Solutions to MATH342 (Number Theory) January 2004 examination

Question 1.

(i) Let the integer d be a common divisor of α and β, that is: $d|\alpha$ and $d|\beta$; then $d|(\alpha+k\beta)$ and so d is a common divisor of $\alpha+k\beta$ and β. Conversely, let d be a common divisor of $\alpha+k\beta$ and β. Then $d|(\alpha+k\beta)-k\beta=\alpha$, so that d is a common divisor of α and β. Hence, the set of common divisors of α,β is the same as the set of common divisors of $\alpha+k\beta,\beta$, and so the greatest common divisor is the same in each case; that is: $(\alpha,\beta)=(\alpha+k\beta,\beta)$. The same type of argument shows: $(\alpha,\beta)=(\alpha,\beta+k\alpha)$.

3 marks. *Bookwork from lectures.*

(ii) Repeated applications of part (i) give: $(m^2-3,m^3-2m+2)=(m^2-3,m^3-2m+2-m(m^2-3))$ $=(m^2-3,m+2)=(m^2-3-m(m+2),m+2)=(-2m-3,m+2)=(-2m-3+2(m+2),m+2)$ $=(1,m+2)=1$, since $d=1$ is the only $d>0$ such that $d|1$.

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

Similarly: $(n!+2,(n+1)!+n+2)=(n!+2,(n+1)!+n+2-(n+1)(n!+2))=(n!+2,-n)$ $=(n!+2,n)=(n!+2-(n-1)!n,n)=(2,n)=1$, when n is odd and 2 when n is even. In summary: $(n!+2,(n+1)!+n+2)=1$ or 2, when n is odd or even, respectively.

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

(iii) First solve $4x\equiv 6 \pmod{10}$. Note that $(4,10)=2|6$, so there is a solution. Divide everything throught by 2 to get: $4x\equiv 6 \pmod{10} \iff 2x\equiv 3 \pmod 5$. Multiply both sides by 3 (which is the inverse of 2 modulo 5) to get: $6x\equiv 9 \pmod 5$, that is: $x\equiv 4 \pmod 5$, so that $x=4+5k$, for some integer k. Substitute this into the second congruence to get: $2(4+5k)\equiv 13 \pmod{17}$, so that $10k\equiv 5 \pmod{17}$. We now need to find the inverse of 10 mod 17.

$$\begin{pmatrix}1&0&17\\0&1&10\end{pmatrix}\to\begin{pmatrix}1&-1&7\\0&1&10\end{pmatrix}\to\begin{pmatrix}1&-1&7\\-1&2&3\end{pmatrix}\to\begin{pmatrix}3&-5&1\\-1&2&3\end{pmatrix}\to\begin{pmatrix}3&-5&1\\-10&17&0\end{pmatrix}.$$

The top line of the last matrix tells us: $3\cdot 17+(-5)\cdot 10=1$, so that -5 is an inverse of 10 mod 17. Multiplying both sides of $10k\equiv 5 \pmod{17}$ by -5 gives: $k\equiv -25\equiv 9 \pmod{17}$; that is: $k=9+17\ell$. Substituting this into $x=4+5k$ gives: $x=4+5(9+17\ell)=49+85\ell$, which is the same as: $x\equiv 49 \pmod{85}$.

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

(iv) The first congruence is satisfied by $x=2+(m^2-3)k$, for any integer k. Substituting this into the second equation give: $2+(m^2-3)k\equiv 4 \pmod{m^3-2m+2}$, that is: $(m^2-3)k\equiv 2 \pmod{m^3-2m+2}$. Need first to find inverse of m^2-3 mod m^3-2m+2.

$$\begin{pmatrix}1&0&m^2-3\\0&1&m^3-2m+2\end{pmatrix}\to\begin{pmatrix}1&0&m^2-3\\-m&1&m+2\end{pmatrix}\to\begin{pmatrix}m^2-2m+1&-m+2&1\\-m&1&m+2\end{pmatrix}.$$

The top line of the last matrix tells us: $(m^2-2m+1)(m^2-3)+(-m+2)(m^3-2m+2)=1$, so that m^2-2m+1 is an inverse of m^2-3 modulo m^3-2m+2. Multiplying both sides of $(m^2-3)k\equiv 2 \pmod{m^3-2m+2}$ by m^2-2m+1 gives $k\equiv 2(m^2-2m+1) \pmod{m^3-2m+2}$, that is: $k=2(m^2-2m+1)+(m^3-2m+2)\ell$. Substituting this into $x=2+(m^2-3)k$ gives $x\equiv 2+2(m^2-3)(m^2-2m+1)+(m^2-3)(m^3-2m+2)\ell$, which is the same as: $x\equiv 2(m^4-2m^3-2m^2+6m-2) \pmod{(m^2-3)(m^3-2m+2)}$.

4 marks. *Unseen, and of a new type.*

(v) When n is even, from part (ii), $(n!+2,(n+1)!+n+2)=2$ which is not a factor of 3, so that the first congruence has no solutions. When n is odd, $(2,n+1)=2$, which is not a factor of 5, so that the second congruence has no solutions. In all cases, there is no solution to the simultaneous congruences.

2 marks. *Unseen, and of a new type.*

Question 2.

(i) 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.

5 marks. *Bookwork from lectures.*

Since $51 = 3 \times 17$, we have $\phi(51) = 2 \times 16 = 32$, so that $5^{32} \equiv 1 \pmod{51}$, since $(5, 51) = 1$. Therefore, $2 \cdot 5^{130} \equiv 2 \cdot 5^2 \cdot 5^{128} \equiv 2 \cdot 5^2 \cdot (5^{32})^4 \equiv 2 \cdot 5^2 \cdot 1^4 \equiv 50$, so that $2 \cdot 5^{130} + 1 = 50 + 1 \equiv 0 \pmod{51}$, that is, $51|(2 \cdot 5^{130} + 1)$.

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

(ii) Writing $n = p_1^{n_1} \ldots p_k^{n_k}$ (prime power factorization), $\phi(n) = p_1^{n_1-1}(p_1 - 1)\ldots p_k^{n_k-1}(p_k - 1)$. If $p|n$ then $p = p_i$ for $1 \leq i \leq n$, so that from the formula $(p - 1)|n$.

Here is a table of $\phi(p^a)$ for small values of the prime p and the exponent $a \geq 1$. Since all rows and columns are strictly increasing, any further entries would be greater than 26 and so are irrelevant.

$a\downarrow$ $p\rightarrow$	2	3	5	7	11	13	17	19	23	29
1	1	2	4	6	10	12	16	18	22	28
2	2	6	20	42						
3	4	18	100							
4	8	54								
5	16									
6	32									

Now the following give all the ways of writing 16 as a product of entries in distinct columns of the table: $16 = 16$, corresponding to $n = 17^1$ and $n = 2^5$; $16 = 1 \cdot 16$, corresponding to $n = 2^1 \cdot 17^1$; $16 = 4 \cdot 4$, corresponding to $n = 2^3 \cdot 5^1$; $16 = 8 \cdot 2$, corresponding to $n = 2^4 \cdot 3^1$; $16 = 2 \cdot 2 \cdot 4$, corresponding to $n = 2^2 \cdot 3^1 \cdot 5^1$. So, $n = 17, 32, 34, 40, 48, 60$ are the only n satisfying $\phi(n) = 16$. Finally note that neither 13 nor 26 occur as entries, so that 26 can never be attained as a product of entries; hence there does not exist n for which $\phi(n) = 26$.

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

(iii) Let n be such that $\phi(n)$ is divisible by 2 but not by 4. Then n cannot be divisible by any prime $p \equiv 1 \pmod{4}$, since by part (ii) that would give $4|(p-1)|n$, a contradiction. Similarly, n cannot be divisible by two distinct odd primes p_1, p_2 since then $4|(p_1 - 1)(p_2 - 1)|n$. So, n can only be of the form $n = 2^r p^a$ for some $r, a \geq 0$ and some $p \equiv 3 \pmod{4}$. If $r \geq 3$ or ($r = 2$ and $a > 0$) then $4|2^{r-1}|\phi(n)$ or $4|2^{r-1}(p-1)|\phi(n)$, respectively, a contradiction in either case. Therefore ($r = 2$ and $a = 0$) or ($r = 0, 1$ and $a > 0$) are the only possibilities; that is, $n = 4, p^a$ or $2p^a$, for some $a > 0$. Indeed in these cases, $\phi(4) = 2$ and $\phi(n) = (p-1)p^{a-1}$, which is divisible by 2 but not by 4 (since $p \equiv 3 \pmod{4}$), as required. Finally, note that if $\phi(n) = 2 \times 5^{130}$ then $n = 4, p^a$ or $2p^a$ for some $a > 0$ and prime $p \equiv 3 \pmod{4}$; we can exclude $n = 4$ since $\phi(4) = 2 \neq 2 \times 5^{130}$, and so $n = p^a$ or $2p^a$, giving $\phi(n) = (p-1)p^{a-1}$. If $a = 1$ then this would mean $p - 1 = 2 \times 5^{130}$, a contradiction, since we have already seen in part (i) that $2 \times 5^{130} + 1$ is divisible by 51 and so is not prime. If $a > 1$ then $(p-1)p^{a-1} = 2 \times 5^{130}$, so that $p = 5$, but then only the left hand side would be divisible by 4, a contradiction.

4 marks. *Unseen.*

Question 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 $n = q_1 \dots q_k$ 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.
7 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) Note that $(p-1)|(p-1)$ so that $p \equiv 1 \pmod{p-1}$. We are given that $(p-1)|(qr-1)$ and so $qr \equiv 1 \pmod{p-1}$. Multiplying these equations gives: $pqr \equiv 1 \pmod{p-1}$, and so: $(p-1)|(pqr-1) = (n-1)$. Similarly, $(q-1)|(pr-1)$ gives that $(q-1)|(n-1)$. Similarly $(r-1)|(pq-1)$ gives that $(r-1)|(n-1)$. Hence n satisfies the conditions of (i) and so is a Carmichael number. Letting $p = 601, q = 1201, r = 1801$, we see that $(qr-1)/(p-1) = 2163000/600 = 3605$, so that $(p-1)|(qr-1)$. Similarly, $(pr-1)/(q-1) = 1082400/1200 = 902$, so that $(q-1)|(pr-1)$. Similarly, $(pq-1)/(r-1) = 721800/1800 = 401$, so that $(r-1)|(pq-1)$. Hence n is a Carmichael number (alternatively, use (ii) with $p = 601, 2p-1 = 1201, 3p-2 = 1801$ all prime).
5 marks. *Unseen.*

Question 4. 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 $2 \nmid m$ 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.

(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 that $\sigma(p^a) = 1 + p + p^2 + \ldots p^a = (p^{a+1} - 1)/(p-1)$.

Writing $n = p_1^{n_1} \ldots p_k^{n_k}$, we have: $\sigma(n) = \frac{p_1^{n_1+1}-1}{p_1-1} \ldots \frac{p_k^{n_k+1}-1}{p_k-1}$.

3 marks. *From lectures.*

If p is odd and a is odd, then each term of $1 + p + p^2 + \ldots + p^a$ is odd, and there is an even number $(a+1)$ of terms, so that the sum is even. If p is odd and a is even, then each term of $1 + p + p^2 + \ldots + p^a$ is again odd, but now there is an odd number $(a+1)$ of terms, so that the sum is odd.

2 marks. *Unseen.*

(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.
The first three such numbers are: $6 = 2^1 \times (2^2-1), 28 = 2^2 \times (2^3-1)$ and $496 = 2^4 \times (2^5-1)$.

4 marks. *Bookwork from lectures.*

(iii) 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. Hence $\sigma(n) \neq 2n$ so that n is not perfect.

7 marks. *Seen similar on exercise sheet.*

(iv) Assume that n is perfect, so that $\sigma(n) = 2n$.
Imagine 3 were not a factor of n then the smallest possible values for $p_1, p_2, p_3, p_4, p_5, p_6$ would be $5, 7, 11, 13, 17, 19$, so that, as in part (iii), $\frac{\sigma(p_1^{n_1})}{p_1^{n_1}}, \frac{\sigma(p_2^{n_2})}{p_2^{n_2}}, \frac{\sigma(p_3^{n_3})}{p_3^{n_3}}, \frac{\sigma(p_4^{n_4})}{p_4^{n_4}}, \frac{\sigma(p_5^{n_5})}{p_5^{n_5}}, \frac{\sigma(p_6^{n_6})}{p_6^{n_6}}$ would be, respectively, less than $\frac{5}{5-1}, \frac{7}{7-1}, \frac{11}{11-1}, \frac{13}{13-1}, \frac{17}{17-1}, \frac{19}{19-1}$. Hence,

$$\frac{\sigma(n)}{n} = \frac{\sigma(p_1^{n_1})\sigma(p_2^{n_2})\sigma(p_3^{n_3})\sigma(p_4^{n_4})\sigma(p_5^{n_5})\sigma(p_6^{n_6})}{p_1^{n_1}p_2^{n_2}p_3^{n_3}p_4^{n_4}p_5^{n_5}p_6^{n_6}} < \frac{5}{4}\frac{7}{6}\frac{11}{10}\frac{13}{12}\frac{17}{16}\frac{19}{18} = \frac{1616615}{829440} < 2,$$

so that $\sigma(n) \neq 2n$ so that n would not be perfect, a contradiction.
Hence $3|n$, as required.

Also, $\sigma(n) = 2n$ gives $\sigma(p_1^{n_1})\sigma(p_2^{n_2})\sigma(p_3^{n_3})\sigma(p_4^{n_4})\sigma(p_5^{n_5})\sigma(p_6^{n_6}) = 2p_1^{n_1}p_2^{n_2}p_3^{n_3}p_4^{n_4}p_5^{n_5}p_6^{n_6}$. Note that the right hand side is divisible by 2, but not by 4 (since $p_1, \ldots, p_6$ are all odd), so that precisely one factor of the left hand side is even; but by the last part of (i), this is the same as saying that precisely one of $n_1, \ldots, n_6$ is odd.

4 marks. *Unseen.*

Question 6.

(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.

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.*

(ii) Check: $(6, 217) = 1$, so that Miller's Test can be applied on 217 to base 6. First compute: $6^3 \equiv 216 \equiv -1 \pmod{217}$. This gives, $6^{217-1} \equiv 6^{216} \equiv (6^3)^{72} \equiv (-1)^{72} \equiv 1$, so that 217 is a pseudoprime to the base 6 (given that $217 = 7 \cdot 31$ and so is composite). The exponent 216 is even, so we continue to compute $6^{108} \equiv (6^3)^{36} \equiv (-1)^{36} \equiv 1$. The exponent 108 is still even, so we continue to compute $6^{54} \equiv (6^3)^{18} \equiv (-1)^{18} \equiv 1$, and then $6^{27} \equiv (6^3)^9 \equiv (-1)^9 \equiv -1 \equiv 216$. We stop, since the exponent is odd, and see that the result is indeed 1 or $217 - 1$, with 217 passing Miller's test to base 6. Thus, 217 is a strong pseudoprime to base 6.

Check: $(8, 65) = 1$, so that Miller's Test can be applied on 65 to base 8. First compute: $8^2 \equiv 64 \equiv -1 \pmod{65}$. This gives, $8^{65-1} \equiv 8^{64} \equiv (8^2)^{32} \equiv (-1)^{32} \equiv 1$, so that 65 is a pseudoprime to the base 8 (given that $65 = 5 \cdot 13$ and so is composite). The exponent 64 is even, so we continue to compute $8^{32} \equiv (8^2)^{16} \equiv (-1)^{16} \equiv 1$. The exponent 32 is even, so we continue to compute $8^{16} \equiv (8^2)^8 \equiv (-1)^8 \equiv 1$. The exponent 16 is even, so we continue to compute $8^8 \equiv (8^2)^4 \equiv (-1)^4 \equiv 1$. The exponent 8 is even, so we continue to compute $8^4 \equiv (8^2)^2 \equiv (-1)^2 \equiv 1$. The exponent 4 is even, so we continue to compute $8^2 \equiv -1 \equiv 64 \pmod{65}$. The residue is no longer 1, and so we stop. We see that the last residue is 1 or $65 - 1$, so that 65 passes Miller's Test to base 8. Thus, 65 is a strong pseudoprime to base 8.

Check: $(2, 129) = 1$, so that Miller's Test can be applied on 129 to base 2. First compute: $2^7 \equiv 128 \equiv -1 \pmod{129}$, so that $2^{129-1} \equiv 2^{128} \equiv 2^{126} \cdot 2^2 \equiv (2^7)^{18} \cdot 2^2 \equiv (-1)^{18} \cdot 4 \equiv 4 \pmod{129}$, giving that 129 is not a pseudoprime to base 2. Miller's Test is immediately failed at Step 1, so that 129 is not a strong pseudoprime to base 2.

7 marks. *Seen similar on exercise sheet.*

(iv) First note that from $n = 2^{2^k} + 1$ we get $2^{2^k} + 1 \equiv 0 \pmod{n}$ and so $2^{2^k} \equiv -1 \pmod{n}$. Since $k \geq 1$, we have that $2^k > k$ and so let $\ell = 2^k - k > 0$. Then $2^{n-1} = 2^{2^{2^k}} = 2^{2^{k+\ell}} = 2^{2^k 2^\ell} = (2^{2^k})^{2^\ell} \equiv (-1)^{2^\ell} \equiv 1 \pmod{n}$, so that n passes Step 1 of Miller's Test. The exponent is even, so we continue to halve the exponent to get: $(2^{2^k})^{2^{\ell-1}} \equiv (-1)^{2^{\ell-1}} \equiv 1, (2^{2^k})^{2^{\ell-2}} \equiv (-1)^{2^{\ell-2}} \equiv 1, \ldots$, until we get: $(2^{2^k})^{2^0} \equiv (-1)^{2^0} = -1 \equiv n-1 \pmod{n}$. The residue is no longer 1, and so we stop. We see that the last residue is 1 or $n-1$, so that n passes Miller's Test to base 2.

4 marks. *Unseen.*

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	$\sqrt{n}$	$3d$
1	$3d$	$6d$	$\frac{3d+\sqrt{n}}{6d}$	1
2	$3d$	1	$3d + \sqrt{n}$	$6d$

Justification of a_0, a_1, a_2 as follows.

$a_0 = [\sqrt{n}]$. But, for all $d \geq 1$, $(3d)^2 = 9d^2 < 9d^2 + 6d < 9d^2 + 6d + 1 = (3d + 1)^2$ and so $3d < \sqrt{9d^2 + 6d} < 3d + 1$, so that $[\sqrt{n}] = 3d$, i.e. $a_0 = 3d$.

$a_1 = \left[\frac{3d+\sqrt{n}}{6d}\right] = \left[\frac{3d+[\sqrt{n}]}{6d}\right] = \left[\frac{3d+3d}{6d}\right] = [1] = 1$.

$a_2 = [3d + \sqrt{n}] = [3d + [\sqrt{n}]] = [3d + 3d] = [6d] = 6d$.

The fact that $Q_2 = 1$ signals recurrence, so that $\sqrt{n} = [3d, \overline{1, 6d}]$, as required.

8 marks. *Seen similar on exercise sheet.*

(iii) $d = 2$ gives $n = 48$ i.e. $\sqrt{48} = [6, \overline{1, 12}]$.
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	6	6	1
1	1	7	1
2	12	90	13
3	1	97	14
4	12	1254	181
5	1	1351	195

This gives three solutions: $x = 7, y = 1$ and $x = 97, y = 14$ and $x = 1351, y = 195$.

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.*

$(\frac{-19}{193}) = (\frac{-1}{193})(\frac{19}{193}) = (\frac{19}{193})$ [by (ii) since $193 \equiv 1 \pmod{4}$]
$= (\frac{193}{19})$ [by QR, since $193 \equiv 1 \pmod{4}$]
$= (\frac{3}{19}) = -(\frac{19}{3})$ [by QR, since 19 and 3 are both $\equiv 3 \pmod{4}$].
$= -(\frac{1}{3}) = -1$ [since $1 \equiv 1^2 \pmod{3}$, so that $(\frac{1}{3}) = 1$].

Note that, $0^2, 1^2, 2^2$ are $0, 1, 1$ mod 3, so that $0, 1$ are quadratic residues mod 3 but 2 is not. We then have $(\frac{1}{3}) = 1$ and $(\frac{2}{3}) = -1$. For $p = 3$ we have $(\frac{p}{3}) \neq 1$. We are given that p is odd, so we do not need to consider $p = 2$. All primes $p \neq 2, 3$ are coprime to 12 and so satisfy $p \equiv 1, 5, 7$ or $11 \pmod{12}$.
When $p \equiv 1 \pmod{12}$, we have $p \equiv 1 \pmod{3}$ and $p \equiv 1 \pmod{4}$, so that
$(\frac{3}{p}) = (\frac{p}{3})$ [by QR, since $p \equiv 1 \pmod{4}$] $= (\frac{1}{3}) = 1$.
When $p \equiv 5 \pmod{12}$, we have $p \equiv 2 \pmod{3}$ and $p \equiv 1 \pmod{4}$, so that
$(\frac{3}{p}) = (\frac{p}{3})$ [by QR, since $p \equiv 1 \pmod{4}$] $= (\frac{2}{3}) = -1$.
When $p \equiv 7 \pmod{12}$, we have $p \equiv 1 \pmod{3}$ and $p \equiv 3 \pmod{4}$, so that
$(\frac{3}{p}) = -(\frac{p}{3})$ [by QR, since p and 3 are both $\equiv 3 \pmod{4}$] $= -(\frac{1}{3}) = -1$.
When $p \equiv 11 \pmod{12}$, we have $p \equiv 2 \pmod{3}$ and $p \equiv 3 \pmod{4}$, so that
$(\frac{3}{p}) = -(\frac{p}{3})$ [by QR, since p and 3 are both $\equiv 3 \pmod{4}$] $= -(\frac{2}{3}) = -(-1) = 1$.
So, in summary, we have that $(\frac{3}{p}) = 1$ iff $p \equiv \pm 1 \pmod{12}$, as required.
5 marks. *Unseen.*

(iv) Let $p_1, p_2, \ldots, p_k$ be primes, all congruent to $-1 \pmod{12}$. Let $n = 3(2p_1p_2 \ldots p_k)^2 - 1$. Note that $n = 12(p_1p_2 \ldots p_k)^2 - 1 \equiv -1 \pmod{12}$. Now, let p be prime and $p|n$. Then $p|3(2p_1p_2 \ldots p_k)^2 - 1$ and so $3(2p_1p_2 \ldots p_k)^2 \equiv 1 \pmod{\text{p}}$. But p is not a factor of $2p_1p_2 \ldots p_k$ (since if $p|2p_1p_2 \ldots p_k$, then the fact that $p|n$ would also give $p|n - 3(2p_1p_2 \ldots p_k)^2 = -1$, that is: $p|(-1)$, a contradiction) giving that $2p_1p_2 \ldots p_k$ has an inverse $\alpha \bmod p$. Multiplying both sides of $3(2p_1p_2 \ldots p_k)^2 \equiv 1 \pmod{\text{p}}$ by α^2 gives $3 \equiv \alpha^2 \pmod{\text{p}}$, and so $(\frac{3}{p}) = 1$. Hence $p \equiv \pm 1 \pmod{12}$ [by part (iii)]. Finally, note that it is impossible for all prime factors of n to be congruent to 1 (mod 12) [since the product of numbers congruent to 1 (mod 12) is congruent to 1 (mod 12), whereas $n \equiv -1 \pmod{12}$]; hence at least one prime p dividing n must satify $p \equiv -1 \pmod{12}$. Thus p is a new prime, distinct from $p_1, p_2, \ldots, p_k$, satisfying $p \equiv -1 \pmod{12}$ [note that p is distinct from $p_1, p_2, \ldots, p_k$, since, if $p = p_i$ then $p|n = 12(p_1p_2 \ldots p_k)^2 - 1$ and $p|12(p_1p_2 \ldots p_k)^2$, implying $p|(-1)$, a contradiction]. Imagine there were only finitely many primes congruent to $-1 \pmod{12}$, 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.
7 marks. *Unseen, but broadly similar in strategy to a problem on an exercise sheet.*