Solutions to MATH342 (Number Theory) January 2003 examination

Question 1.

(i) $x^2 \equiv x \pmod{1000} \iff x^2 \equiv x \pmod{8 \text{ and } 125}$. The forward direction is trivial, since $2^3 | 2^3 \cdot 5^3$ and $5^3 | 2^3 \cdot 5^3$. The reverse direction holds because $(2^3, 5^3) = 1$, using the general result that $a \equiv b \pmod{m \text{ and } n}$ and $(m,n) = 1 \Rightarrow a \equiv b \pmod{mn}$.

2 marks. *Seen similar in lectures.*

We have to solve $x(x-1) \equiv 0 \pmod{2^3 \text{ and mod } 5^3}$. We have $p^k | x(x-1) \Rightarrow p^k | x$ or $p^k | x-1$ (p prime), since $(x, x-1) = 1$ (using general result that $p^k | ab$ and $(a,b) = 1 \Rightarrow p^k | a$ or $p^k | b$). Hence: $x \equiv 0$ or $1 \pmod 8$ and $x \equiv 0$ or $1 \pmod{125}$. There are thus 4 cases:

Case (a). $x \equiv 0 \pmod 8$ and $x \equiv 0 \pmod{125}$. Holds $\iff x \equiv 0 \pmod{1000}$.

Case (b). $x \equiv 0 \pmod 8$ and $x \equiv 1 \pmod{125}$. From the first equation, $x = 8k$. Substituting this into the second equation gives: $8k \equiv 1 \pmod{125}$. Need to find the inverse of 8 mod 125:

$$\begin{pmatrix} 1 & 0 & 125 \\ 0 & 1 & 8 \end{pmatrix} \to \begin{pmatrix} 1 & -15 & 5 \\ 0 & 1 & 8 \end{pmatrix} \to \begin{pmatrix} 1 & -15 & 5 \\ -1 & 16 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & -31 & 2 \\ -1 & 16 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & -31 & 2 \\ -3 & 47 & 1 \end{pmatrix}.$$

The second line of the last matrix tells us: $(-3) \cdot 125 + 47 \cdot 8 = 1$, so that 47 is an inverse of 8 mod 125. Multiplying both sides of $8k \equiv 1 \pmod{125}$ by 47 gives: $k \equiv 47 \pmod{125}$; that is: $k = 47 + 125\ell$. Substituting this into $x = 8k$ gives: $x = 8(47 + 125\ell) = 376 + 1000\ell$, which is the same as: $x \equiv 376 \pmod{1000}$.

Case (c). $x \equiv 1 \pmod 8$ and $x \equiv 0 \pmod{125}$. From the first equation, $x = 125k$. Substituting this into the second equation gives: $125k \equiv 1 \pmod 8$, so that: $5k \equiv 1 \pmod 8$. Multiplying both sides by 5 then gives: $25k \equiv 5 \pmod 8$, so that $k \equiv 5 \pmod 8$; that is: $k = 5 + 8\ell$. Substituting this into $x = 125k$ gives: $x = 125(5 + 8\ell) = 625 + 1000\ell$, which is the same as: $x \equiv 625 \pmod{1000}$.

Case (d). $x \equiv 1 \pmod 8$ and $x \equiv 1 \pmod{125}$. Holds $\iff x \equiv 1 \pmod{1000}$.

In summary the final solution is: $x \equiv 0, 1, 376$, or $625 \pmod{1000}$.

8 marks. *Seen similar (but simpler) in lectures.*

(ii) If x is divisible by 3, then $x = 3k$ for some integer k, so that: $x^3 = 27k^3 \equiv 0 \pmod 9$. If x is not divisible by 3, then $x \equiv 3k \pm 1$ for some integer k, so that: $x^3 = (3k \pm 1)^3 \equiv 27k^3 \pm 27k^2 + 9k \pm 1 \equiv \pm 1 \pmod 9$. Hence, in all cases, we have $x^3 \equiv 0, 1$, or $-1 \pmod 9$. This gives 27 possibilities to consider for $x^3 + y^3 + z^3$:

$-1-1-1, -1-1+0, -1-1+1, -1+0-1, -1+0+0, -1+0+1, -1+1-1, -1+1+0, -1+1+1,$
$0-1-1, 0-1+0, 0-1+1, 0+0-1, 0+0+0, 0+0+1, 0+1-1, 0+1+0, 0+1+1,$
$1-1-1, 1-1+0, 1-1+1, 1+0-1, 1+0+0, 1+0+1, 1+1-1, 1+1+0, 1+1+1,$

which are congruent mod 9 to: $6, 7, 8, 7, 8, 0, 8, 0, 1, 7, 8, 0, 8, 0, 1, 0, 1, 2, 8, 0, 1, 0, 1, 2, 1, 2, 3,$ respectively. None of these is 4 (mod 9), so that $x^3 + y^3 + z^3$ is never of the form $9m + 4$.

5 marks. *Unseen, although similar ideas seen.*

(iii) Any x satisfies: $x \equiv 0, 1, 2, 3, 4, 5$ or $6 \pmod 7$, so that $x^2 \equiv 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2 \equiv 0, 1, 4, 2, 2, 4, 1 \equiv 0, 1, 2$ or $4 \pmod 7$, and the same for y^2. Therefore, there are 16 cases for $x^2 + y^2$, namely: $0+0, 0+1, 0+2, 0+4, 1+0, 1+1, 1+2, 1+4, 2+0, 2+1, 2+2, 2+4, 4+0, 4+1, 4+2, 4+4$, which are congruent (mod 7) to: $0, 1, 2, 4, 1, 2, 3, 5, 2, 3, 4, 6, 4, 5, 6, 1$, respectively. The only case where $x^2 + y^2 \equiv 0 \pmod 7$ is the case when both $x^2 \equiv 0$ and $y^2 \equiv 0 \pmod 7$; that is: $x \equiv 0$ and $y \equiv 0 \pmod 7$. Suppose that $x^2 + y^2 = 7(7m + 1)$. Then $x^2 + y^2 \equiv 0$, giving that $x \equiv 0$ and $y \equiv 0 \pmod 7$, by the previous result; say: $x = 7r$ and $y = 7s$. Then $7^2(r^2 + s^2) = 7(7m + 1)$, so that $7(r^2 + s^2) = (7m + 1)$, which is impossible, since the LHS is divisible by 7, but not the RHS.

5 marks. *Unseen, and a new idea.*

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.*

Using Fermat's Theorem, since $17 \not| 3$, we have: $3^{16} \equiv 1 \pmod{17}$ and so $3^{50} = (3^{16})^3 \cdot 3^2 \equiv 1^3 \cdot 9 \equiv 9 \pmod{17}$. Similarly, since $17 \not| 5$, we have: $5^{16} \equiv 1 \pmod{17}$ and so $5^{50} = (5^{16})^3 \cdot 5^2 \equiv 1^3 \cdot 25 \equiv 8 \pmod{17}$. Hence, $3^{50} + 5^{50} \equiv 9 + 8 = 17 \equiv 0 \pmod{17}$, giving that $3^{50} + 5^{50}$ is divisible by 17.

3 marks. *Seen similar on exercise sheet.*

(ii) Let $n = r^6 + 1$. If $7 \not| r$ then by Fermat's Theorem, $r^6 \equiv 1 \pmod{7}$, so that $n = r^6 + 1 \equiv 1 + 1 \equiv 2 \pmod{7}$. If $7|r$ then $r \equiv 0 \pmod{7}$, so that $n = r^6 + 1 \equiv 0^6 + 1 \equiv 1 \pmod{7}$. In all cases, $n \not\equiv 0 \pmod{7}$; that is: n is never divisible by 7.

If $3 \not| r$ then by Fermat's Theorem, $r^2 \equiv 1 \pmod{3}$, so that $n = (r^2)^3 + 1 \equiv 1^3 + 1 \equiv 2 \pmod{3}$. If $3|r$ then $r \equiv 0 \pmod{3}$, so that $n = r^6 + 1 \equiv 0^6 + 1 \equiv 1 \pmod{3}$. In all cases, $n \not\equiv 0 \pmod{3}$; that is: n is never divisible by 3.

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

Imagine n were a multiple of 11, so that $n = r^6 + 1 \equiv 0 \pmod{11}$. Then $r^6 \equiv -1 \pmod{11}$. If $11 \not| r$ then by Fermat's Theorem, $r^{10} \equiv 1 \pmod{11}$, and so $r^4 \cdot r^6 \equiv 1 \pmod{11}$. Substituting $r^6 \equiv -1 \pmod{11}$ into this last equation gives: $r^4 \cdot (-1) \equiv 1 \pmod{11}$, and so: $r^4 \equiv -1 \pmod{11}$; cubing both sides gives: $r^{12} \equiv (-1)^3 \equiv -1 \pmod{11}$. On the other hand, squaring both sides of $r^6 \equiv -1 \pmod{11}$ gives $r^{12} \equiv (-1)^2 \equiv 1 \pmod{11}$, a contradiction. If $11|r$ then $r^6 \equiv 0^6 \equiv 0 \pmod{11}$, which immediately contradicts $r^6 \equiv -1 \pmod{11}$. In either case, we have a contradiction, so that is not possible for n to be a multiple of 11.

3 marks. *Seen similar on a exercise sheet (although this one is slightly harder).*

Imagine $n = r^6 + 1$ were a multiple of p, where p is a prime of the form $p = 12m + 7$. Then $n = r^6 + 1 \equiv 0 \pmod{p}$. Then $r^6 \equiv -1 \pmod{p}$. If $p \not| r$ then by Fermat's Theorem, $r^{p-1} \equiv 1 \pmod{p}$; that is: $r^{12m+6} \equiv 1 \pmod{p}$. But, since $r^6 \equiv -1 \pmod{p}$, we also have: $r^{12m+6} \equiv (r^6)^{2m+1} \equiv (-1)^{2m+1} \equiv -1 \pmod{p}$, a contradiction. If $p|r$ then $r^6 \equiv 0^6 \equiv 0 \pmod{p}$, which immediately contradicts $r^6 \equiv -1 \pmod{p}$. In either case, we have a contradiction, so that is not possible for n to be a multiple of p.

4 marks. *Unseen.*

Question 3.

(i) For $n \geq 1$ define $\phi(n)$ to be the number of integers x satisfying $1 \leq x \leq n$ and $(x, n) = 1$. 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),

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

4 marks. *Bookwork.*

If p is prime and $p|n$ then p is one of the p_i in the above prime power factorization of n, and so $p - 1 = p_i - 1$ occurs as a factor of the formula for $\phi(n)$, giving that $(p-1)|\phi(n)$. If p is prime and $p^2|n$ then again p is one of the p_i in the above prime power factorization of n, and $n_i \geq 2$, so that $p^{n_i-1} = p_i^{n_i-1}$ occurs as a factor of the formula for $\phi(n)$, giving that $p^{n_i-1}|\phi(n)$, and so $p|\phi(n)$, since $n_i - 1 \geq 1$.

2 marks. *Unseen.*

(ii) We have: $10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \cdot 5) = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$, which is the prime power factorization of $10!$. So, by the formula, $\phi(10!) = 2^7(2-1)3^3(3-1)5^1(5-1)7^0(7-1) = 829440$. The binomial coefficient $a = (21 \cdot 22 \cdot 23 \cdot 24 \cdot 25)/(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5) = (3 \cdot 7 \cdot 2 \cdot 11 \cdot 23 \cdot 2^3 \cdot 3 \cdot 5^2)/(1 \cdot 2 \cdot 3 \cdot 2^2 \cdot 5) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$, so that $\phi(a) = 2^0(2-1)3^0(3-1)5^0(5-1)7^0(7-1)11^0(11-1)23^0(23-1) = 10560$.

6 marks. *Unseen.*

(iii) If n is divisible by an odd prime p, then $(p-1)|\phi(n)$ so that $\phi(n)$ is even and cannot be of the form 3^k. If n is not divisible by any odd prime p, the n must be a power of 2, say $n = 2^r$; but then $\phi(n) = 2^{r-1}$, which again is not of the form 3^k.

In seeking odd primes p such that $\phi(p)$ is a power of 2, we use the fact that $\phi(p) = p - 1$, so this requires $p - 1$ to be a power of 2; that is, p must be a prime which is one more than a power of 2. The first few numbers one more than a power of 2 are: $2^0 + 1, 2^1 + 1, 2^2 + 1, 2^3 + 1, 2^4 + 1$, which are: $2, 3, 5, 9, 17$, of which $2, 3, 5, 17$ are prime. However, we are asked for odd primes, so we exclude 2, and we have found three values of prime $p = 3, 5, 17$ satisfying the condition that $\phi(p)$ is a power of 2. Check: $\phi(3) = 2^1$, $\phi(5) = 2^2$, and $\phi(17) = 2^4$.

It is natural to look at n of the form $n = 3^k \cdot p$, where p is one of the primes just found, since then $\phi(n)$ will have only 2 and 3 as prime factors; this will be a power of 6 when 2 and 3 occur to the same power. For $p = 3$, we try $n = 3^k \cdot 3 = 3^{k+1}$, for which $\phi(n) = 3^k(3-1) = 3^k \cdot 2$; we need take $k = 1$ to get $n = 9$ and $\phi(n) = 6$. For $p = 5$, we try $n = 3^k \cdot 5$, for which $\phi(n) = 3^{k-1}(3-1)(5-1) = 3^{k-1} \cdot 2^3$; we need take $k = 4$ to get $n = 3^4 \cdot 5 = 405$ and $\phi(n) = 6^3$. For $p = 17$, we try $n = 3^k \cdot 17$, for which $\phi(n) = 3^{k-1}(3-1)(17-1) = 3^{k-1} \cdot 2^5$; we need take $k = 6$ to get $n = 3^6 \cdot 17 = 12393$ and $\phi(n) = 6^5$. In summary, we have found: $n = 9, 405, 12393$.

8 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.*

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) We say that n is a *pseudoprime* to base b if n is composite and $b^n \equiv b \pmod{n}$. When $(b, n) = 1$ this is the same as: $b^{n-1} \equiv 1 \pmod{n}$. We say that n is a *strong pseudoprime* to base b if n is composite and n passes Miller's Test to base b.

2 marks. *Definitions from lectures.*

(iii) Check: $(2, 645) = 1$, so that Miller's Test can be applied on 645 to base 2. First compute: $2^{14} \equiv 16384 \equiv 259$, $2^{28} \equiv (2^{14})^2 \equiv 259^2 \equiv 67081 \equiv 1 \pmod{645}$. This gives, $2^{645-1} \equiv 2^{644} \equiv (2^{28})^{23} \equiv 1^{23} \equiv 1$, so that 645 is a pseudoprime to the base 2 (given that $645 = 3 \cdot 5 \cdot 43$ and so is composite). The exponent 644 is even, so we continue to compute $2^{322} \equiv (2^{28})^{11} \cdot 2^{14} \equiv 1^{11} \cdot 259 \equiv 259$; this is neither 1 nor $645 - 1$, and so we stop, with 645 failing (at Step 2) of Miller's test to base 2. Thus, 645 is not a strong pseudoprime to base 2.

Check: $(3, 121) = 1$, so that Miller's Test can be applied on 121 to base 3. First compute: $3^5 \equiv 243 \equiv 1 \pmod{121}$. This gives, $3^{121-1} \equiv 3^{120} \equiv (3^5)^{24} \equiv 1^{24} \equiv 1$, so that 121 is a pseudoprime to the base 3 (given that $121 = 11^2$ and so is composite). The exponent 120 is even, so we continue to compute $3^{60} \equiv (3^5)^{12} \cdot 1^{12} \equiv 1$. The exponent 60 is even, so we continue to compute $3^{30} \equiv (3^5)^6 \cdot 1^6 \equiv 1$. The exponent 30 is even, so we continue to compute $3^{15} \equiv (3^5)^3 \cdot 1^3 \equiv 1$. The exponent 15 is odd, and so we stop, with 121 passing Miller's Test to base 3. Thus, 121 is a strong pseudoprime to base 3.

Check: $(2, 33) = 1$, so that Miller's Test can be applied on 33 to base 2. First compute: $2^5 \equiv 32 \equiv -1 \pmod{33}$, so that $2^{33-1} \equiv (2^5)^6 \cdot 2^2 \equiv (-1)^6 \cdot 4 \equiv 4 \pmod{33}$, giving that 33 is not a pseudoprime to base 2. Miller's Test is immediately failed at Step 1, so that 33 is not a strong pseudoprime to base 2.

7 marks. *Seen similar on exercise sheet.*

(iv) Since n is a pseudoprime to base a and base ab, it follows that n is composite, with $a^n \equiv a \pmod{n}$ and $(ab)^n \equiv ab \pmod{n}$; that is: $a^n b^n \equiv ab \pmod{n}$. Substituting the first congruence into the LHS of the last gives: $ab^n \equiv ab \pmod{n}$. Cancelling a from both sides (allowable, since $(a, n) = 1$) then gives: $ab^n \equiv ab \pmod{n}$, so that n is a pseudoprime to base b.

2 marks. *Unseen.*

Question 5.

(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. the order of 10 mod m is k, which is the length of the period.

8 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.

3 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 already 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 $m = 23$, we know that $\text{ord}_{23} 10$ is a factor of $\phi(23) = 22$, and so the only possibilities are $1, 2, 11, 22$. Compute powers of 10 mod 23:

$10^1 \equiv 10$, $10^2 \equiv 8$, $10^3 \equiv 11$, $10^4 \equiv 18$, $10^5 \equiv 19$, $10^6 \equiv 6$, $10^7 \equiv 14$, $10^8 \equiv 2$, $10^9 \equiv 20$, $10^{10} \equiv 16$, $10^{11} \equiv 22 \pmod{23}$,

which already is enough to exclude $1, 2, 11$ as possible values of $\text{ord}_{23} 10$, so that $\text{ord}_{23} 10 = 22$, which must be the length of the decimal period of $\frac{1}{23}$.

For $m = 161 = 7 \cdot 23$, we have from part (ii) that $\text{ord}_{161} 10$ is the least common multiple of $\text{ord}_7 10$ and $\text{ord}_{23} 10$; that is: the least common multiple of 6 and 22, which is 66, which is therefore the length of the decimal period of $\frac{1}{161}$.

6 marks. *Seen similar in lectures.*

(iv) The length of the decimal period of $\frac{1}{7p}$ is $\text{ord}_{7p} 10$, which by (ii) is $\text{ord}_{7p} 10 = [\text{ord}_7 10, \text{ord}_p 10]$. We also know that $\text{ord}_7 10 | \phi(7)$ and $\text{ord}_p 10 | \phi(p)$. If $\text{ord}_7 10 = \phi(7) = 6$ and $\text{ord}_p 10 = \phi(p) = p-1$ then $\text{ord}_{7p} 10 = [\text{ord}_7 10, \text{ord}_p 10] = \text{ord}_7 10 \, \text{ord}_p 10 / (\text{ord}_7 10, \text{ord}_p 10) = 6(p-1)/(6, p-1) \leq 3(p-1)$, since $p-1$ is even and $(6, p-1) \geq 2$. If $\text{ord}_7 10 \neq \phi(7)$ or $\text{ord}_p 10 \neq \phi(p)$ then $\text{ord}_7 10 \leq \phi(7)/2$ or $\text{ord}_p 10 \leq \phi(p)/2$, so that $\text{ord}_{7p} 10 = [\text{ord}_7 10, \text{ord}_p 10] = \text{ord}_7 10 \, \text{ord}_p 10 / (\text{ord}_7 10, \text{ord}_p 10) \leq \text{ord}_7 10 \, \text{ord}_p 10 \leq 6(p-1)/2 = 3(p-1)$. In either case, we have the period length bounded above by $3(p-1)$, as required.

3 marks. *Unseen.*

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 96 and so are irrelevant.

$p \rightarrow$ / $a \downarrow$	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	...	89	97	...
1	3	4	6	8	12	14	18	20	24	30	32	38	42	44	48	...	90	98	...
2	7	13	31	57	133														
3	15	40	156																
4	31	121																	
5	63																		
6	127																		

Now the following give all the ways of writing 96 as a product of entries in different columns of the table: $3 \cdot 4 \cdot 8$ or $3 \cdot 32$ or $4 \cdot 24$ or $8 \cdot 12$. These give

$n = 2^1 \cdot 3^1 \cdot 7^1$, $2^1 \cdot 31^1$, $3^1 \cdot 23^1$, $7^1 \cdot 11^1$, that is: $n = 42, 62, 69, 77$ are the only solutions to $\sigma(n) = 96$.

9 marks. *Seen similar on exercise sheet.*

(iii) Since $d(n) = (n_1+1)(n_2+1)\ldots$, the only way for $d(n) = 14$ is if there exists $n_j + 1 = 14$ and all other $n_i = 0$, or when there exist $n_j + 1 = 7, n_k + 1 = 2$ and all other $n_i = 0$. These correspond to n have the form: $n = p^{13}$ for some prime p, or $n = p^6 q^1$, for some distinct primes p, q. The smallest number of the first type is $2^{13} = 8192$. The smallest number of the second type is $2^6 3^1 = 192$. So, the smallest n such that $d(n) = 14$ is $n = 192$.

2 marks. *Seen similar on exercise sheet.*

(iv) Since $2^5, 3^3, p, q$ are coprime, we have:

$$\sigma(n) = \sigma(2^5)\sigma(3^3)\sigma(p)\sigma(q) = \frac{2^6-1}{2-1}\frac{3^4-1}{3-1}\frac{p^2-1}{p-1}\frac{q^2-1}{q-1} = 63 \cdot 40 \cdot (p+1)(q+1),$$

so that the given equation $\sigma(n) = 4n$ becomes: $63 \cdot 40 \cdot (p+1)(q+1) = 4 \cdot 2^5 \cdot 3^3 \cdot p \cdot q$. Dividing both sides by 72 then gives: $35(p+1)(q+1) = 48pq$. So, $35|48pq$, giving $35|pq$, since $(35, 48) = 1$. This imples: $5|pq$, so that $5|p$ or $5|q$; that is, either $p = 5$ or $q = 5$, since p, q are prime. Similarly, $7|pq$ and so $p = 7$ or $q = 7$, since p, q are prime. Since $p < q$, the only possibility is $p = 5, q = 7$ and indeed we see that these values of p, q do satisfy the equation $35(p+1)(q+1) = 48pq$, since both sides evaluate to 1680.

5 marks. *Seen similar on exercise sheet.*

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

Justification of a_0, a_1, a_2 as follows.

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

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

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

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

8 marks. *Seen similar on exercise sheet.*

(iii) $d = 3$ 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 $(\frac{p}{q}) = -(\frac{q}{p})$.

$(\frac{6}{79}) = (\frac{2}{79})(\frac{3}{79}) = (\frac{3}{79})$ [by (iii) since $79 \equiv -1 \pmod{8}$]
$= -(\frac{79}{3})$ [by QR, since 79 and 3 are $\equiv 3 \pmod{4}$]
$= -(\frac{1}{3}) = -1$ [since $1 \equiv 1^2 \pmod{3}$].

$(\frac{-11}{151}) = (\frac{-1}{151})(\frac{11}{151}) = -(\frac{11}{151})$ [by (ii), since $151 \equiv 3 \pmod{4}$]
$= (\frac{151}{11})$ [by QR, since 11 and 151 are $\equiv 3 \pmod{4}$]
$= (\frac{8}{11}) = (\frac{2}{11})^3 = (-1)^3$ [by (iii) since $11 \equiv 3 \pmod{8}$] $= -1$.

When $p \equiv 1 \pmod{4}$: $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (\frac{3}{p})$ [by (ii)] $= (\frac{p}{3})$ [by QR].

When $p \equiv 3 \pmod{4}$: $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = -(\frac{3}{p})$ [by (ii)] $= (\frac{p}{3})$ [by QR].

In all cases, we have $(\frac{-3}{p}) = (\frac{p}{3})$. Now, $0^2, 1^2, 2^2$ are $0, 1, 1$ mod 3, so that $0, 1$ are quadratic residues mod 3 but 2 is not. When $p \equiv 1 \pmod{3}$, we therefore get $(\frac{-3}{p}) = (\frac{p}{3}) = (\frac{1}{3}) = 1$. When $p \equiv 2 \pmod{3}$, we simlarly get $(\frac{-3}{p}) = (\frac{p}{3}) = (\frac{2}{3}) = -1$. The case $p \equiv 0 \pmod{3}$ can only happen when $p = 3$ and in this case $(\frac{-3}{p}) = 0$. In summary, $(\frac{-3}{p}) = 1 \iff p \equiv 1 \pmod{3}$.

7 marks. *Unseen.*