Solutions to MATH342 (Number Theory) May 2000 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: $(\alpha, \beta) = (\alpha, \beta + k\alpha)$.
4 marks. *Bookwork from lectures.*

(ii) Repeated applications of part (i) give: $(x^3 - 2, x^2 + 1) = (x^3 - 2 - x(x^2 + 1), x^2 + 1)$ $= (-x-2, x^2+1) = (-x-2, x^2+1+x(-x-2)) = (-x-2, -2x+1) = (-x-2, -2x+1-2(-x-2))$ $= (-x-2, 5) = (x+2, 5)$, which is 5 when $5|(x+2)$ and is 1 otherwise. Hence: $(x^3-2, x^2+1) = 5$ when $x \equiv 3 \pmod 5$ and $(x^3 - 2, x^2 + 1) = 1$ otherwise.
4 marks. *Seen similar on an exercise sheet.*

(iii) On dividing $x^n - 1$ by $x - 1$ we get the standard equation: $x^n - 1 = (x - 1)f(x)$ where $f(x) = x^{n-1} + x^{n-2} + x^{n-3} + \ldots + 1$. Clearly $f(x)$ is an integer (since x is an integer) and so $(x^n - 1)/(x - 1) = f(x)$ is an integer.

Dividing the polynomial $f(x) = x^{n-1} + x^{n-2} + x^{n-3} + \ldots + 1$, found above, by $x - 1$ gives $(x^n - 1)/(x - 1) = (x - 1)g(x) + n$, where $g(x) = x^{n-2} + 2x^{n-3} + 3x^{n-4} + \ldots + (n - 1)$. Hence, by part (i), $((x^n - 1)/(x - 1), x - 1) = ((x^n - 1)/(x - 1) - (x - 1)g(x), x - 1) = (n, x - 1)$.
5 marks. *Unseen.*

(iv) Replacing x by n^b and n by q in the equation $x^n - 1 = (x - 1)f(x)$ of part (iii) gives:

$$(n^b)^q - 1 = (n^b - 1)((n^b)^{q-1} + (n^b)^{q-2} + \ldots + 1).$$

Multiplying both sides by n^r and then adding $n^r - 1$ to both sides gives

$$n^{bq+r} - 1 = (n^b - 1)(n^{b(q-1)+r} + n^{b(q-2)+r} + \ldots + n^r) + (n^r - 1).$$

Since $a = bq + r$, this is of the form $A = BQ + R$, where $Q = n^{b(q-1)+r} + n^{b(q-2)+r} + \ldots + n^r$. It follows that $(A, B) = (A - BQ, B) = (R, B)$, and that the first step of Euclid's Algorithm for finding (A, B) is identical to that for finding (a, b), but with a, b, r replaced by $A = n^a - 1, B = n^b - 1, R = n^r - 1$. Repeatedly applying the same argument shows that the same must be true of all subsequent steps of Euclid's Algorithm, and so the final nonzero remainders: (a, b) and (A, B) are related in the same way, that is: $(A, B) = n^{(a,b)} - 1$, as required. We can therefore compute $(3^{87} - 1, 3^{69} - 1) = 3^{(87,69)} - 1 = 3^3 - 1 = 26$.
7 marks. *Seen similar in lectures.*

Question 2.

(i) $x^2 \equiv x \pmod{216} \Rightarrow 216 \mid (x^2 - x) \Rightarrow 8 \mid 216 \mid (x^2 - x)$ and $27 \mid 216 \mid (x^2 - x)$
$\Rightarrow x^2 \equiv x \pmod 8$ and $x^2 \equiv x \pmod{27}$.

The arrows in the above argument can be reverse (giving the required $\iff$) by using the facts that $216 = 8 \times 27$, where $(8, 27) = 1$, and the standard fact that:

$$m \mid a,\ n \mid a,\ (m, n) = 1 \Rightarrow mn \mid a. \qquad (*)$$

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

Now use the standard fact, for any prime p and any a, b with $(a, b) = 1$, that: $p^r|ab \iff p^r|a$ or $p^r|b$. Since $(x, x-1) = 1$, this gives: $x^2 \equiv x \pmod 8 \iff 2^3 \mid (x^2 - x) \iff 2^3 \mid x(x-1) \iff 2^3 \mid x$ or $2^3 \mid (x-1) \iff x \equiv 0$ or $1 \pmod 8$.

Similarly, $x^2 \equiv x \pmod{27} \iff x \equiv 0$ or $1 \pmod{27}$. Therefore:

$$x^2 \equiv x \pmod{216} \iff (x \equiv 0 \text{ or } 1 \pmod 8) \text{ and } (x \equiv 0 \text{ or } 1 (\text{mod } 27)).$$

(a) $x \equiv 0 \pmod 8$ and $x \equiv 0 \pmod{27}$. Then $x \equiv 0 \pmod{216}$ by (*).

(b) $x \equiv 1 \pmod 8$ and $x \equiv 1 \pmod{27}$. Then $x \equiv 1 \pmod{216}$ by (*).

(c) $x \equiv 0 \pmod 8$ and $x \equiv 1 \pmod{27}$. Then $x = 8k$ and $8k \equiv 1 \pmod{27}$. The inverse of 8 is 17 (mod 27), since $8 \times 17 = 136 \equiv 1 \pmod{27}$ [found either by Euclid's Algorithm or trial and error]. Multiplying both sides of the congruence by 17 gives: $k \equiv 17 \pmod{27}$, and so $x = 8k \equiv 136 \pmod{216}$.

(d) $x \equiv 1 \pmod 8$ and $x \equiv 0 \pmod{27}$. Then $x = 27k$ and $27k \equiv 1 \pmod 8$, that is: $3k \equiv 1 \pmod 8$, since $27 \equiv 3 \pmod 8$. The inverse of 3 is 3 (mod 8), since $3 \times 3 = 9 \equiv 1 \pmod 8$ [found either by Euclid's Algorithm or trial and error]. Multiplying both sides of the congruence by 3 gives: $k \equiv 3 \pmod{27}$, and so $x = 27k \equiv 81 \pmod{216}$.

Thus, the solution to the congruence is: $x \equiv 0, 1, 81, 136 \pmod{216}$.

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

(ii) 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 $i \ne j$ (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 $i \ne j$, $1 \le i, j \le (p-1)$. 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.*

Suppose $n^2 \equiv -1 \pmod 7$. Then $7\not|\, n$ [since if $7|\, n$ then the LHS would be $0 \pmod 7$]. Cubing both sides gives: $n^6 \equiv -1 \pmod 7$. But, by Fermat's Theorem, $n^6 \equiv 1 \pmod 7$ since $7\not|\, n$. Hence $n^2 \equiv -1 \pmod 7$ is impossible, since $-1 \not\equiv 1 \pmod 7$.
3 marks. *Unseen.*

If $p = 8\ell + 5$ and $n^4 \equiv -1 \pmod p$ then $p\not|\, n$ [since if $p|\, n$ then the LHS would be $0 \pmod p$]. Taking both sides to the power of $(2\ell + 1)$ gives: $(n^4)^{(2\ell+1)} \equiv -1 \pmod p$, that is: $n^{p-1} \equiv -1 \pmod p$. But, by Fermat's Theorem, $n^{p-1} \equiv 1 \pmod p$, since $p\not|\, n$. Hence $n^4 \equiv -1 \pmod p$ is impossible, since $-1 \not\equiv 1 \pmod p$ [since $p \neq 2$]. That is: $p\not|\,(n^4 + 1)$, as required.
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 $(x, n) = 1$. 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.*

(i) 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 20 and so are irrelevant.

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

Now the following give all the ways of writing 20 as a product of entries in distinct columns of the table: $20 = 20$, corresponding to $n = 5^2$; $20 = 1 \cdot 20$, corresponding to $n = 2^1 \cdot 5^2$; $20 = 2 \cdot 10$, corresponding to $n = 3^1 \cdot 11^1$ or $n = 2^2 \cdot 11^1$; $20 = 1 \cdot 2 \cdot 10$, corresponding to $n = 2^1 \cdot 3^1 \cdot 11^1$ (note that 4 never occurs as an entry, so that $20 = 4 \cdot 5$ is not available). So, $n = 25, 33, 44, 50, 66$ are the only n satisfying $\phi(n) = 20$. Finally note that neither 7 nor 14 occur as entries, so that 14 can never be attained as a product of entries; hence there does not exist n for which $\phi(n) = 14$.
9 marks. *Seen similar on an exercise sheet.*

(ii) For $p \equiv -1 \pmod{12}$ and a even, $\phi(p^a) = p^{a-1}(p-1) \equiv (-1)^{a-1}(-2) \equiv (-1)(-2) \equiv 2 \pmod{12}$.
2 marks. *Unseen.*

(iii) Let $p > 3$ be prime and let $b \geq 3$ be odd. Then p is not divisible by $2, 3$ and so we can eliminate $0, 2, 3, 4, 6, 8, 9, 10$ from $0, 1, \ldots, 11$, leaving $1, 5, 7, 11$ as the only possible numbers congruent to $p \pmod{12}$; that is: $\pm 1, \pm 5 \pmod{12}$.

$p \equiv 1 \pmod{12} \Rightarrow \phi(p^b) = p^{b-1}(p-1) \equiv 1^{b-1} \cdot 0 \equiv 0 \not\equiv 2 \pmod{12}$.

$p \equiv -1 \pmod{12} \Rightarrow \phi(p^b) = p^{b-1}(p-1) \equiv (-1)^{b-1} \cdot (-2) \equiv 1 \cdot (-2)$ [since $b-1$ is even] $\not\equiv 2 \pmod{12}$.

$p \equiv 5 \pmod{12} \Rightarrow \phi(p^b) = p^{b-1}(p-1) \equiv 5^{b-1} \cdot 4 \not\equiv 2 \pmod{12}$ [since $(5^{b-1} \cdot 4, 12) = 4 \not| \, 2$].

$p \equiv -5 \pmod{12} \Rightarrow \phi(p^b) = p^{b-1}(p-1) \equiv (-5)^{b-1} \cdot (-6) \not\equiv 2 \pmod{12}$ [since $((-5)^{b-1} \cdot (-6), 12) = 6 \not| \, 2$].

6 marks. *Unseen.*

Question 4.

(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.*

(a) Base $b = 2$; check $(2, 85) = 1$ so that Miller's test is applicable. Now, $2^8 = 256 \equiv 1 \pmod{85}$, so $2^{84} \equiv (2^8)^{10} \times 2^4 \equiv 1^{44} \times 16 \equiv 16 \pmod{85}$. Thus, 85 fails Miller's test to base 2 at Step 1, and so 85 is a not even a pseudoprime to base 2.

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

(b) Base $b = 4$; check $(4, 85) = 1$ so that Miller's test is applicable. Now, $4^4 \equiv 2^8 \equiv 1 \pmod{85}$, so $4^{84} \equiv (4^4)^{21} \equiv 1^{21} \equiv 1 \pmod{85}$. Thus, 85 passes Step 1 of Miller's test, and so 85 is a pseudoprime to base 4. Moving onto Step 2, compute $4^{42} \equiv 2^{84} \equiv 16 \pmod{85}$, which is neither 1 nor $85 - 1 \pmod{85}$, and so 85 fails Miller's test to base 4. Thus 85 is a not a strong pseudoprime to base 4.

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

(c) Base $b = 13$; check $(13, 85) = 1$ so that Miller's test is applicable. Now, $13^2 = 169 \equiv -1 \pmod{85}$, so $13^{84} \equiv (13^2)^{42} \equiv (-1)^{42} \equiv 1 \pmod{85}$. Thus, 85 passes Step 1 of Miller's test, and so 85 is a pseudoprime to base 13. Moving onto Step 2, compute $13^{42} \equiv (13^2)^{21} \equiv (-1)^{21} \equiv -1 \pmod{85}$. Thus, 85 passes Miller's test to base 13, and so 85 is a a strong pseudoprime to base 4.

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

(ii) $n - 1 \equiv 0 - 1 \equiv -1 \pmod{n}$, so that $(n-1)^{n-1} \equiv (-1)^{n-1} \equiv 1 \pmod{n}$, since $n - 1$ is even, which means that n passes Step 1 of Miller's test to base $n - 1$. Subsequent steps replace the exponent $n - 1$ by $(n-1)/2, (n-1)/4, \ldots$ which, when even, continue to give $\pmod{n}$:

$$(n-1)^{(n-1)/2}, (n-1)^{(n-1)/4}, \ldots \equiv (-1)^{(n-1)/2}, (-1)^{(n-1)/4}, \ldots,$$

all of which are congruent to $1 \pmod{n}$, until one gets to $(n-1)/2^k$ odd, when $(n-1)^{(n-1)/2^k} \equiv (-1)^{(n-1)/2^k} \equiv -1 \pmod{n}$. At this point, Miller's test terminates, with n passing Miller's test to base $n - 1$.

3 marks. *Unseen.*

(iii) First note that $m^m \equiv -1 \pmod{n}$. So, $m^{n-1} = m^{(m^m)} = m^{m(m^{m-1})} = (m^m)^{(m^{m-1})} \equiv (-1)^{(m^{m-1})} \equiv 1 \pmod{n}$, since m^{m-1} is even, which means that n passes Step 1 of Miller's test to base m. Subsequent steps replace the exponent $n-1$ by $(n-1)/2, (n-1)/4, \ldots$ which, when $(m^{m-1})/2, (m^{m-1})/4, \ldots$ is even, continue to give (mod n):

$$m^{(n-1)/2}, m^{(n-1)/4}, \ldots \equiv m^{(m^m)/2}, m^{(m^m)/4}, \ldots \equiv m^{m(m^{m-1})/2}, m^{m(m^{m-1})/4}, \ldots$$
$$= (m^m)^{(m^{m-1})/2}, (m^m)^{(m^{m-1})/4}, \ldots \equiv (-1)^{(m^{m-1})/2}, (-1)^{(m^{m-1})/4}, \ldots,$$

all of which are congruent to 1 (mod n), until one gets to $(m^{m-1})/2^k$ odd, when $m^{(n-1)/2^k} \equiv (-1)^{(m^{m-1})/2^k} \equiv -1 \pmod{n}$. At this point, Miller's test terminates, with n passing Miller's test to base m.

4 marks. *Unseen.*

Question 5. 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 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 6.

(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 $\sigma(p^a) = 1 + p + p^2 + \ldots p^a$. There are $a + 1$ terms in this sum. If $\sigma(p^a)$ is odd and $p \neq 2$, then p is odd, and so each term in the sum is odd; since the whole sum is odd, it follows that the number of terms, $a + 1$, is odd, and so a is even.

Writing $n = p_1^{n_1} \ldots p_k^{n_k}$ (prime power factorization),

$$\sigma(n) = (1 + p_1 + p_1^2 + \ldots p_1^{n_1}) \ldots (1 + p_k + p_k^2 + \ldots p_k^{n_k}).$$

If $\sigma(n)$ is odd, then each of the above factors is odd; we have already shown that this implies n_i is even for all $p_i \neq 2$. If also the power of 2 is even then n is a square (since then all power would be even), otherwise n is twice a square.

8 marks. *From lectures.*

(ii) Let n be an even perfect number (where n is *perfect* means $\sigma(n) = 2n$). Recall the result from lectures that any even perfect number n is of the form $n = 2^s(2^{s+1} - 1)$ with $2^{s+1} - 1$ a prime number. First note that if $s + 1$ were composite, $s + 1 = ab$, say, with $a > 1, b > 1$, then $2^{s+1} - 1 = 2^{ab} - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \ldots + 1)$, contradicting the fact that $2^{s+1} - 1$ a prime number. Hence $s + 1$ is prime, and so $s + 1 = 2$ or $s + 1$ is odd. In the first case, $n = 6$ and so the result is true. In the second case (where $s + 1$ is odd and so s is even), consider the integer $n/2$. First note that $2^1, 2^2, 2^3, 2^4$ are, respectively $2, 4, 3, 1 \pmod 5$, and so $2^{4k} \equiv (2^4)^k \equiv 1^k \equiv 1 \pmod 5$ for any k, and similarly $2^{4k+1} \equiv 2 \pmod 5$, $2^{4k+2} \equiv 4 \pmod 5$ and $2^{4k+3} \equiv 3 \pmod 5$. Now, $n/2 = 2^{s-1}(2^{s+1} - 1) = 2^{2s} - 2^{s-1}$. But 2^{2s} is 2 to the power of a multiple of 4 (since s is even) and so $2^{2s} \equiv 1 \pmod 5$; also 2^{s-1} is 2 to an odd power and so $2^{s-1} \equiv 2$ or $3 \pmod 5$. Thus, $n/2 = 2^{2s} - 2^{s-1} \equiv 1 - (2 \text{ or } 3) \equiv (4 \text{ or } 3) \pmod 5$. Multiplying everything (including the modulus) through by 2 gives: $n \equiv 8$ or $6 \pmod{10}$, as required.

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

(iii) We have already seen in (ii) that $n = 2^s(2^{s+1} - 1)$ with $2^{s+1} - 1$ a prime number, and that indeed $s + 1$ a prime number, so that $s + 1 = 2$ or $s + 1$ is odd. When $n > 6$ we have $s + 1 > 2$ and so $s + 1$ must be odd and s must be even, $s = 2r$, say. Then $n = 2^s(2^{s+1} - 1) = k^2(2k^2 - 1)$, with $k = 2^r$, which is the sum of the consecutive odd cubes up to $(2k - 1)^3$, by the identity given in the question. The first three values of $s + 1 > 2$ for which $2^{s+1} - 1$ is prime are: $s+1 = 3, 5, 7$, with corresponding even perfect numbers: $n = 2^2(2^3 - 1), 2^4(2^5 - 1), 2^6(2^7 - 1)$, that is: $n = 28, 496, 8128$. The corresponding values of k are $k = 2^1, 2^2, 2^3$, and so $2k - 1 = 3, 7, 15$, respectively. This gives: $28 = 1^3 + 3^3$, $496 = 1^3 + 3^3 + 5^3 + 7^3$, and $8128 = 1^3 + 3^3 + \ldots + 15^3$.

6 marks. *Unseen.*

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	$\sqrt{n}$	$2d$
1	$2d$	d	$\frac{2d+\sqrt{n}}{d}$	4
2	$2d$	1	$2d + \sqrt{n}$	$4d$

Justification of a_0, a_1, a_2 as follows.

$a_0 = [\sqrt{n}]$. But, for all $d \geq 1$, $(2d)^2 = 4d^2 < 4d^2 + d < 4d^2 + 4d + 1 = (2d + 1)^2$ and so $2d < \sqrt{4d^2 + d} < 2d + 1$, so that $[\sqrt{n}] = 2d$, i.e. $a_0 = 2d$.

$a_1 = \left[\frac{2d+\sqrt{n}}{d}\right] = \left[\frac{2d+[\sqrt{n}]}{d}\right] = \left[\frac{2d+2d}{d}\right] = [4] = 4$.

$a_2 = [2d + \sqrt{n}] = [2d + [\sqrt{n}]] = [2d + 2d] = [4d] = 4d$.

The fact that $Q_2 = 1$ signals recurrence, so that $\sqrt{n} = [2d, \overline{4, 4d}]$, as required.

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

(iii) $d = 3$ gives $n = 39$ i.e. $\sqrt{39} = [6, \overline{4, 12}]$. Using $p_0 = a_0, q_0 = 1, p_1 = a_0a_1 + 1, q_1 = a_1$, 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	4	25	4
2	12	306	49
3	4	1249	200
4	12	15294	2449
5	4	62425	9996

This gives three solutions: $x = 25, y = 4$ and $x = 1249, y = 200$ and $x = 62425, y = 9996$.
6 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 $1 \cdot 2 \cdot \ldots \cdot (p-1)/2$ (coprime to p), 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. $p \equiv 1 \pmod{8}$, so $p = 8k + 1$, $(p-1)/2 = 4k$, 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. $p \equiv -1 \pmod{8}$, so $p = 8k - 1$, $(p-1)/2 = 4k - 1$, 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. $p \equiv 3 \pmod{8}$, so $p = 8k + 3$, $(p-1)/2 = 4k + 1$, 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. $p \equiv -3 \pmod{8}$, so $p = 8k - 3$, $(p-1)/2 = 4k - 2$, 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 $(\frac{2}{p}) = -1$.
6 marks. *Bookwork from lectures.*

(iv) Any odd prime is congruent to one of $1, 3, 5, 7 \pmod{8}$.
Case 1. $p \equiv 1 \pmod{8}$, so $p \equiv 1 \pmod{4}$. $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = 1 \cdot 1 = 1$ [by (i),(ii)].
Case 2. $p \equiv 3 \pmod{8}$, so $p \equiv 3 \pmod{4}$. $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = (-1) \cdot (-1) = 1$ [by (i),(ii)].
Case 3. $p \equiv 5 \pmod{8}$, so $p \equiv 1 \pmod{4}$. $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = 1 \cdot (-1) = -1$ [by (i),(ii)].
Case 4. $p \equiv 7 \pmod{8}$, so $p \equiv 3 \pmod{4}$. $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = (-1) \cdot 1 = -1$ [by (i),(ii)].
Hence $(\frac{-2}{p}) = 1$ if and only if $p \equiv 1$ or $3 \pmod{8}$, as required.
4 marks. *Seen on an exercise sheet.*

(v) First note that $3^2 = 9 \equiv 1 \pmod 8$, so that $n = (p_1 p_2 \dots p_k)^2 + 2 = p_1^2 p_2^2 \dots p_k^2 + 2 \equiv 1 + 2 \equiv 3 \pmod 8$. Now, let p be prime and $p|n$. Then $p|(p_1 p_2 \dots p_k)^2 + 2$ and so $-2 \equiv (p_1 p_2 \dots p_k)^2 \pmod p$, giving that $(\frac{-2}{p}) = 1$; hence (from part (iv)) $p \equiv 1$ or $3 \pmod 8$. Note that it is impossible for all prime factors of n to be congruent to $1 \pmod 8$ [since the product of numbers congruent to $1 \pmod 8$ is congruent to $1 \pmod 8$, whereas $n \equiv 3 \pmod 8$]; hence at least one prime p dividing n must satify $p \equiv 3 \pmod 8$. Thus p is a new prime, distinct from $p_1, p_2, \dots, p_k$, satisfying $p \equiv 3 \pmod 8$ [note that p is distinct from $p_1, p_2, \dots, p_k$, since, if $p = p_i$ then $p|n = (p_1 p_2 \dots p_k)^2 + 2$ and $p|(p_1 p_2 \dots p_k)^2$, implying $p|2$, a contradiction, since $p \equiv 3 \pmod 8$ and so p is odd]. Finally, suppose that there are only finitely many primes $p_1, p_2, \dots, p_k$ congruent to $3 \pmod 8$. The above argument gives a new such prime p distinct from $p_1, p_2, \dots, p_k$, a contradiction; hence there are infinitely many such primes.

6 marks. *Unseen.*