Solutions to MATH342 (Number Theory) May 2001 examination

Question 1.
$ac - bd = (a-b)c + b(c-d)$ and the r.h.s. is a multiple of n since $n|(a-b), n|(c-d)$; hence so is the l.h.s.
1 mark.

(i) If $k \equiv 1 \pmod 2$, write $k = 2r+1$. First note that $10^2 \equiv 100 \equiv 1 \pmod{11}$. So, $10^k \equiv (10^2)^r \cdot 10 \equiv 10 \equiv -1 \pmod{11}$, so $m = 4 \cdot 10^k + 367 \equiv -4 + 367 = 363 \equiv 0 \pmod{11}$.
3 marks.

(ii) If $k \equiv 1 \pmod 3$, write $k = 3r+1$. First note that $10^3 \equiv 1000 \equiv 1 \pmod{37}$. So, $10^k \equiv (10^3)^r \cdot 10 \equiv 10 \pmod{37}$, and so $m = 4 \cdot 10^k + 367 \equiv 40 + 367 \equiv 407 \equiv 0 \pmod{37}$.
3 marks.

(iii) None of $n_1 = 1, \ldots, 6$ give the required information. Take $n_1 = 7$. If $k \equiv 0 \pmod 6$, write $k = 6r$. First note that $10^6 \equiv (1000)^2 \equiv (-1)^2 \equiv 1 \pmod 7$. So, $10^k \equiv (10^6)^r \equiv 1 \pmod 7$, and so $m = 4 \cdot 10^k + 367 \equiv 4 + 367 \equiv 371 \equiv 0 \pmod 7$.
4 marks.

(iv) None of $n_1 = 1, \ldots, 12$ give the required information. Take $n_2 = 13$. If $k \equiv 2 \pmod 6$, write $k = 6r+2$. First note that $10^6 \equiv (1000)^2 \equiv (-1)^2 \equiv 1 \pmod{13}$. So, $10^k \equiv (10^6)^r \cdot 10^2 \equiv 9 \pmod{13}$, and so $m = 4 \cdot 10^k + 367 \equiv 36 + 367 \equiv 403 \equiv 0 \pmod{13}$.
5 marks.

Collecting together the above information, we see that $m \equiv 0$ modulo at least one of 11,37,7,13 for every: $k \equiv 1 \pmod 2$, $k \equiv 1 \pmod 3$, $k \equiv 0 \pmod 6$, $k \equiv 2 \pmod 6$; that is: $k \equiv 1,3,5 \pmod 6$, $k \equiv 1,4 \pmod 6$, $k \equiv 0 \pmod 6$, $k \equiv 2 \pmod 6$, which covers every possibility mod 6. Hence m is divisible by at least one of 11,37,7,13 for every k. Since $m > 37$ it follows that m is composite.
4 marks. *Whole question: Seen similar on an exercise sheet.*

Question 2.
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: $a^p \equiv a \pmod p$. 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: $b^{m-1} \equiv 1 \pmod m$.
4 marks. *From lectures.*

(i) Any $d|n$ and $d|a$ will satisfy $d|n - (a^{2p-2} + a^{2p-4} + \ldots + a^2) = 1$, so that $(a,n) = 1$. Also, the terms $a^{2p-2}, a^{2p-4}, \ldots, a^2$ will either be all even or all odd (depending on whether a is even or odd), and there are $p-1$ of these terms, which is an even number of terms. Hence, $n - 1 = a^{2p-2} + a^{2p-4} + \ldots + a^2$ is even.
4 marks. *Seen similar in lectures.*

(ii) $a^{2p} - 1 = n(a^2 - 1) \equiv 0 \pmod n$, so that $a^{2p} \equiv 1 \pmod n$.
2 marks. *Seen similar in lectures.*

(iii) $(n-1)(a^2-1) = n(a^2-1) - (a^2-1) = (a^{2p}-1) - (a^2-1) = a^{2p} - a^2 = a^2(a^{2p-2} - 1)$. Since p does not divide a, we have $a^{p-1} \equiv 1 \pmod p$ by Fermat's Theorem, and so $a^{2p-2} \equiv (a^{p-1})^2 \equiv 1 \pmod p$, giving $(n-1)(a^2-1) = a^2(a^{2p-2}-1) \equiv a^2(1-1) \equiv 0 \pmod p$. This is the same as: $p|(n-1)(a^2-1)$; but we know that p does not divide $a^2 - 1$ so that $p|n-1$. From (i) we also know that $2|n-1$; since p is an odd prime, we can combine $p|n-1$ and $2|n-2$ to give $2p|n-1$.
5 marks. *Seen similar in lectures.*

(iv) From (iii), we can write $n-1 = 2pr$, for some integer r, so that $a^{n-1} = (a^{2p})^r \equiv 1^r \equiv 1 \pmod{n}$, by (ii).
2 marks. *Seen similar in lectures.*

(v) Taking $a = 3$, we must choose p to be an odd prime not dividing $a = 3$ or $a^2 - 1 = 8$, the smallest choice being $p = 5$. This gives $n = (3^{10} - 1)/(3^2 - 1) = 7381$. This is divisible by 11, and so composite. Furthermore, (iv) gives that $3^{7380} \equiv 1 \pmod{7381}$, and so 7381 is a pseudoprime to the base 3.
3 marks. *Unseen.*

Question 3. 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.*

For a prime p and $a \geq 1$, the numbers in $1, 2, \ldots, p^a$ which are not coprime to p^a are the multiples of p, namely: $p, 2p, \ldots, p^a$, of which there are $p^a/p = p^{a-1}$ in number. These need to be removed from $1, 2, \ldots, p^a$, leaving $p^a - p^{a-1}$ numbers coprime to p^a. Hence $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$, as required. Writing $n = p_1^{n_1}\ldots p_k^{n_k}$ (prime power factorization),

$$\phi(n) = p_1^{n_1-1}(p-1)\ldots p_k^{n_k-1}(p_k-1).$$

3 marks. *Bookwork from lectures.*

(i) By Euler's Theorem, since $(m, 8) = 1$, we have: $m^{\phi(8)} \equiv 1 \pmod{8}$, where $\phi(8) = 2^2(2-1)$; that is: $m^4 \equiv 1 \pmod{8}$, giving $m^{100} \equiv (m^4)^{25} \equiv 1 \pmod{8}$. Similarly, since $(m, 125) = 1$, we have: $m^{\phi(125)} \equiv 1 \pmod{125}$, where $\phi(125) = 5^2(5-1) = 100$; that is: $m^{100} \equiv 1 \pmod{125}$. Since $(8, 125) = 1$, we can deduce that $m^{100} \equiv 1$ (1000). Since $(37, 10) = (21, 10) = 1$, we can also deduce that $37^{100} - 21^{100} \equiv 1 - 1 \equiv 0 \pmod{1000}$; that is, the last 3 digits of $37^{100} - 21^{100}$ are: 000.
4 marks. *Seen similar in lectures.*

(ii) For $n > 2$, either $n = 2^k$ for $k \geq 2$ or n is divisible by some odd prime p. In the first case, $\phi(n) = 2^{k-1}$, and in the second case, $p - 1 | n$ (using the above formula); in either case, n is even.
3 marks. *Seen on an exercise sheet.*

(iii) If $\phi(n) \equiv 2 \pmod{4}$ then $\phi(n)$ is not divisible by 4. From the above formula, this excludes n being divisible by two distinct odd primes p_1, p_2 (since then $\phi(n)$ would be divisible by $(p_1 - 1)(p_2 - 1)$), and so $n = 2^a p^b$ for odd prime p and some integers $a, b \geq 0$. We cannot have $p \equiv 1 \pmod{4}$ (since then $4|(p-1)|\phi(n)$, using the above formula). We cannot have $a > 2$ (since then $4|2^{a-1}|n$), so that $a = 0, 1, 2$ are the only possibilities. When $b = 0$, so that $n = 2^a$, we see that $\phi(n) = 2^{a-1} \equiv 2 \pmod{4} \iff a = 2 \iff n = 4$. When $b > 0$, then we must not have $p \equiv 1 \pmod{4}$, since then $4|p-1|n$, using the above formula. In this case, $a \neq 2$ (since if $a = 2$ then $\phi(n) = 2^{a-1}p^{b-1}(p-1)$ would be divisible by 4, since $2|2^{a-1}$ and $2|p-1$); when $a = 0, 1$, $\phi(n) = p^{b-1} \equiv 2 \pmod{4}$. In summary, $\phi(n) \equiv 2 \pmod{4}$ if and only if: $n = 4, p^b$ or $2p^b$, where b is a positive integer, and p is a prime $\equiv 3 \pmod{4}$.
4 marks. *Unseen.*

Question 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.

4 marks. *From lectures.*

(i) Base $b = 2$; check $(2, 325) = 1$ so that Miller's test is applicable. Now, $2^{10} = 1024 \equiv 49 \pmod{325}$, so $2^{20} \equiv (2^{10})^2 \equiv 49^2 = 2401 \equiv 126 \pmod{325}$, and $2^{30} \equiv 2^{10} \cdot 2^{20} \equiv 49 \cdot 126 = 6174 \equiv -1 \pmod{325}$, giving: $2^{60} \equiv (2^{30})^2 \equiv (-1)^2 \equiv 1 \pmod{325}$. Now, $2^{324} \equiv (2^{60})^5 \cdot 2^{20} \cdot 2^4 \equiv 1^5 \cdot 126 \cdot 16 \equiv 2016 \equiv 66 \not\equiv 1 \pmod{325}$, and so 325 is neither a pseudoprime nor a strong pseudoprime to base 2, and fails Miller's Test to base 2.

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

(ii) Base $b = 7$; check $(7, 325) = 1$. Now, $7^3 = 343 \equiv 18 \pmod{325}$, so that $7^6 = (7^3)^2 \equiv 18^2 = 324 \equiv -1 \pmod{325}$, and $7^{12} = (7^6)^2 \equiv (-1)^2 \equiv 1 \pmod{325}$. This gives: $7^{324} \equiv (7^{12})^{27} \equiv 1^{27} \equiv 1 \pmod{325}$. Also, $325 = 5^2 \cdot 13$ is composite. Hence 325 is a pseudoprime to base 7. Continuing to Step 2 of Miller's Test: $7^{162} \equiv (7^{12})^{13} \cdot 7^6 \equiv 1^{13} \cdot 324 \pmod{325}$. So 325 passes Miller's Test to base 7, since $324 = 325 - 1$. Hence 325 is a strong pseudoprime to base 7.

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

(iii) Base $b = 24$; check $(24, 325) = 1$. Now, $24^3 = 13824 \equiv 174 \pmod{325}$, and $24^6 = (24^3)^2 \equiv 174^2 = 30276 \equiv 51 \pmod{325}$, and $24^{12} = (24^6)^2 \equiv 51^2 = 2601 \equiv 1 \pmod{325}$. So $24^{324} \equiv (24^{12})^{27} \equiv 1^{27} \equiv 1 \pmod{325}$. Hence 325 is a pseudoprime to base 24. Continuing to Step 2: $24^{162} \equiv (24^{12})^{13} \cdot 24^6 \equiv 1^{13} \cdot 51 \pmod{325}$, so 325 fails Miller's Test to base 24, since 51 is not congruent to 1 or 324 (mod 325). Hence 325 is not a strong pseudoprime to base 24.

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

(iv) Base $b = 126$; check $(126, 325) = 1$. Now, $126^2 = 15876 \equiv 276 \pmod{325}$, and $126^3 = 126 \cdot 126^2 \equiv 126 \cdot 276 \equiv 34776 \equiv 1 \pmod{325}$. This gives: $126^{324} \equiv (126^3)^{108} \equiv 1^{108} \equiv 1 \pmod{325}$. Hence 325 is a pseudoprime to base 126. Continuing to Step 2 of Miller's test: $126^{162} \equiv (126^3)^{54} \equiv 1^{54} \equiv 1 \pmod{325}$. Continuing: $126^{81} \equiv (126^3)^{27} \equiv 1^{27} \equiv 1 \pmod{325}$. Now we stop, since the exponent is odd, with 325 passing Miller's Test to base 126. Hence 325 is a strong pseudoprime to base 126.

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

Question 5. The *order of a mod n* is the smallest integer $k \geq 1$ such that $a^k \equiv 1 \pmod n$. We say that g is a *primitive root mod n* if $\mathrm{ord}_n g = \phi(n)$.

2 marks. *Definitions from lectures.*

(i) First recall the standard results from lectures:

(*) $a^k \equiv 1 \pmod n \iff \mathrm{ord}_n(a) | k$.   (**) $\mathrm{ord}_n(a) | \phi(n)$.

To show that $\mathrm{ord}_p 2 = 2^{k+1}$ we have to show (mod p):

(a) $2^{2^{k+1}} \equiv 1$, (b) If $r < 2^{k+1}$ then $2^r \not\equiv 1$.

For (a), note that $p|F_k$ so $2^{2^k} \equiv -1 \bmod p$. Squaring gives the result required.
For (b), note first that, by (a) and (*), the order of 2 mod p is a *factor* of 2^{k+1}. Hence the order is a power of 2, say: $\text{ord}_p 2 = 2^r$ for some $r, 0 \le r \le k+1$. We want to prove that in fact $r = k+1$ so assume for a contradiction that $r \le k$. Hence $2^{2^r} \equiv 1 \pmod p$ and by squaring this $k - r$ times we will get $2^{2^k} \equiv 1 \bmod p$. But this contradicts the fact that $2^{2^k} \equiv -1 \bmod p$. (Note that p certainly cannot be 2 since F_k is odd.)

The last part, $2^{k+1}|\phi(p) = (p-1)$, follows immediately from the above and (**).

Finally, for $k = 5$, any prime factor $p|F_5$ must therefore satisfy $2^6|p-1$ and so $p \equiv 1 \pmod{64}$. The only possibilities ≤ 100 are $1, 65$, neither of which are prime.
9 marks. *Unseen.*
(ii) Working out powers of 3 mod 17 gives

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^k mod 17	3	–8	–7	–4	5	–2	–6	–1	–3	8	7	4	–5	2	6	1

This verifies that $\text{ord}_{17} 3 = 16 = \phi(17)$, so that 3 is a primitive root mod 17. Then:
$4^x \equiv 8 \pmod{17} \iff 3^{12x} \equiv 3^{10} \pmod{17} \iff 12x \equiv 10 \pmod{16}$,
which has no solution, since $(12, 16) = 4$ which does not divide 10.
For $y^{10} \equiv 2 \pmod{17}$, note that this implies that $(y, 17) = 1$ since any common factor of $y, 17$ would also have to divide and the r.h.s. 2 of the congruence, and so would be a common factor of $2, 17$, which are coprime. Hence we can write y as a power of the primitive root 3; that is: $y \equiv 3^x \pmod{17}$, for some x. Then: $y^{10} \equiv 2 \pmod{17} \iff 3^{10x} \equiv 3^{14} \pmod{17} \iff 10x \equiv 14 \pmod{16} \iff 5x \equiv 7 \pmod 8 \iff x \equiv 3 \pmod 8 \iff x \equiv 3, 11 \pmod{16} \iff y \equiv 3^x \equiv 10, 7 \pmod{17}$. Thus, the two solutions are: $y \equiv 7, 10 \pmod{17}$.
9 marks. *Seen similar on an exercise sheet.*

Question 6. $\sigma(n)$ = 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 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
$n = 31,\ 3 \cdot 7$, that is: $n = 31, 21$ are the only solutions to $\sigma(n) = 32$.
7 marks. *Seen similar on exercise sheet.*

(ii) $\sigma(n) = \sigma(2^s)\sigma(2^{s+1} - 1)$ [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. *Bookwork from lectures.*

(iii) Let n be an even perfect number, and let s be the highest power of 2 dividing n $(s \ge 1)$. That is, $n = 2^s t$, where $s \ge 1$ and t is odd. Then:

$2^{s+1}t = 2n = \sigma(n)$ [since n is perfect] $= \sigma(2^s t) = \sigma(2^s)\sigma(t)$ [since $(2^s, t) = 1$] $= (2^{s+1} - 1)\sigma(t)$.
That is: (*) $2^{s+1}t = (2^{s+1} - 1)\sigma(t)$.
So $2^{s+1} | (2^{s+1} - 1)\sigma(t)$. But $(2^{s+1}, 2^{s+1} - 1) = 1$, so $2^{s+1} | \sigma(t)$, which means that we can write $\sigma(t) = 2^{s+1}q$ for some integer $q \geq 1$. Substituting into (*) gives: $2^{s+1}t = (2^{s+1} - 1)2^{s+1}q$.
That is: (**) $t = (2^{s+1} - 1)q$.
Imagine that $q > 1$. We have from (**) that $q|t$, and that $q \neq t$ [since $s \geq 1$ and so $2^{s+1} - 1 > 1$]. Then $1, q, t$ are all distinct divisors of t, giving: $\sigma(t) \geq 1 + q + t$. But then: $\sigma(t) = 2^{s+1}q = (2^{s+1} - 1)q + q = t + q$ [by (**)], a contradiction.
Hence $q = 1$. So $\sigma(t) = 2^{s+1}q = 2^{s+1} = t + 1$ [since (**) and $q = 1$ give $t = 2^{s+1} - 1$]. Therefore t only has divisors $1, t$ giving that t is prime. In summary, $n = 2^s t = 2^s(2^{s+1} - 1)$, with $t = 2^{s+1} - 1$ prime, as required.
6 marks. *(Harder) Bookwork from lectures.*

Question 7.
(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	$\sqrt{n}$	$d-1$
1	$d-1$	$2d-3$	$\frac{d-1+\sqrt{n}}{2d-3}$	1
2	$d-2$	2	$\frac{d-2+\sqrt{n}}{2}$	$d-2$
3	$d-2$	$2d-3$	$\frac{d-2+\sqrt{n}}{2d-3}$	1
4	$d-1$	1	$d-1+\sqrt{n}$	$2d-2$

Justification of a_0, a_1, a_2 as follows.
$a_0 = [\sqrt{n}]$. But, for all $d \geq 3$:
$(d-1)^2 = d^2 - 2d + 1 = d^2 - 2(d-2) - 3 < d^2 - 2(d-2) - 2 < d^2 - 2$ [since $d - 2 > 0$] $< d^2$, and so $d - 1 < \sqrt{d^2 - 2} < d$, so that $[\sqrt{n}] = d - 1$, i.e. $a_0 = d - 1$.

$$a_1 = \left[\frac{d-1+\sqrt{n}}{2d-3}\right] = \left[\frac{d-1+[\sqrt{n}]}{2d-3}\right] = \left[\frac{2d-2}{2d-3}\right] = 1.$$

$$a_2 = \left[\frac{d-2+\sqrt{n}}{2}\right] = \left[\frac{d-2+[\sqrt{n}]}{2}\right] = \left[\frac{2d-3}{2}\right] = d - 2.$$

$$a_3 = \left[\frac{d-2+\sqrt{n}}{2d-3}\right] = \left[\frac{d-2+[\sqrt{n}]}{2d-3}\right] = \left[\frac{2d-3}{2d-3}\right] = 1.$$

$$a_4 = [d - 1 + \sqrt{n}] = [d - 1 + [\sqrt{n}]] = [2d - 2] = 2d - 2.$$

The fact that $Q_4 = 1$ signals recurrence, so that $\sqrt{n} = [d-1, \overline{1, d-2, 1, 2d-2}]$, as required.
9 marks. *Seen similar on an exercise sheet (although this one is harder).*

(iii) $d = 5$ gives $n = 23$ i.e. $\sqrt{23} = [4, \overline{1, 3, 1, 8}]$. Using $p_0 = a_0, q_0 = 1, p_1 = a_0 a_1 + 1, q_1 = a_1$, 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 $p_k^2 - nq_k^2 = (-1)^{k+1}Q_{k+1}$, we get

k	a_k	p_k	q_k
0	4	4	1
1	1	5	1
2	3	19	4
3	1	24	5

This gives the solution: $x = 24, y = 5$.

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

Question 8.

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

1 mark. *Statement of result from lectures.*

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

3 marks. *Bookwork from lectures.*

(iii) By (i), $(\frac{2}{p}) \equiv 2^{(p-1)/2} \pmod{p}$. Now note that, if $1 \leq r, s \leq (p-1)/2$ and $2r \equiv \pm 2s \pmod{p}$, then $r \equiv \pm s \pmod{p}$ [since $(2,p) = 1$] and so $r = s$. Hence the numbers (*) given by: $2 \cdot 1, 2 \cdot 2, \ldots 2 \cdot (p-1)/2$ have least absolute residues mod p with distinct absolute values. Let (**) be the same list of numbers, except with each number replaced by its least absolute residue mod p, which gives $(p-1)/2$ nonzero numbers of distinct absolute value, and so their absolute values must be $1, 2, \ldots, (p-1)/2$ in some order. Equating the product of (*) with that of (**) mod p, and cancelling $1 \cdot 2 \cdot \ldots \cdot (p-1)/2$, gives that $2^{(p-1)/2} \equiv (-1)^m \pmod{p}$, where m is the number of minus signs in (**), which is the same as the number of members x of (*) in the range $(p-1)/2 < x < p$. Any odd prime $p \equiv \pm 1, \pm 3 \pmod{8}$, and in each case, we need to check whether m is even, in which case $(\frac{2}{p}) = 1$, or m is odd, in which case $(\frac{2}{p}) = -1$.

Case 1. $p \equiv 1 \pmod{8}$, that is $p = 8k+1$ for some k. Then $(p-1)/2 = 4k$, and (*) has precisely the $2k$ numbers $4k+2, 4k+4, \ldots, 8k$ in the range $(p-1)/2 < x < p$. Thus $m = 2k$ is even, and so $(\frac{2}{p}) = 1$.

Case 2. $p \equiv -1 \pmod{8}$, that is $p = 8k - 1$ for some k. Then $(p-1)/2 = 4k-1$, and (*) has precisely the $2k$ numbers $4k, 4k+2, \ldots, 8k-2$ in the range $(p-1)/2 < x < p$. Thus $m = 2k$ is even, and so $(\frac{2}{p}) = 1$.

Case 3. $p \equiv 3 \pmod{8}$, that is $p = 8k+3$ for some k. Then $(p-1)/2 = 4k+1$, and (*) has precisely the $2k+1$ numbers $4k+2, 4k+4, \ldots, 8k+2$ in the range $(p-1)/2 < x < p$. Thus $m = 2k+1$ is odd, and so $(\frac{2}{p}) = -1$.

Case 4. $p \equiv -3 \pmod{8}$, that is $p = 8k-3$ for some k. Then $(p-1)/2 = 4k-2$, and (*) has precisely the $2k-1$ numbers $4k, 4k+2, \ldots, 8k-4$ in the range $(p-1)/2 < x < p$. Thus $m = 2k-1$ is odd, and so $(\frac{2}{p}) = -1$.

8 marks. *Bookwork from lectures.*

(iv) Let $p_1, p_2, \ldots, p_k$ be primes, all congruent to 5 (mod 8). Let $n = (p_1 p_2 \ldots p_k)^2 + 4$. Note that $5^2 = 25 \equiv 1 \pmod{8}$, so that $n = (p_1 p_2 \ldots p_k)^2 + 4 = p_1^2 p_2^2 \ldots p_k^2 + 4 \equiv 1 + 4 = 5 \pmod{8}$. Now, let p be prime and $p|n$. Then $p|(p_1 p_2 \ldots p_k)^2 + 4$ and so $(p_1 p_2 \ldots p_k)^2 \equiv -4 \pmod{8}$, giving that $(\frac{-4}{p}) = 1$. But $(\frac{-4}{p}) = (\frac{-1}{p})(\frac{4}{p})$ and $(\frac{4}{p}) = 1$ [since $4 \equiv 2^2 \pmod{p}$], so that $(\frac{-1}{p}) = 1$. Hence $p \equiv 1 \pmod{4}$ [by part (ii)] which is the same as $p \equiv 1$ or $5 \pmod{8}$. Finally, note that it is impossible for all prime factors of n to be congruent to 1 (mod 8) [since the product of numbers congruent to 1 (mod 8) is congruent to 1 (mod 8), whereas $n \equiv 5 \pmod{8}$]; hence at least one prime p dividing n must satify $p \equiv 5 \pmod{8}$. Thus p is a new prime, distinct from $p_1, p_2, \ldots, p_k$, satisfying $p \equiv 5 \pmod{8}$ [note that p is distinct from $p_1, p_2, \ldots, p_k$, since, if $p = p_i$ then $p|n = (p_1 p_2 \ldots p_k)^2 + 4$ and $p|(p_1 p_2 \ldots p_k)^2$, implying $p|4$, a contradiction, since $p \equiv 5 \pmod{8}$ and so p is odd]. Imagine there were only finitely many primes congruent to 5 (mod 8), 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.*