Solutions to MATH342 (Number Theory) May 2002 examination

Question 1.

(i) The number of positive multiples of an integer $k > 0$ which are $\leq n$ is clearly $\left[\frac{n}{k}\right]$. 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.

4 marks. *Seen in lectures.*

(ii) Let $60! = 2^{a_1}5^{b_1}c_1$ where c_1 is not a multiple of 2 or 5. Then the power of 10 dividing 60! is clearly the smaller of a_1 and b_1. Working out a_1 we get $\left[\frac{60}{2}\right] + \left[\frac{60}{4}\right] + \left[\frac{60}{8}\right] + \left[\frac{60}{16}\right] + \left[\frac{60}{32}\right]$, since all subsequent terms are zero. This gives $a_1 = 30 + 15 + 7 + 3 + 1 = 56$. Working out b_1 we get $\left[\frac{60}{5}\right] + \left[\frac{60}{25}\right]$, since all subsequent terms are zero. This gives $b_1 = 12 + 2 = 14$. So, there are min(56,14) = 14 zeros at the end of 60!.

4 marks. *Similar to exercise sheet question.*

(iii) By definition, $[x] \leq x, [y] \leq y, [z] \leq z$, giving that $[x] + [y] + [z]$ is an integer $\leq x + y + z$; so $[x]+[y]+[z]$ must be $\leq$ (the greatest integer $\leq x+y+z$); that is to say, $[x]+[y]+[z] \leq [x+y+z]$.

2 marks. *Unseen.*

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

$$(a+b+c)! = \ldots p^{r_1} \ldots, \quad a! = \ldots p^{r_2} \ldots, \quad b! = \ldots p^{r_3} \ldots, \quad c! = \ldots p^{r_4} \ldots,$$

and $r_1 \geq r_2 + r_3 + r_4$, which is the same as the power of p dividing $a!b!c!$. Hence by prime-power decompositions, $a!b!c! | (a + b + c)!$.

4 marks. *Unseen.*

We already know from (ii) that $60! = 2^{a_1}5^{b_1}c_1$, where $a_1 = 56, b_1 = 14$ and c_1 is not a multiple of 2 or 5. Let $10! = 2^{a_2}5^{b_2}c_2$ where c_2 is not a multiple of 2 or 5. Working out a_2 we get $\left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right]$, since all subsequent terms are zero. This gives $a_2 = 5 + 2 + 1 = 8$. Working out b_2 we get $\left[\frac{10}{5}\right]$, since all subsequent terms are zero. This gives $b_2 = 2$. Let $20! = 2^{a_3}5^{b_3}c_3$ where c_3 is not a multiple of 2 or 5. Working out a_3 we get $\left[\frac{20}{2}\right] + \left[\frac{20}{4}\right] + \left[\frac{20}{8}\right] + \left[\frac{20}{16}\right]$, since all subsequent terms are zero. This gives $a_3 = 10 + 5 + 2 + 1 = 18$. Working out b_3 we get $\left[\frac{20}{5}\right]$, since all subsequent terms are zero. This gives $b_3 = 4$. Let $30! = 2^{a_4}5^{b_4}c_4$ where c_4 is not a multiple of 2 or 5. Working out a_4 we get $\left[\frac{30}{2}\right] + \left[\frac{30}{4}\right] + \left[\frac{30}{8}\right] + \left[\frac{30}{16}\right]$, since all subsequent terms are zero. This gives $a_4 = 15 + 7 + 3 + 1 = 26$. Working out b_4 we get $\left[\frac{30}{5}\right] + \left[\frac{30}{25}\right]$, since all subsequent terms are zero. This gives $b_4 = 6 + 1 = 7$.

Let $\frac{60!}{10!20!30!} = 2^{a_5}5^{b_5}c_5$ where c_5 is not a multiple of 2 or 5. Then $a_5 = a_1 - a_2 - a_3 - a_4 = 56 - 8 - 18 - 26 = 4$ and $b_5 = b_1 - b_2 - b_3 - b_4 = 14 - 2 - 4 - 7 = 1$. So, there is min(4,1) =1 zero at the end of $\frac{60!}{10!20!30!}$.

6 marks. *Similar to exercise sheet question.*

Question 2.

(i) Fermat's Theorem states that:

(a) If p is prime and p does not divide a then $a^{p-1} \equiv 1 \pmod p$.

(b) For any a (whether p divides a or not), we have: $a^p \equiv a \pmod p$.

Proof.

(a) Consider $a, 2a, \ldots, (p-1)a$ $(*)$. For any j in the range $1 \le j \le (p-1)$, we have $p \nmid j$. Since also $p \nmid a$, it follows that $p \nmid ja$; that is, none of the numbers in (*) is congruent to 0 (mod p). Also, imagine $ia \equiv ja \pmod p$ for $i \neq j$ (say, $i < j$) and $1 \le i, j \le (p-1)$; then $(i-j)a \equiv 0 \pmod p$ and so $p \mid (i-j)a$; but $p \nmid (i-j)$, since $0 < i - j < p$, and so $p|a$, a contradiction. Hence $ia \not\equiv ja$ whenever $i \neq j$, $1 \le i, j \le (p-1)$. It follows that the numbers: $a, 2a, \ldots, (p-1)a$ are all distinct mod p and none are 0 mod p. For each of the $p-1$ numbers $a, 2a, \ldots, (p-1)a$ there are only $p-1$ possibilities mod p: $1, 2, \ldots, p-1$. It follows that $\{a, 2a, \ldots, (p-1)a\}$ is the same set as $\{1, 2, \ldots, p-1\}$, possibly with a different order. Hence $a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1)$; that is: $(p-1)!a^{p-1} \equiv (p-1)! \pmod p$. Clearly $((p-1)!, p) = 1$ [since each of $1, \ldots, p-1$ is coprime to p], and so $a^{p-1} \equiv 1 \pmod p$, as required.

(b) If $p \nmid a$, then we have already shown $a^{p-1} \equiv 1 \pmod p$. Multiplying both sides by a gives $a^p \equiv a \pmod p$. If $p \mid a$ then $a^p \equiv a \pmod p$ is trivially true, since $a^p \equiv 0$ and $a \equiv 0 \pmod p$.
5 marks. *Bookwork from lectures.*

(ii) We say that m is a *pseudoprime* to the base b if m is composite and $b^m \equiv b \pmod m$. When $(b, m) = 1$, this is equivalent to: $b^{m-1} \equiv 1 \pmod m$.

By Fermat's theorem, $3^{10} \equiv 1 \pmod{11}$, and so $3^{670} \equiv (3^{10})^{67} \equiv 1^{67} \equiv 1 \pmod{11}$. Similarly, by Fermat's theorem, $3^{60} \equiv 1 \pmod{61}$, and so $3^{660} \equiv (3^{60})^{11} \equiv 1^{11} \equiv 1 \pmod{61}$. Therefore, $3^{670} \equiv 3^{660}3^{10} \equiv 3^{10} \equiv (3^5)^2 \equiv 243^2 \equiv (-1)^2 \equiv 1 \pmod{61}$. In summary, we have shown that: $3^{670} \equiv 1 \pmod{11}$ and $3^{670} \equiv 1 \pmod{61}$; since $(11, 61) = 1$, it follows that $3^{670} \equiv 1$ (mod $(11 \cdot 61 = 671)$. Since $671 = 11 \cdot 61$ is composite, it follows that 3 is a pseudoprime to base 3.
5 marks. *Seen similar on exercise sheet.*

(iii) Since n is a pseudoprime to base b, we have $b^n = b \pmod n$. Squaring both sides give: $(b^n)^2 = b^2 \pmod n$, which is the same as: $(b^2)^n = b^2 \pmod n$, so that n is also a pseudoprime to base b^2.
2 marks. *Unseen.*

(iv) We have: $4^2 = 16 \equiv 1 \pmod{15}$, so that: $4^{14} \equiv (4^2)^7 \equiv 1^7 \equiv 1 \pmod{15}$; since also $15 = 3 \cdot 5$ is composite, this gives that 15 is a pseudoprime to base 4. However, $2^4 = 16 \equiv 1 \pmod{15}$, so that: $2^{14} \equiv (2^4)^3 \cdot 2^2 \equiv 1^4 \cdot 4 \equiv 4 \not\equiv 1 \pmod{15}$, which means that 15 is not a pseudoprime to base 2.
2 marks. *Seen similar on exercise sheet.*

For $n = b^2 - 1$ and base b^2, for odd $b \ge 3$, first note that $n = (b+1)(b-1)$, with both factors ≥ 2, so that n is composite. Also, $b^2 = (b^2 - 1) + 1 = n + 1 \equiv 1 \pmod n$, so that: $(b^2)^{n-1} \equiv 1^{n-1} \equiv 1 \pmod n$, so that n is a pseudoprime to base b^2. For base b, note that $n - 1$ is odd, say that $n = 2k + 1$, giving: $b^{n-1} \equiv b^{2k+1} \equiv (b^2)^k \cdot b \equiv 1^k \cdot b \equiv b \not\equiv 1 \pmod n$ [since $1 < b < b^2 - 1 = n$], so that n is not a pseudoprime to base b.
6 marks. *Unseen.*

Question 3.

(i) 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.

6 marks. *From lectures.*

First compute: $7^2 \equiv 49 \equiv 24$, $7^4 \equiv (7^2)^2 \equiv 24^2 \equiv 576 \equiv 1 \pmod{25}$. This gives, $7^{25-1} \equiv 7^{24} \equiv (7^4)^6 \equiv 1^6 \equiv 1$; the exponent 24 is even, so we continue to compute $7^{12} \equiv (7^4)^3 \equiv 1$; the exponent 12 is still even, so we continue to compute $7^6 \equiv 7^4 \cdot 7^2 \equiv 1 \cdot 49 \equiv 25 - 1$, and so we stop, with 25 passing Miller's test to base 7.

First compute: $5^2 \equiv 25$, $5^4 \equiv 625 \equiv 191$, $5^6 \equiv 5^2 \cdot 5^4 \equiv 25 \cdot 191 \equiv 4775 \equiv 1 \pmod{217}$. So, $5^{216} \equiv (5^6)^{36} \equiv 1^{36} \equiv 1$; the exponent 216 is even so we continue to compute $5^{108} \equiv (5^6)^{18} \equiv 1^{18} \equiv 1$; the exponent 108 is even so we continue to compute $5^{54} \equiv (5^6)^9 \equiv 1^9 \equiv 1$; the exponent 54 is even so we continue to compute $5^{27} \equiv (5^6)^4 \cdot 5^3 \equiv 1^4 \cdot 125 \equiv 125$, which is neither 1 nor $217 - 1 \pmod{217}$. So, 217 fails Miller's test to base 5.

8 marks. *Seen similar on exercise sheet.*

(ii) Given that $b^{n-1} \equiv 1 \pmod{n}$, we see that n passes Step 1 of Miller's Test to base b. Since $n - 1$ is even, we proceed to Step 2; since $b^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$, it fails Miller's Test.

Let $c = (b^{(n-1)/2} - 1, n)$; then by definition, $c | b^{(n-1)/2} - 1$ and $c | n$, so that c is a factor of n. Imagine $c = n$; then we would have $n | b^{(n-1)/2} - 1$, that is: $b^{(n-1)/2} \equiv 1 \pmod{n}$, contradicting the given information that $b^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$. Imagine $c = 1$; then we would have $(b^{(n-1)/2} - 1, n) = 1$; combining this with the given information that $b^{n-1} \equiv 1 \pmod{n}$ gives that $n | b^{n-1} - 1 = (b^{(n-1)/2} + 1)(b^{(n-1)/2} - 1)$, so we would have $n | b^{(n-1)/2} + 1$, that is: $b^{(n-1)/2} \equiv -1 \pmod{n}$, which would again contradict $b^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$. Hence, $c | n$, but $c \neq 1, n$, as required.

6 marks. *Unseen.*

Question 4. All congruences are mod m in what follows. Clearly

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

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 $10 r_{(i+k)-1} \equiv r_{i+k} = r_i \equiv 10 r_{i-1}$ and 10 can be cancelled since $2 \nmid m$ and $5 \nmid m$, 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 length of the period.

9 marks.

Now suppose p is prime, $p \neq 2, p \neq 5$. When the length of the period is $2k$ we have $r_{2k+1} \equiv 10^{2k} \equiv 1$ so that $(10^k)^2 \equiv 1$ and since the modulus is prime, this implies $10^k \equiv \pm 1$. But it cannot be 1 since the period is $2k$ not k so $r_{k+1} \equiv -1$, which in view of $0 < r_i < p$ implies $r_{k+1} = p - 1$.

4 marks.

$r_2 \equiv 10, r_{k+2} \equiv 10^{k+1} = 10^k \cdot 10 \equiv -10 \equiv -r_2, \quad r_{k+3} \equiv 10^{k+1} = 10^k \cdot 10^2 \equiv -10^2 \equiv -r_3$, etc., i.e. $r_{k+j} + r_j \equiv 0,\ j = 1, 2, \ldots$, but both these are strictly between 0 and p so they must add up to p.

Finally, note that, since $10r_i = pq_i + r_{i+1}$ and $10r_{i+k} = pq_{i+k} + r_{i+k+1}$, we can add these two equations to give: $10(r_i + r_{i+k}) = p(q_i + q_{i+k}) + (r_{i+1} + r_{i+k+1})$, so that $10p = p(q_i + q_{i+k}) + p$ (from the previous result), so that $q_i + q_{i+k} = 9$, as required.

7 marks. *All bookwork from lectures.*

Question 5. $\sigma(n) =$ 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 $n = p_1^{n_1} \ldots p_k^{n_k}$, we have: $\sigma(n) = \frac{p_1^{n_1+1}-1}{p_1-1} \cdots \frac{p_k^{n_k+1}-1}{p_k-1}$.
3 marks. *From lectures.*

(i) 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 42 and so are irrelevant.

$a \downarrow$ $p \rightarrow$	2	3	5	7	11	13	17	19	23	29	31	37	41	...
1	3	4	6	8	12	14	18	20	24	30	32	38	42	...
2	7	13	31	57										
3	15	40	156											
4	31	121												
5	63													

Now the following give all the ways of writing 42 as a product of entries in different columns of the table: $7 \cdot 6$ or $3 \cdot 14$ or 42. These give
$n = 2^2 \cdot 5^1$, $2^1 \cdot 13^1$, 41^1, that is: $n = 20, 26, 41$ are the only solutions to $\sigma(n) = 42$. For the case $\sigma(n) = 21$, note that 21 does not occur as an entry anywhere in the table; 7 and 3 each occur exactly once, but in the same column; therefore it is not possible to write 21 as a product of entries in different columns of the table, and so there does not exist n such that $\sigma(n) = 21$.
9 marks. *Seen similar on exercise sheet.*
(ii) We have

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1} < \frac{p^{a+1}}{p - 1} = p^a \left(\frac{p}{p - 1}\right).$$

Also

$$\frac{p}{p - 1} = 1 + \frac{1}{p - 1},$$

so if $p \geq p_0$ then we have

$$\frac{p}{p - 1} = 1 + \frac{1}{p - 1} \leq 1 + \frac{1}{p_0 - 1} = \frac{p_0}{p_0 - 1}.$$

Applying this to $p_0 = 3$ and 5 we get that

$$p \geq 3 \Longrightarrow \frac{\sigma(p^a)}{p^a} < \frac{p}{p - 1} \leq \frac{3}{2}, \qquad q \geq 5 \Longrightarrow \frac{\sigma(q^b)}{q^b} < \frac{q}{q - 1} \leq \frac{5}{4}.$$

As p and q are distinct primes, $(p^a, q^b) = 1$, and so:

$$\frac{\sigma(n)}{n} = \frac{\sigma(p^a)\sigma(q^b)}{p^a q^b} < \frac{3}{2} \times \frac{5}{4} = \frac{15}{8} < 2,$$

as required.
8 marks. *Seen similar on exercise sheet.*

Question 6.
(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 $g^k \equiv 1 \bmod n$ is $k = \phi(n)$.
2 marks. *From lectures.*

(ii) Let $n = ab$ where $a > 2, b > 2$ and $(a, b) = 1$. Let $(g, n) = 1$; that is: $(g, ab) = 1$. First show that $\phi(a)$ is even. Proof: Since $a > 2$, we must have either $a = 2^k, k \geq 2$ or a has an odd prime factor. If $a = 2^k, k \geq 2$, we have $\phi(a) = 2^{k-1}$ which is even. If a has an odd prime factor p, then the formula for $\phi(a)$ has an even factor $p - 1$. In either case, $\phi(a)$ is even. Similarly, $\phi(b)$ is even. Now note the standard result that $(g, ab) = 1 \Rightarrow (g, a) = 1$, and so $g^{\phi(a)} \equiv 1 \bmod a$, by Euler's Theorem. Hence

$$g^{\phi(a)\phi(b)/2} = \left(g^{\phi(a)}\right)^{\phi(b)/2} \equiv 1^{\phi(b)/2} \bmod a,$$

Note that here we use the fact that $\phi(b)$ is even, so that the power on the right is an integer. Similarly by interchanging a and b we get

$$g^{\phi(a)\phi(b)/2} = \left(g^{\phi(b)}\right)^{\phi(a)/2} \equiv 1^{\phi(a)/2} \bmod b,$$

using the fact that $\phi(a)$ is even. Hence $g^{\phi(a)\phi(b)/2} \equiv 1 \bmod a$ and mod b, and hence mod $ab = n$ since $(a, b) = 1$ (Standard result: if the same congruence holds mod a and mod b then it holds mod $\mathrm{lcm}(a, b)$, which here is ab since $(a, b) = 1$.) Using $(a, b) = 1$ again, and the general fact that this implies $\phi(a)\phi(b) = \phi(n)$, we find $g^{\phi(n)/2} \equiv 1 \bmod n$. It follows that every g has order at most $\phi(n)/2$ mod n, and so there does not exist g of order $\phi(n)$; that is, there does not exist a primitive root mod n.
8 marks. *Bookwork from lectures.*

(iii) Working out powers of 5 mod 34 gives

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

This verifies that $\mathrm{ord}_{34}5 = 16 = \phi(34)$ and so 5 is a primitive root mod 34.
3 marks. *Seen similar in exercises.*

(a) From table, $23 \equiv 5^3, 15 \equiv 5^{14} \pmod{34}$ so given equation $23^x \equiv 15 \pmod{34}$ becomes

$$5^{3x} \equiv 5^{14} \pmod{34} \Leftrightarrow 3x \equiv 14 \pmod{16}$$

by the general results that, for a primitive root g mod n: $g^a \equiv g^b \pmod{n} \Leftrightarrow a \equiv b \pmod{\phi(n)}$. This gives $11 \cdot 3x \equiv 11 \cdot 14$, that is: $x \equiv 10 \bmod 16$.
3 marks. *Seen similar in exercises.*

(b) Note that $y^4 \equiv 21 \pmod{34}$ implies that $(y, 34) = 1$ since any common factor would also have to divide the r.h.s. 21 of the congruence, and so would be a common factor of $34, 21$, which are coprime. Hence $y \equiv 5^x \pmod{34}$ for some x (since 5 is a primitive root). Also $5^{12} \equiv 21$ from the table. The given congruence turns into

$$5^{4x} \equiv 5^{12} \pmod{34} \Leftrightarrow 4x \equiv 12 \pmod{16}.$$

by the same general result used in part (a). This gives $x \equiv 3 \bmod 4$, i.e. $x \equiv 3, 7, 11, 15 \pmod{16}$ which, from the table, gives: $y \equiv 23, 27, 11, 7 \bmod 34$.
4 marks. *Seen similar in exercises.*

Question 7.

(i) First, note $P_1 = a_0Q_0 - P_0 = a_0 \cdot 1 - 0 = a_0 = [\sqrt{n}]$
and $Q_1 = (n - P_1^2)/Q_0 = (n - a_0^2)/1 = n - a_0^2$.

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,

$P_{k+1} = a_kQ_k - P_k = a_k - P_k = a_0 = P_1$ 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	$2d$	$\frac{d+\sqrt{n}}{2d}$	1
2	d	1	$d + \sqrt{n}$	$2d$

Justification of a_0, a_1, a_2 as follows.

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

$a_1 = \left[\frac{d+\sqrt{n}}{2d}\right] = \left[\frac{d+[\sqrt{n}]}{2d}\right] = \left[\frac{d+d}{2d}\right] = [1] = 1$.

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

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

8 marks. *Seen similar on exercise sheet.*

(iii) $d = 5$ gives $n = 35$ i.e. $\sqrt{35} = [5, \overline{1, 10}]$.
Using initial values $p_0 = a_0, q_0 = 1, p_1 = a_0a_1 + 1, q_1 = a_1$ 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 $p_k^2 - nq_k^2 = (-1)^{k+1}Q_{k+1}$, we get

k	a_k	p_k	q_k
0	5	5	1
1	1	6	1
2	10	65	11
3	1	71	12
4	10	775	131
5	1	846	143

This gives three solutions: $x = 6, y = 1$ and $x = 71, y = 12$ and $x = 846, y = 143$.

6 marks. *Seen similar on exercise sheet.*

Question 8.

(i) Euler's Criterion: Let p be an odd prime not dividing n. Then $(\frac{n}{p}) \equiv n^{(p-1)/2} \pmod{p}$.

2 marks. *Statement of result from lectures.*

(ii) By (i), $(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} \equiv 1 \pmod{p} \iff 2|(p-1)/2 \iff 4|(p-1) \iff p \equiv 1 \pmod{4}$.

4 marks. *Bookwork from lectures.*

(iii) *Gauss' Law of Quadratic Reciprocity:* Let p, q be two odd primes. If $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$ then $(\frac{p}{q}) = (\frac{q}{p})$. If $p \equiv 3 \pmod{4}$ and $q \equiv 3 \pmod{4}$ then $(\frac{p}{q}) = -(\frac{q}{p})$.

2 marks. *Statement of result from lectures.*

Applying this result, we see $(\frac{5}{p}) = (\frac{p}{5})$ for any odd prime p, since $5 \equiv 1 \pmod 4$. Furthermore, $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1 \pmod 5$, so that the quadratic residues mod 5 are: $0, 1, 4$, that is: $0, 1, -1 \pmod 5$. We can discount $p \equiv 0 \pmod 5$, since then $p = 5$ and $(\frac{p}{5}) = 0$. Hence the values of p for which the legendre symbol equals 1 are precisely $p \equiv \pm 1 \pmod 5$.
4 marks. *Unseen.*

(iv) Let $p_1, p_2, \ldots, p_k$ be primes, all congruent to $-1 \pmod 5$. Let $n = 4(p_1 p_2 \ldots p_k)^2 - 5$. Note that $p_1 p_2 \ldots p_k \equiv (-1)^k \equiv \pm 1 \pmod 5$, so that $n = 4(p_1 p_2 \ldots p_k)^2 - 5 \equiv 4(\pm 1)^2 - 5 \equiv 4 = -1 \pmod 5$. Now, let p be prime and $p|n$. Then $p|4(p_1 p_2 \ldots p_k)^2 - 5$ and so $(2p_1 p_2 \ldots p_k)^2 \equiv 5 \pmod p$, giving that $(\frac{5}{p}) = 1$. Hence $p \equiv \pm 1 \pmod 5$ [by part (iii)]. Finally, note that it is impossible for all prime factors of n to be congruent to $1 \pmod 5$ [since the product of numbers congruent to $1 \pmod 5$ is congruent to $1 \pmod 5$, whereas $n \equiv -1 \pmod 5$]; hence at least one prime p dividing n must satify $p \equiv -1 \pmod 5$. Thus p is a new prime, distinct from $p_1, p_2, \ldots, p_k$, satisfying $p \equiv -1 \pmod 5$ [note that p is distinct from $p_1, p_2, \ldots, p_k$, since, if $p = p_i$ then $p|n = 4(p_1 p_2 \ldots p_k)^2 - 5$ and $p|4(p_1 p_2 \ldots p_k)^2$, implying $p|5$, a contradiction, since $p \equiv -1 \pmod 5$ and so $p \neq 5$]. Imagine there were only finitely many primes congruent to $-1 \pmod 5$, and that $p_1, \ldots, p_k$ lists all of them; the above argument shows the existence of a new such prime p, a contradiction; hence there are infinitely many such primes, as required.
8 marks. *Unseen.*