Solutions to MATH342 (Number Theory) January 2005 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 $80! = 2^{a_1}5^{b_1}c_1$ 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 $\left[\frac{80}{2}\right] + \left[\frac{80}{4}\right] + \left[\frac{80}{8}\right] + \left[\frac{80}{16}\right] + \left[\frac{80}{32}\right] + \left[\frac{80}{64}\right]$, since all subsequent terms are zero. This gives $a_1 = 40 + 20 + 10 + 5 + 2 + 1 = 78$. Working out b_1 we get $\left[\frac{80}{5}\right] + \left[\frac{80}{25}\right]$, since all subsequent terms are zero. This gives $b_1 = 16 + 3 = 19$. So, there are min(78,19) = 19 zeros at the end of 80!.

4 marks. *Similar to exercise sheet question.*

Similarly, let $35! = 2^{a_2}5^{b_2}c_2$ where c_2 is not a multiple of 2 or 5. Working out a_2 we get $\left[\frac{35}{2}\right] + \left[\frac{35}{4}\right] + \left[\frac{35}{8}\right] + \left[\frac{35}{16}\right] + \left[\frac{35}{32}\right]$, since all subsequent terms are zero. This gives $a_2 = 17 + 8 + 4 + 2 + 1 = 32$. Working out b_2 we get $\left[\frac{35}{5}\right] + \left[\frac{35}{25}\right]$, since all subsequent terms are zero. This gives $b_2 = 7 + 1 = 8$.

Similarly, let $45! = 2^{a_3}5^{b_3}c_3$ where c_3 is not a multiple of 2 or 5. Working out a_3 we get $\left[\frac{45}{2}\right] + \left[\frac{45}{4}\right] + \left[\frac{45}{8}\right] + \left[\frac{45}{16}\right] + \left[\frac{45}{32}\right]$, since all subsequent terms are zero. This gives $a_3 = 22 + 11 + 5 + 2 + 1 = 41$. Working out b_3 we get $\left[\frac{45}{5}\right] + \left[\frac{45}{25}\right]$, since all subsequent terms are zero. This gives $b_3 = 9 + 1 = 10$.

It follows that $\begin{pmatrix} 80 \\ 35 \end{pmatrix} = 80!/(35!\ 45!) = 2^{a_1}5^{b_1}c_1/(2^{a_2}5^{b_2}c_2 2^{a_3}5^{b_3}c_3) = 2^{a_4}5^{b_4}c_4$, where c_4 is not a multiple of 2 or 5, and where $a_4 = a_1 - a_2 - a_3 = 78 - 32 - 41 = 5$ and $b_4 = b_1 - b_2 - b_3 = 19 - 8 - 10 = 1$. So, there is min(5,1) = 1 zero at the end of $\begin{pmatrix} 80 \\ 35 \end{pmatrix}$.

6 marks. *Similar to exercise sheet question.*

(iii) The power of 2 is $[\frac{n}{2}] + \left[\frac{n}{2^2}\right] + \ldots$ and the power of 5 is $[\frac{n}{5}] + \left[\frac{n}{5^2}\right] + \ldots$. Clearly, each term of the second sum is $\leq$ the corresponding term of the first sum, and the first terms $[\frac{n}{2}] > [\frac{n}{5}]$ so long as $n \geq 2$. So, the power of 2 $>$ the power of 5.

2 marks. *Unseen.*

(iv) Write $n! = 2^a 5^b c$, where c is not a multiple of 2 or 5; from (iii) we know that $a > b$, giving: $n! = 2^{a-b}10^b c$, with $a - b > 0$, so that there are b zeros and $n!/10^b$ is even; hence the last nonzero digit is even.

The power of 5 in $(5n)!$ is $\left[\frac{5n}{5}\right] + \left[\frac{5n}{5^2}\right] + \left[\frac{5n}{5^3}\right] + \ldots = n + [\frac{n}{5}] + \left[\frac{n}{5^2}\right] + \ldots = n+$ the power of 5 in $n!$. Since the power of 2 is always at least the power of 5, it follows that the number of zeros at the end of each decimal expression is the same as the power of 5; hence the number of zeros at the end of the decimal expression of $(5n)!$ is n more than that of $n!$.

4 marks. *Unseen.*

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 $a, 2a, \ldots, (p-1)a \quad (*)$. For any j in the range $1 \leq j \leq (p-1)$, we have $p \not| j$. Since also $p \not| a$, it follows that $p \not| ja$; 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 $1 \leq i, j \leq (p-1)$; then $(i-j)a \equiv 0 \pmod{p}$ and so $p \mid (i-j)a$; but $p \not| (i-j)$, since $0 < i-j < p$, and so $p|a$, a contradiction. Hence $ia \not\equiv ja$ whenever $i \neq j$, $1 \leq i, j \leq (p-1)$. 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 mod p 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 $p \not| a$, 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.*

By Fermat's Theorem, since $5 \not| 2$, we have: $2^4 \equiv 1 \pmod{5}$ and so $2^{75} = (2^4)^{18} \cdot 2^3 \equiv 1^{18} \cdot 8 \equiv 3 \pmod{5}$. Similarly, since $5 \not| 3$, we have: $3^4 \equiv 1 \pmod{5}$ and so $3^{75} = (3^4)^{18} \cdot 3^3 \equiv 1^{18} \cdot 27 \equiv 2 \pmod{5}$. Hence, $2^{75} + 3^{75} \equiv 3 + 2 = 5 \equiv 0 \pmod{5}$, giving that $2^{75} + 3^{75}$ is divisible by 5.

3 marks. *Seen similar on exercise sheet.*

(ii) Let $n = r^4 + 1$. If $5 \not| r$ then by Fermat's Theorem, $r^4 \equiv 1 \pmod{5}$, so that $n = r^4 + 1 \equiv 1 + 1 \equiv 2 \pmod{5}$. If $5|r$ then $r \equiv 0 \pmod{5}$, so that $n = r^4 + 1 \equiv 0^4 + 1 \equiv 1 \pmod{5}$. In all cases, $n \not\equiv 0 \pmod{5}$; that is: n is never divisible by 5.

Imagine n were a multiple of 13, so that $n = r^4 + 1 \equiv 0 \pmod{13}$. Then $r^4 \equiv -1 \pmod{13}$, and on cubing both sides: $r^{12} \equiv (-1)^3 = -1 \pmod{13}$. But this contradicts both the case when $13 \not| r$ [since then by Fermat's Theorem $r^{12} \equiv 1 \pmod{13}$] and the case when $13|r$ [since then $r^{12} \equiv= 0^{12} \equiv 0 \pmod{13}$]. Hence it is not possible for n to be a multiple of 13.

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

Imagine $n = r^4 + 1$ were a multiple of p, where p is a prime of the form $p = 4m + 3$. Then $n = r^4 + 1 \equiv 0 \pmod{p}$. Then $r^4 \equiv -1 \pmod{p}$. If $p \not| r$ then by Fermat's Theorem, $r^{p-1} \equiv 1 \pmod{p}$; that is: $r^{4m+2} \equiv 1 \pmod{p}$. But, since $r^4 \equiv -1 \pmod{p}$, we also have: $r^{4m+2} \equiv (r^4)^m r^2 \equiv (-1)^m r^2 \equiv \pm r^2 \pmod{p}$; combining these last two equations gives that $\pm r^2 \equiv 1 \pmod{p}$, and so on squaring both sides: $r^4 \equiv 1 \pmod{p}$, which contradicts $r^4 \equiv -1 \pmod{p}$. If $p|r$ then $r^4 \equiv 0^4 \equiv 0 \pmod{p}$, which immediately contradicts $r^4 \equiv -1 \pmod{p}$. In either case, we have a contradiction, so that is not possible for n to be a multiple of p.

3 marks. *Unseen.*

(iii) Imagine $n = r^{2k} + 1$ were a multiple of p, where p is a prime of the form $p = 4mk + 2k + 1$. Then $n = r^{2k} + 1 \equiv 0 \pmod{p}$. Then $r^{2k} \equiv -1 \pmod{p}$. If $p \not| r$ then by Fermat's Theorem, $r^{p-1} \equiv 1 \pmod{p}$; that is: $r^{4mk+2k} \equiv 1 \pmod{p}$. But, since $r^{2k} \equiv -1 \pmod{p}$, we also have: $r^{4mk+2k} \equiv (r^{2k})^{2m} r^{2k} \equiv (-1)^{2m} r^{2k} \equiv r^{2k} \pmod{p}$; combining these last two equations gives that $r^{2k} \equiv 1 \pmod{p}$, which contradicts $r^{2k} \equiv -1 \pmod{p}$. If $p|r$ then $r^{2k} \equiv 0^{2k} \equiv 0 \pmod{p}$, which immediately contradicts $r^{2k} \equiv -1 \pmod{p}$. In either case, we have a contradiction, so that is not possible for n to be a multiple of p.

3 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.

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: $(19, 169) = 1$, so that Miller's Test can be applied on 169 to base 19. First compute: $19^3 \equiv 6859 \equiv 99 \pmod{169}$, so that $19^6 \equiv (19^3)^2 \equiv 99^2 \equiv 9801 \equiv -1 \pmod{169}$. This gives, $19^{169-1} \equiv 19^{168} \equiv (19^6)^{28} \equiv (-1)^{28} \equiv 1$, so that 169 is a pseudoprime to the base 19 (given that $169 = 13 \cdot 13$ and so is composite). The exponent 168 is even, so we continue to compute $19^{84} \equiv (19^6)^{14} \equiv (-1)^{14} \equiv 1$. The exponent 84 is still even, so we continue to compute $19^{42} \equiv (19^6)^7 \equiv (-1)^7 \equiv -1 \equiv 168$. The residue is no longer 1, and so we stop. We see that the last residue is 1 or $169 - 1$, so that 169 passes Miller's Test to base 19. Thus, 169 is a strong pseudoprime to base 19.

Check: $(5, 217) = 1$, so that Miller's Test can be applied on 217 to base 5. First compute: $5^6 \equiv 15625 \equiv 1 \pmod{217}$, so that $5^{217-1} \equiv 5^{216} \equiv (5^6)^{36} \equiv 1^{36} \equiv 1 \pmod{217}$, so that 217 is a pseudoprime to the base 5 (given that $217 = 7 \cdot 31$ and so is composite). 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 $5^{27} \equiv (5^6)^4 \cdot 5^3 \equiv 1^4 \cdot 125 \equiv 125$. This is neither 1 nor $217 - 1$, so 217 fails Miller's Test to base 5. Thus, 217 is not a strong pseudoprime to base 5.

Check: $(2, 105) = 1$, so that Miller's Test can be applied on 105 to base 2. First compute: $2^{12} \equiv 4096 \equiv 1 \pmod{105}$, so that $2^{105-1} \equiv 2^{104} \equiv (2^{12})^8 \cdot 2^8 \equiv 1^8 \cdot 256 \equiv 46 \pmod{105}$, giving that 105 is not a pseudoprime to base 2. Miller's Test is immediately failed at Step 1, so that 105 is not a strong pseudoprime to base 2.

8 marks. *Seen similar on exercise sheet.*

(iii) Let $b_1 = n - b$. First note that $b_1 \equiv 0 - b \equiv -b \pmod{n}$. Since n passes Step 1 to base b, we have $b^{n-1} \equiv 1$ and so $b_1^{n-1} \equiv (-b)^{n-1} \equiv 1 \pmod{n}$ also, since $n - 1$ is even; thus, n passes Step 1 to base b_1 also. Imagine that n fails some application of Step 2 to base b_1, so that $b_1^{n-1} \equiv b_1^{(n-1)/2} \equiv \ldots \equiv b_1^{2k} \equiv 1 \pmod{n}$ and $b_1^k \not\equiv \pm 1 \pmod{n}$ for some k. But then $b^{n-1} \equiv b^{(n-1)/2} \equiv \ldots \equiv b^{2k} \equiv 1 \pmod{n}$ [since $b \equiv -b_1$ and the exponenents are all even], and $b^k \equiv (-b_1)^k \equiv \pm b_1^k \not\equiv \pm 1 \pmod{n}$, contradicting the given fact that n passes Miller's Test on n to base b. Hence n passes Miller's Test on n to base b_1.

3 marks. *Unseen.*

Question 4.

(i) 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. $\text{ord}_m 10 = k$, which is the length of the period.

7 marks. *Bookwork from lectures.*

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

2 marks. *Seen similar in lectures.*

(iii) As usual, $\text{ord}_m 10$ is the smallest $k > 0$ for which $10^k \equiv 1 \pmod{m}$. In each case, by (i), this is the same as the decimal period length of $\frac{1}{m}$. We can also use the general result that $\text{ord}_m a$ is always a factor of $\phi(m)$ for any a, m.

For $m = 7$, we know that $\text{ord}_7 10$ is a factor of $\phi(7) = 6$, and so the only possibilities are $1, 2, 3, 6$. Compute powers of 10 mod 7: $10^1 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv 6 \pmod 7$, which is enough to exclude $1, 2, 3$ as possible values of $\text{ord}_7 10$, so that $\text{ord}_7 10 = 6$, which must be the length of the decimal period of $\frac{1}{7}$.

For $m = 31$, we know that $\text{ord}_{31} 10$ is a factor of $\phi(31) = 30$, and so the only possibilities are $1, 2, 3, 5, 6, 10, 15, 30$. Compute powers of 10 mod 31: $10^1 \equiv 10$, $10^2 \equiv 7$, $10^3 \equiv 8$, $10^4 \equiv 18$, $10^5 \equiv 25$, $10^6 \equiv 2$, $10^{10} \equiv (10^5)^2 \equiv 625 \equiv 5$, $10^{15} \equiv 10^5 \cdot 10^{10} \equiv 25 \cdot 5 \equiv 125 \equiv 1 \pmod{31}$, which is enough to exclude $1, 2, 3, 5, 6, 10$ as possible values of $\text{ord}_{31} 10$, so that $\text{ord}_{31} 10 = 15$, which must be the length of the decimal period of $\frac{1}{31}$.

For $m = 217 = 7 \cdot 31$, we have from part (ii) that $\text{ord}_{217} 10$ is the least common multiple of $\text{ord}_7 10$ and $\text{ord}_{31} 10$; that is: the least common multiple of 6 and 15, which is 30, which is therefore the length of the decimal period of $\frac{1}{217}$.

6 marks. *Seen similar in lectures.*

(iv) From lectures, write $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$, where $p_1, \ldots, p_k$ are distinct primes each $a_i \geq 0, b_i \geq 0$ and, for each i, we have $a_i > 0$ or $b_i > 0$. Then, from lectures, $(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_k^{\min(a_k,b_k)}$ and $[a,b] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_k^{\max(a_k,b_k)}$, so that: $(a,b)[a,b] = p_1^{\min(a_1,b_1)+\max(a_1,b_1)} p_2^{\min(a_2,b_2)+\max(a_2,b_2)} \ldots p_k^{\min(a_k,b_k)+\max(a_k,b_k)}$. Also: $ab = p_1^{a_1+b_1} p_2^{a_2+b_2} \ldots p_k^{a_k+b_k}$. These are the same, since for all i, $\min(a_i,b_i)+\max(a_i,b_i) = a_i + b_i$.

2 marks. *Bookwork from lectures.*

(v) The length of the decimal period of $\frac{1}{pq}$ is $\text{ord}_{pq} 10$, which by (ii) is $\text{ord}_{pq} 10 = [\text{ord}_p 10, \text{ord}_q 10]$. We also know that $\text{ord}_p 10 | \phi(p)$ and $\text{ord}_q 10 | \phi(q)$. If $\text{ord}_p 10 = \phi(p) = p - 1$ and $\text{ord}_q 10 = \phi(q) = q - 1$ then $\text{ord}_{pq} 10 = [\text{ord}_p 10, \text{ord}_q 10] = \text{ord}_p 10 \ \text{ord}_q 10 / (\text{ord}_p 10, \text{ord}_q 10) = (p-1)(q-1)/(p-1, q-1) \leq (p-1)(q-1)/2$, since $p-1$ and $q-1$ are even and $(p-1, q-1) \geq 2$. If $\text{ord}_p 10 \neq \phi(p)$ or $\text{ord}_q 10 \neq \phi(q)$ then $\text{ord}_p 10 \leq \phi(p)/2$ or $\text{ord}_q 10 \leq \phi(q)/2$, so that $\text{ord}_{pq} 10 = [\text{ord}_p 10, \text{ord}_q 10] = \text{ord}_p 10 \ \text{ord}_q 10 / (\text{ord}_p 10, \text{ord}_q 10) \leq \text{ord}_p 10 \ \text{ord}_q 10 \leq (p-1)(q-1)/2$. In either case, we have the period length bounded above by $(p-1)(q-1)/2$, as required.

3 marks. *Unseen.*

Question 5.

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

7 marks. *Bookwork from lectures.*

(iii) Working out powers of 3 mod 38 gives

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$3^k \bmod 38$	3	9	27	5	15	7	21	25	37	35	29	11	33	23	31	17	13	1

This verifies that $\text{ord}_{38}3 = 18 = \phi(38)$ and so 3 is a primitive root mod 38.

4 marks. *Seen similar in exercises.*

(a) From table, $7 \equiv 3^6, 25 \equiv 3^8 \pmod{38}$ so the given equation $7^x \equiv 25 \pmod{38}$ becomes

$$3^{6x} \equiv 3^8 \pmod{38} \Leftrightarrow 6x \equiv 8 \pmod{18}$$

by the general results that, for a primitive root g mod n: $g^a \equiv g^b \pmod{n} \Leftrightarrow a \equiv b \pmod{\phi(n)}$. But the equation $6x \equiv 8 \pmod{18}$ has no solutions, since $(6, 18) = 6$ which is not a factor of 8; hence the given equation also has no solutions.

3 marks. *Seen similar in exercises.*

(b) Note that $y^4 \equiv 23 \pmod{38}$ implies that $(y, 38) = 1$ since any common factor would also have to divide the r.h.s. 23 of the congruence, and so would be a common factor of $38, 23$, which are coprime. Hence $y \equiv 3^x \pmod{38}$ for some x (since 3 is a primitive root). Also $3^{14} \equiv 23$ from the table. The given congruence turns into

$$3^{4x} \equiv 3^{14} \pmod{38} \Leftrightarrow 4x \equiv 14 \pmod{18}.$$

by the same general result used in part (a). This gives $2x \equiv 7 \pmod{9}$; multiplying both sides by 5 (which is the inverse of 2 mod 9) gives: $x \equiv 35 \equiv 8 \pmod{9}$, i.e. $x \equiv 8, 17 \pmod{18}$ which, from the table, gives: $y \equiv 25, 13 \bmod 38$.

4 marks. *Seen similar in exercises.*

Question 6.

(i) $d(n)$ = the number of the divisors of n which are ≥ 1. $\sigma(n)$ = the sum of the divisors of n which are ≥ 1.

p^a has divisors $1, p, p^2, \ldots p^{a-1}, p^a$, of which there are $a+1$, so that $d(p^a) = a+1$ and $\sigma(p^a) = 1 + p + p^2 + \ldots p^a = (p^{a+1}-1)/(p-1)$.

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

4 marks. *From lectures.*

(ii) Here is a table of values of $\sigma(p^a)$ for small p and a. Since all rows and columns are strictly increasing, any further entries would be greater than 48 and so are irrelevant.

$p \rightarrow$ / $a \downarrow$	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	...
1	3	4	6	8	12	14	18	20	24	30	32	38	42	44	48	...
2	7	13	31	57												
3	15	40	156													
4	31	121														
5	63															
6	127															

Now the following give all the ways of writing 48 as a product of entries in different columns of the table: $4 \cdot 12$ or $6 \cdot 8$ or or 48. These give

$n = 3^1 \cdot 11^1$, $5^1 \cdot 7^1$, 47^1, that is: $n = 33, 35, 47$ are the only solutions to $\sigma(n) = 48$.

9 marks. *Seen similar on exercise sheet.*

(iii) Since $d(n) = (n_1+1)(n_2+1)\ldots$, the only way for $d(n) = 27$ is if there exists $n_j + 1 = 27$ and all other $n_i = 0$, or when there exist $n_j + 1 = 9, n_k + 1 = 3$ and all other $n_i = 0$, or when there exist $n_j + 1 = 3, n_k + 1 = 3, n_\ell = 3$ and all other $n_i = 0$. These correspond to n have the form: $n = p^{26}$ for some prime p, or $n = p^8 q^2$, for some distinct primes p, q, or $n = p^2 q^2 r^2$, for some distinct primes p, q, r, The smallest number of the first type is $2^{26} = 67108864$. The smallest number of the second type is $2^8 \cdot 3^2 = 2304$. The smallest number of the third type is $2^2 \cdot 3^2 \cdot 5^2 = 900$. So, the smallest n such that $d(n) = 27$ is $n = 900$.

3 marks. *Seen similar on exercise sheet, but this one is harder.*

(iv) Note that, since $2^k, 3, 5$ are pairwise coprime, we have $\sigma(2^k \cdot 15) = \sigma(2^k)\sigma(3)\sigma(5) = \frac{2^{k+1}-1}{2-1} \cdot 4 \cdot 6 = 24(2^{k+1}-1)$. For $n = 2^k \cdot 15$ to be perfect, we must have $\sigma(n) = 2n$, that is: $24(2^{k+1}-1) = 2 \cdot 2^k \cdot 15$, which is the same as: $2^3 \cdot 3(2^{k+1}-1) = 2^{k+1} \cdot 15$. But the power of 2 in the left hand side is 2^3 and the power of 2 in the right hand side is 2^{k+1}, which forces $k = 2$ as the only possible value of k. But on substituting $k = 2$ into both sides, gives $2^3 \cdot 3 \cdot (2^3 - 1) = 168$ as the left hand side, and $2^3 \cdot 15 = 120$ as the right hand side, which are not equal. Hence there is no value of k satisfying the equation, and so no value of k for which $2^k \cdot 15$ is perfect.

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

Justification of a_0, a_1, a_2 as follows.

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

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

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

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

8 marks. *Seen similar on exercise sheet.*

(iii) $d = 6$ gives $n = 42$ i.e. $\sqrt{42} = [6, \overline{2, 12}]$.

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	2	13	2
2	12	162	25
3	2	337	52
4	12	4206	649
5	2	8749	1350

This gives three solutions: $x = 13, y = 2$ and $x = 337, y = 52$ and $x = 8749, y = 1350$.

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), $(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} \equiv 1 \pmod{p} \iff 2|(p-1)/2 \iff 4|(p-1) \iff p \equiv 1 \pmod{4}$.
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) *Gauss' Law of Quadratic Reciprocity:* Let p, q be two distinct 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 $(\frac{p}{q}) = -(\frac{q}{p})$.

$(\frac{14}{71}) = (\frac{2}{71})(\frac{7}{71}) = (\frac{7}{71})$ [by (iii) since $71 \equiv -1 \pmod{8}$]
$= -(\frac{71}{7})$ [by QR, since 71 and 7 are $\equiv 3 \pmod{4}$]
$= -(\frac{1}{7}) = -1$ [since $1 \equiv 1^2 \pmod{7}$].

$(\frac{-3}{71}) = (\frac{-1}{71})(\frac{3}{71}) = -(\frac{3}{71})$ [by (ii), since $71 \equiv 3 \pmod{4}$]
$= (\frac{71}{3})$ [by QR, since 71 and 3 are $\equiv 3 \pmod{4}$]
$= (\frac{2}{3}) = (\frac{-1}{3}) = -1$ [by (ii), since $3 \equiv 3 \pmod{4}$].

$(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p}) = (\frac{2}{p})(\frac{p}{5})$ [by QR, since $5 \equiv 1 \pmod{4}$]
$= 1 \iff (\frac{2}{p}) = (\frac{p}{5}) = 1$ or $(\frac{2}{p}) = (\frac{p}{5}) = -1$
$\iff (p \equiv \pm 1 \pmod{8}$ and $p \equiv \pm 1 \pmod{5})$ or $(p \equiv \pm 3 \pmod{8}$ and $p \equiv \pm 2 \pmod{5})$
$\iff p \equiv \pm 1, \pm 9 \pmod{40}$ or $p \equiv \pm 3, \pm 13 \pmod{40}$.

In summary, $(\frac{10}{p}) = 1 \iff p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$, as required.
7 marks. *Unseen.*