p$, prime, then $b^{p-1} \equiv 1 \pmod p$ by Fermat's Theorem, and so n passes Step 1. At any application of Step 2, we have k even and $b^k \equiv 1 \pmod p$, so that $(b^{k/2})^2 \equiv b^k \equiv 1 \pmod p$, and so $b^{k/2} \equiv \pm 1 \equiv 1$ or $p - 1 \pmod p$ [using the fact that, for p prime, $x^2 \equiv 1$ has only the solutions $x \equiv \pm 1 \pmod p$]. If $b^{k/2} \equiv p - 1 \pmod p$ or $k/2$ is odd, then p passes Miller's test to base b, otherwise Step 2 is repeated. Therefore, when Miller's test terminates, p will pass.

5 marks. *From lectures.*

(i) Base $b = 12$; check $(12, 133) = 1$ so that Miller's test is applicable. Now, $12^3 = 1728 \equiv -1 \pmod{133}$, so $12^{132} \equiv (12^3)^{44} \equiv (-1)^{44} \equiv 1 \pmod{133}$. Since $133 = 7 \times 19$ is composite, this gives that 133 is a pseudoprime to base 12. Continuing to Step 2 of Miller's Test: $12^{66} \equiv (12^3)^{22} \equiv (-1)^{22} \equiv 1 \pmod{133}$, and $12^{33} \equiv (12^3)^{11} \equiv (-1)^{11} \equiv -1 \pmod{133}$, so 133 passes Miller's Test to base 12. Hence 133 is a strong pseudoprime to base 12.

3 marks. *Seen similar on an exercise sheet.*

(ii) Base $b = 11$; check $(11, 133) = 1$. Now, $11^3 = 1331 \equiv 1 \pmod{133}$, so $11^{132} \equiv (11^3)^{44} \equiv 1^{44} \equiv 1 \pmod{133}$. Hence 133 is a pseudoprime to base 11. Continuing to Step 2 of Miller's Test: $11^{66} \equiv (11^3)^{22} \equiv 1^{22} \equiv 1 \pmod{133}$, and $11^{33} \equiv (11^3)^{11} \equiv 1^{11} \equiv 1 \pmod{133}$, so 133 passes Miller's Test to base 11, since exponent 33 is odd. Hence 133 is a strong pseudoprime to base 11.

2 marks. *Seen similar on an exercise sheet.*

(iii) Base $b = 8$; check $(8, 133) = 1$. Now, $8^3 = 512 \equiv 113 \pmod{133}$, and $8^6 = (8^3)^2 \equiv 113^2 = 12769 \equiv 1 \pmod{133}$, so $8^{132} \equiv (8^6)^{22} \equiv 1^{22} \equiv 1 \pmod{133}$. Hence 133 is a pseudoprime to base 8. Continuing to Step 2 of Miller's Test: $8^{66} \equiv (8^6)^{11} \equiv 1^{11} \equiv 1 \pmod{133}$, and $8^{33} = (8^6)^5 \cdot 8^3 \equiv 1^5 \cdot 113 \equiv 113 \pmod{133}$, so 133 fails Miller's Test to base 8, since 133 is not congruent to 1 or 132 (mod 133). Hence 133 is not a strong pseudoprime to base 8.

3 marks. *Seen similar on an exercise sheet.*

(iv) Base $b = 2$; check $(2, 133) = 1$. Now, $2^{132} = (2^3)^{44} = 8^{44} = (8^6)^7 \cdot 8^2 \equiv 1^7 \cdot 64$ [from (iii)] $\equiv 64 \pmod{133}$, which is not congruent to 1 (mod 133), and so 133 is neither a pseudoprime nor a strong pseudoprime to base 2, and fails Miller's Test to base 2.

2 marks. *Seen similar on an exercise sheet.*

5.

(i) 'g is a primitive root mod n' means that the order of g mod n is $\phi(n)$, i.e. the smallest $k > 0$ for which $g^k \equiv 1$ mod n is $k = \phi(n)$.

Let g be a primitive root mod n. Assume that $g^r \equiv g^s \pmod{n}$, and without loss of generality take $r \geq s$. Since $(g, n) = 1$ (which follows from g being a primitive root), we can cancel g^s from both sides to get $g^{r-s} \equiv 1 \pmod{n}$, and so $\text{ord}_n g | (r - s)$, giving $\phi(n) | (r - s)$, i.e. $r \equiv s \pmod{\phi(n)}$. Conversely, $r \equiv s \pmod{\phi(n)} \Rightarrow \phi(n)|(r-s) \Rightarrow g^{r-s} \equiv 1 \pmod{n} \Rightarrow g^r \equiv g^s \pmod{n}$.
4 marks. *Bookwork from lectures.*

(ii) Working out powers of 3 mod 34 gives

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^k mod 34	3	9	27	13	5	15	11	33	31	25	7	21	29	19	23	1

This shows that $\text{ord}_{34} 3 = 16 = \phi(34)$ and so 3 is a primitive root mod 34. Now, using the table, $15^x \equiv 21 \pmod{34} \iff (3^6)^x \equiv 3^{12} \pmod{34} \iff 3^{6x} \equiv 3^{12} \pmod{34} \iff 6x \equiv 12 \pmod{\phi(34)} \iff 6x \equiv 12 \pmod{16} \iff 3x \equiv 6 \pmod{8} \iff 3 \cdot 3x \equiv 3 \cdot 6 \pmod{8} \iff x \equiv 2 \pmod{8}$.

Working out the powers of 13 mod 34 gives

k	1	2	3	4
13^k mod 34	13	33	21	1

This shows that $\text{ord}_{34} 13 = 4 \neq 16 = \phi(34)$, and so 13 is not a primitive root mod 34.
8 marks. *Seen similar on exercise sheet.*

(iii) If $x^2 \equiv 1 \pmod{n}$ then $(x, n) = 1$ (since any common factor of x and n would have to divide 1), and so we can write $x \equiv g^k$, for some k (since powers of a primitive root give all numbers mod n which are coprime to n). Then $x^2 \equiv 1 \pmod{n} \iff (g^k)^2 \equiv 1 \pmod{n} \iff g^{2k} \equiv g^0 \pmod{n} \iff 2k \equiv 0 \pmod{\phi(n)} \iff k \equiv 0 \pmod{\phi(n)/2} \iff k \equiv 0, \phi(n)/2 \pmod{\phi(n)} \iff x \equiv g^0, g^{\phi(n)/2} \pmod{n}$ [note that, since $n > 2$ we must have $\phi(n)$ even, and so $\phi(n)/2$ is an integer]. Thus, there are exactly two solutions to the congruence $x^2 \equiv 1 \pmod{n}$. Further, $x \equiv 1$ and $x \equiv -1$ are distinct solutions to this congruence, and so they must be the only solutions, as required.
5 marks. *Seen similar in lectures.*

(iv) We are given: $n = 4h$, $h > 1$ and $x = 2h + 1$. Then $x^2 = (2h + 1)^2 = 4h^2 + 4h + 1 = 4h(h+1)+1 \equiv 1 \pmod{n}$. But x is not congruent to 1 or $-1 \pmod{n}$ [since $1 < 2h+1 < n-1$], and so n cannot have a primitive root by (iii).
3 marks. *Unseen.*

6.

(i) Given m, an integer not divisible by 2 or 5, consider the standard equations which occur in the calculation of the decimal expansion of $\frac{1}{m}$:

$$\begin{aligned} 1 &= r_1, \\ 10r_1 &= mq_1 + r_2, \\ 10r_2 &= mq_2 + r_3, \text{ etc.,} \end{aligned}$$

where $0 < r_i < m$ and $0 \leq q_i \leq 9$ for each i so that the q_i are the decimal digits.

All congruences are mod m in what follows. Clearly

$$r_1 \equiv 1, \quad r_2 \equiv 10r_1 \equiv 10, \quad r_3 \equiv 10r_2 \equiv 10^2, \quad \text{etc.,}$$

and generally $r_{j+1} \equiv 10^j$. It is also clear that the calculation of the decimal places q_i repeats when one of the remainders r_j becomes equal to a previous remainder r_i. I claim that when this happens, $i = 1$. Proof: If $i > 1$ and $r_{i+k} = r_i$ $(k \geq 1)$ is the first repeat then $10r_{(i+k)-1} \equiv r_{i+k} = r_i \equiv 10r_{i-1}$ and 10 can be cancelled since $2 \not| m$ and $5 \not| m$, so that $r_{i-1+k} \equiv r_{i-1}$ and consequently these remainders are equal since both are between 1 and $m-1$. But this contradicts the assumption that $r_{i+k} = r_i$ is the *first* repeat.

Thus recurrence starts with $r_{k+1} = r_1 = 1$, i.e. $q_1 = q_{k+1}, q_2 = q_{k+2}$ and so on. Thus k is the smallest number such that $10^k \equiv 1$, i.e. the order of 10 mod m is k, which is the period length.
8 marks. *Bookwork from lectures.*

(ii) $x^k \equiv 1 \pmod{mn} \iff x^k \equiv 1 \pmod{m}$ and $x^k \equiv 1 \pmod{n}$ [since $(m,n) = 1$] $\iff$ $\text{ord}_m x | k$ and $\text{ord}_n x | k \iff k$ is a common multiple of $\text{ord}_m x$ and $\text{ord}_n x \iff k$ is a multiple of $[\text{ord}_m x, \text{ord}_n x]$. Hence, $\text{ord}_{mn} x = [\text{ord}_m x, \text{ord}_n x]$, as required.
4 marks. *Seen similar in lectures.*

(iii) As usual, $\text{ord}_m 10$ is the smallest $k > 0$ for which $10^k \equiv 1 \pmod{m}$. In each case, by (i), this is the same as the decimal period length of $\frac{1}{m}$.

$10^1 \equiv 10,\ 10^2 \equiv 9,\ 10^3 \equiv 6,\ 10^4 \equiv 4,\ 10^5 \equiv 5,\ 10^6 \equiv 1 \pmod{7}$, so $\text{ord}_7 10 = 6$.
$10^1 \equiv 10,\ 10^2 \equiv 1 \pmod{11}$, so $\text{ord}_{11} 10 = 2$.
$10^1 \equiv 10,\ 10^2 \equiv 9,\ 10^3 \equiv 12,\ 10^4 \equiv 3,\ 10^5 \equiv 4,\ 10^6 \equiv 1 \pmod{13}$, so $\text{ord}_{13} 10 = 6$.
$10^1 \equiv 10,\ 10^2 \equiv 15,\ 10^3 \equiv 14,\ 10^4 \equiv 4,\ 10^5 \equiv 6,\ 10^6 \equiv 9,\ 10^7 \equiv 5,\ 10^8 \equiv 16,\ 10^9 \equiv 7,\ 10^{10} \equiv 2,$
$10^{11} \equiv 3,\ 10^{12} \equiv 13,\ 10^{13} \equiv 11,\ 10^{14} \equiv 8,\ 10^{15} \equiv 12,\ 10^{16} \equiv 1 \pmod{17}$, so $\text{ord}_{17} 10 = 16$.
$\text{ord}_{77} 10 = [\text{ord}_7 10, \text{ord}_{11} 10] = [6, 2] = 6$, by (ii).
$\text{ord}_{91} 10 = [\text{ord}_7 10, \text{ord}_{13} 10] = [6, 6] = 6$, by (ii).
$\text{ord}_{143} 10 = [\text{ord}_{11} 10, \text{ord}_{13} 10] = [2, 6] = 6$, by (ii).
$\text{ord}_{221} 10 = [\text{ord}_{13} 10, \text{ord}_{17} 10] = [6, 16] = 48$, by (ii).

Can also, if desired, reduce computations by using $\text{ord}_m 10 | \phi(m)$.
8 marks. *Unseen.*

7.

(i) $\sigma(n)$ = the sum of the divisors of n which are ≥ 1.
p^a has divisors $1, p, p^2, \ldots p^{a-1}, p^a$ so $\sigma(p^a) = 1 + p + p^2 + \ldots p^a = (p^{a+1} - 1)/(p - 1)$.
Writing $n = p_1^{n_1} \ldots p_k^{n_k}$ (prime power factorization), $\sigma(n) = \frac{p_1^{n_1+1}-1}{p_1-1} \cdots \frac{p_k^{n_k+1}-1}{p_k-1}$.
4 marks. *From lectures.*

(ii) Here is a table of values of $\sigma(p^a)$ for small p and a. Since all rows and columns are strictly increasing, any further entries would be greater than 32 and so are irrelevant.

$a\downarrow$ $p \rightarrow$	2	3	5	7	11	13	17	...	31	...
1	3	4	6	8	12	14	18	...	32	...
2	7	13	31	57						
3	15	40								
4	31									
5	63									

Now the following give all the ways of writing 32 as a product of entries in different columns of the table: 32 or $4 \cdot 8$. These give
$n = 31$ or $3 \cdot 7$, that is: $n = 31$ or 21 are the only solutions to $\sigma(n) = 32$.
7 marks. *Seen similar on exercise sheet.*

(iii) $\sigma(n) = \sigma(2^s)\sigma(2^{s+1} - 1)$ [since $(2^s, 2^{s+1} - 1) = 1$]. But $\sigma(2^s) = (2^{s+1} - 1)/(2 - 1) = 2^{s+1} - 1$, by the formula in (i), and $\sigma(2^{s+1} - 1) = 1 + (2^{s+1} - 1)$ [since $2^{s+1} - 1$ is prime]. So:
$\sigma(n) = (2^{s+1} - 1)(1 + (2^{s+1} - 1)) = 2^{s+1}(2^{s+1} - 1) = 2(2^s(2^{s+1} - 1)) = 2n$. Hence n is perfect.
4 marks. *From lectures.*

(iv) $s(p) = 1$ and $s(p^2) = 1 + p$ for p prime. Any $n > 1$ is divisible by some prime p, and if n is neither prime nor the square of a prime, we must have $p \neq n$ and $p^2 \neq n$. Hence, $1, p, n/p$ are all distinct divisors of n, and all are $\neq n$. Hence $s(n) \geq 1 + p + n/p$, as required.

Now, suppose that $s(n) = 7$. Note that 7 is none of: $0, 1, 1 + p$ for any prime p, so that n is not 1, n is not prime, and n is not the square of a prime. So, $s(n) \geq 1 + p + n/p$, which becomes: $7 \geq 1 + p + n/p$ and so: $n/p \leq 6 - p$, giving

$$n \leq 6p - p^2 = 9 - (p - 3)^2 \leq 9.$$

Thus, we need only check n up to 9. In fact: $s(1) = 0$, $s(2) = 1$, $s(3) = 1$, $s(4) = 3$, $s(5) = 1$, $s(6) = 6$, $s(7) = 1$, $s(8) = 7$ and $s(9) = 4$. Conclusion: $n = 8$ is the only n for which $s(n) = 7$.

5 marks. *Hard, but seen similar in lectures.*

8.

(i) First, note $P_1 = a_0 Q_0 - P_0 = a_0 \cdot 1 - 0 = a_0 = [\sqrt{n}]$
and $Q_1 = (n - P_1^2)/Q_0 = (n - P_1^2)/Q_0 = (n - a_0^2)/1 = n - a_0^2$.

Suppose $Q_k = 1$ for some $k \geq 1$. Then $x_k = P_k + \sqrt{n}$ so $a_k = [x_k] = P_k + [\sqrt{n}] = P_k + a_0$. That is, $a_k - P_k = a_0$. Hence,

$P_{k+1} = a_k Q_k - P_k = a_k - P_k = a_0 = P_1$ and $Q_{k+1} = (n - P_{k+1}^2)/Q_k = (n - a_0^2)/1 = Q_1$.

Furthermore, $x_{k+1} = (P_{k+1} + \sqrt{n})/Q_{k+1} = (P_1 + \sqrt{n})/Q_1 = x_1$ and so $a_{k+1} = [x_{k+1}] = [x_1] = a_1$. This means that rows P_1, Q_1, x_1, a_1 and $P_{k+1}, Q_{k+1}, x_{k+1}, a_{k+1}$ are identical and so clearly $a_{k+1} = a_1, a_{k+2} = a_2, \ldots$. So the continued fraction is $[a_0, \overline{a_1, \ldots, a_k}]$.

6 marks. *Bookwork from lectures.*

(ii) Draw the following table.

k	P_k	Q_k	x_k	a_k
0	0	1	$\sqrt{n}$	d
1	d	d	$\frac{d+\sqrt{n}}{d}$	2
2	d	1	$d + \sqrt{n}$	$2d$

Justification of a_0, a_1, a_2 as follows.

$a_0 = [\sqrt{n}]$. But, for all $d \geq 1$, $d^2 < d^2 + d < d^2 + 2d + 1$ and so $d < \sqrt{d^2 + d} < d + 1$, so that $[\sqrt{n}] = d$, i.e. $a_0 = d$.

$a_1 = \left[\frac{d+\sqrt{n}}{d}\right] = \left[\frac{d+[\sqrt{n}]}{d}\right] = \left[\frac{d+d}{d}\right] = [2] = 2.$

$a_2 = [d + \sqrt{n}] = [d + [\sqrt{n}]] = [d + d] = [2d] = 2d.$

The fact that $Q_2 = 1$ signals recurrence, so that $\sqrt{n} = [d, \overline{2, 2d}]$, as required.

8 marks. *Seen similar on exercise sheet.*

(iii) $d = 4$ gives $n = 20$ i.e. $\sqrt{20} = [4, \overline{2, 8}]$.

Using initial values $p_0 = a_0, q_0 = 1, p_1 = a_0 a_1 + 1, q_1 = a_1$ together with the standard recurrence relations: $p_{k+1} = a_{k+1} p_k + p_{k-1}$ and $q_{k+1} = a_{k+1} q_k + q_{k-1}$ for convergents p/q of $\sqrt{n}$, and the identity $p_k^2 - n q_k^2 = (-1)^{k+1} Q_{k+1}$, we get

k	a_k	p_k	q_k
0	4	4	1
1	2	9	2
2	8	76	17
3	2	161	36
4	8	1364	305
5	2	2889	646

This gives three solutions: $x = 9, y = 2$ and $x = 161, y = 36$ and $x = 2889, y = 646$.

6 marks. *Seen similar on exercise sheet.*