Solutions to 2MP62 May 1998 examination

1.
(i) $x \equiv 1 \bmod 4 \Longrightarrow x \equiv 1$ or 5 or $9 \bmod 12$. Working mod 12 the given congruences are satisfied precisely by
$x \equiv 0, 2, 4, 6, 8, 10$;
$x \equiv 0, 3, 6, 9$;
$x \equiv 1, 5, 9$;
$x \equiv 5, 11$;
$x \equiv 7$.
Since all possibilities mod 12 are included here, every x satisfies at least one of these congruences.
7 marks. Unseen, but straightforward.

(ii) There are several approaches to this one. Here is one. Since $p^n|x(x-2)$ we certainly have $p|x(x-2)$ and, by the standard property of primes ('$p|ab \Rightarrow\ p|a$ or $p|b$') we get $p|x$ or $p|(x-2)$.

Suppose $p|x$. Then we *cannot* have $p|(x-2)$ as well, since if $p|(x-2)$ then $p|(x-(x-2))$, i.e. $p|2$, which is false because we are given than p is an *odd* prime, i.e. $p > 2$.

Now use the standard fact: $p\not|a \Rightarrow (p^n, a) = 1$ (given in lectures). We get $(p^n, x-2) = 1$, and now we use

$$p^n|x(x-2), (p^n, x-2) = 1 \ \Rightarrow\ p^n|x.$$

(General, quotable fact from lectures: $a|bc, (a, b) = 1 \Rightarrow\ a|c$.)

Similarly, if $p|(x-2)$ then we deduce in succession $p\not|x, (p^n, x) = 1, p^n|(x-2)$. Hence

$$p^n|x(x-2) \Rightarrow\ p^n|x \text{ or } p^n|(x-2).$$

For the converse, note $p^n|x \Rightarrow p^n|x(x-2)$, since $x|x(x-2)$. Similarly $p^n|(x-2) \Rightarrow p^n|x(x-2)$.
7 marks. Unseen.

To solve $x^2 \equiv 2x \bmod 225 = 3^2 \cdot 5^2$ we start with:
$x^2 \equiv 2x \bmod 3^2 \cdot 5^2 \Longleftrightarrow x^2 \equiv 2x \bmod 3^2$ and mod 5^2,
since $(3^2, 5^2) = 1$. Now using the above result (3 and 5 being odd primes!) we get 4 cases:
(a) $x \equiv 0 \bmod 9$ and mod 25: $x \equiv 0 \bmod 225$.
(b) $x \equiv 2 \bmod 9$ and mod 25: $x \equiv 2 \bmod 225$.
(c) $x \equiv 0 \bmod 9$ and $x \equiv 2 \bmod 25$: substitute $x = 9k$ in the second congruence to get $9k \equiv 2 \bmod 25$. Now $9 \cdot 11 \equiv -1 \bmod 25$ so multiplying by -11 gives $k \equiv -22 \equiv 3 \bmod 25$. Thus $x = 9k \equiv 27 \bmod 225$.
(d) $x \equiv 2 \bmod 9$ and $x \equiv 0 \bmod 25$: substitute $x = 25k$ in the first congruence to get $25k \equiv 7k \equiv 2 \bmod 9$, so $k \equiv -1 \equiv 8 \bmod 9$, giving $x \equiv 200 \bmod 225$.
Hence the solutions are $x \equiv 0, 2, 27, 200 \bmod 225$.
6 marks. Unseen.

2.
(i) Suppose that $n = ab$ where $a > 1, b > 1$. Then

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

Now the first bracket here is > 1 since $a > 1$ and, if the second bracket were 1 then the first bracket would be $2^n - 1$, which implies $n = a$, i.e. $b = 1$: contradiction with $b > 1$. Thus $2^n - 1$ is composite, since it is the product of two factors both > 1.
5 marks. Seen on an exercise sheet.

(ii) n is a pseudoprime to base 2 means that n is composite and $2^n \equiv 2 \bmod n$.
We have $2^{10} \equiv 1 \bmod 11$, by Fermat's theorem (11 being prime) so $2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \bmod 11$. Similarly $2^{30} \equiv 1 \bmod 31$, since 31 is prime, so $2^{330} \equiv 1 \bmod 31$. Also, $2^{10} = (2^5)^2 = 32^2 \equiv 1^2 \equiv 1 \bmod 31$. It follows that $2^{340} = 2^{330}2^{10} = 1 \cdot 1 \equiv 1 \bmod 31$. Hence $2^{340} \equiv 1 \bmod 11$ and mod 31, hence mod $341 = 11 \cdot 31$, as 11 and 31 are primes. Hence $2^{341} \equiv 2 \bmod 341$. Of course 341 is composite since it is $11 \cdot 31$.
8 marks. Seen on an exercise sheet.

(iii) Assume that n is a pseudoprime to base 2, so that n is composite and $2^n \equiv 2 \bmod n$. The second of these, and $m - 1 = 2^n - 2$, immediately gives $n|(m-1)$. The same factorization as (i) shows that $m = (2^n - 1)|(2^{m-1} - 1)$, so that $2^{m-1} \equiv 1 \bmod m$. Thus $2^m \equiv 2 \bmod m$. That m is composite follows from the fact that n is composite and (i).
7 marks. Unseen.

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.
7 marks. From lectures.
Using the power algorithm to find 7^{24} (mod 25):
$7^1 \equiv 7$, $7^2 \equiv 24$, $7^4 \equiv 24^2 \equiv 1$, $7^8 \equiv 1^2 \equiv 1$, $7^{16} \equiv 1^2 \equiv 1$ (mod 25).
This gives, $7^{25-1} \equiv 7^{24} \equiv 7^8 \times 7^{16} \equiv 1$; the exponent 24 is even, so we continue to compute $7^{12} \equiv 7^4 \times 7^8 \equiv 1$; the exponent 12 is still even, so we continue to compute $7^6 \equiv 7^2 \times 7^4 \equiv 24 = 25 - 1$, and so we stop, with 25 passing Miller's test to base 7.
Using the power algorithm to compute 6^{34} (mod 35):
$6^1 \equiv 6$, $6^2 \equiv 1$, $6^4 \equiv 6^8 \equiv 6^{16} \equiv 6^{32} \equiv 1$ (mod 35).
So, $6^{34} \equiv 6^2 \times 6^{32} \equiv 1$; the exponent 34 is even so we continue to compute $6^{17} \equiv 6^1 \times 6^{16} \equiv 6$, which is neither 1 nor $35 - 1$ (mod 35). So, 35 fails Miller's test to base 6.
8 marks. Seen similar.

(ii) Miller's test starts with $2^{n-1} \equiv 1 \bmod n$. Here, $2^{n-1} = 2^{4p} = (2^p)^4 \equiv 1$ since $2^p \equiv 1 \bmod n$. Next, as the power $n - 1 = 4p$ is even, we look at $2^{\frac{n-1}{2}} = 2^{2p}$ which will be 1 for the same reason. The power $\frac{n-1}{2} = 2p$ is still even, so we look at $2^{\frac{n-1}{4}} = 2^p$, which is still 1 mod n. But now the power is p which is *odd* so we can't continue and n has passed Miller's test.
5 marks. Unseen.

4. (i) For $n \geq 1$ define $\phi(n)$ to be the number of integers x satisfying $1 \leq x \leq n$ and $(x, n) = 1$. If $n = p_1^{n_1} \dots p_k^{n_k}$ is the prime power decomposition of n (the p_i are distinct primes and each n_i is ≥ 1) then a formula for $\phi(n)$ is: $p_1^{n_1}(1 - \frac{1}{p_1}) \dots p_k^{n_k}(1 - \frac{1}{p_k})$, or: $p_1^{n_1-1}(p_1 - 1) \dots p_k^{n_k-1}(p_k - 1)$.
5 marks. From lectures.
$\phi(2 \times 7^2) = 1 \times 7 \times 6 = 2 \times 3 \times 7$. $\phi(2 \times 5 \times 17) = 1 \times 4 \times 16 = 2^6$, $\phi(2^4 \times 5 \times 257^5) = 2^3(2-1) \times 4 \times 257^4(257-1) = 2^{13}257^4$.
3 marks. Seen similar.
Suppose p is prime and $p^2|n$. Let the power of p dividing n be $s \geq 2$. Then the formula for $\phi(n)$ contains a factor $p^{s-1}(p-1)$ and since $s - 1 \geq 1$ this is divisible by p.
3 marks. Seen similar.

Suppose $\phi(n) = 2^k$. Then in the expression for $\phi(n)$ which is a product of terms $p^{s-1}(p-1)$ *all these terms* must be powers of 2. From the previous part there can be no odd primes p which satisfy $p^2|n$ (for that would give an odd factor to $\phi(n)$). So all the exponents s are 1 except possibly for that corresponding to $p = 2$. Furthermore if p is an odd prime dividing n then the factor $p - 1$ occurring in $\phi(n)$ must be a power of 2. Hence $p = 2^r + 1$ for some r. Hence n must have the form

$$n = 2^s q_1 q_2 \ldots q_m, \tag{1}$$

where the q_i are distinct primes of the form $2^r + 1, r \geq 1$.
4 marks. Unseen.

(ii) Now suppose that $\phi(n) = 2^{31}$. We want n to be odd so $s = 0$ in (1), and the only primes available to us are $p = 2^r + 1$ for $r = 1, 2, 4, 8, 16$. The product of the terms $p - 1$ has to be 2^{31}. Since $1 + 2 + 4 + 8 + 16 = 31$ the solution is

$$n = (2 + 1)(2^2 + 1)(2^4 + 1)(2^8 + 1)(2^{16} + 1).$$

However, if n is even, then we can make $t > 0$ in (1), which means that $\phi(n)$ receives a factor of 2^{s-1} from the 2^s in n. Examples of suitable n are
$n = 2^{17}(2^{16} + 1),\quad 2^{25}(2^8 + 1),\quad 2^{21}(2^4 + 1)(2^8 + 1)$. (or, of course, 2^{33}).
5 marks. Unseen.

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 $r_{j+1} \equiv 10^j$. { A formal induction argument would not be required in a simple case like this. } 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.

6. (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. Alternative Proof: For any x coprime to a, pair x with $a-x$; note that we never have $x = a-x$, since that would mean $a = 2x$ and so $x > 1$ and $(x, a) = (x, 2x) \geq x > 1$; this means that we have divided all positive integers coprime to a into pairs of distinct integers $x, a-x$; hence there are an even number of positive integers coprime to a; that is $\phi(a)$ is even, as required. [Either of these two proofs is acceptable]. 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 $\operatorname{lcm}(a, b)$, 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 $\phi(n)/2 \bmod n$, and so there does not exist g of order $\phi(n)$; that is, there does not exist a primitive root mod n.
8 marks. Bookwork

(iii) Working out powers of 7 mod 22 gives

k	1	2	3	4	5	6	7	8	9	10
7^k mod 22	7	5	13	3	21	15	17	9	19	1

This verifies that $\text{ord}_{22}7 = 10 = \phi(22)$ and so 7 is a primitive root mod 22 (in fact the values of k up to 5 do that since the order of 7 mod 22 must be a factor of $\phi(22) = 10$, and once it is > 5 it must then be 10.)
3 marks. Seen similar in exercises.

(a) From table, $19 \equiv 7^9, 17 \equiv 7^7 \pmod{22}$ and the given equation $19^x \equiv 17 \pmod{22}$ becomes

$$7^{9x} \equiv 7^7 \pmod{22} \Leftrightarrow 9x \equiv 7 \pmod{10}$$

by the general results that, for a primitive root g mod n: $g^a \equiv g^b \pmod{n} \Leftrightarrow a \equiv b \pmod{\phi(n)}$. This gives $x \equiv -7 \equiv 3 \bmod 10$.
3 marks. Seen similar in exercises.

(b) Note that $y^5 \equiv -1 \pmod{22}$ implies that $(y, 22) = 1$ since any common factor would have to divide the r.h.s. –1 of the congruence. Hence $y \equiv 7^x \pmod{22}$ for some x (since 7 is a primitive root). Also $7^5 \equiv -1$ from the table, hence *one* solution is $y \equiv 7$. The given congruence turns into

$$7^{5x} \equiv 7^5 \pmod{22} \Leftrightarrow 5x \equiv 5 \pmod{10}$$

by the same general results quoted in part (a). This gives $x \equiv 1 \bmod 2$, i.e. $x \equiv 1, 3, 5, 7, 9 \pmod{10}$ which, from the table, gives: $y \equiv 7, 13, 21, 17, 19 \bmod 22$.
4 marks. Seen similar in exercises.

7.
(i) $d(n)$ = number of $x \geq 1$ which are divisors of n.
$\sigma(n)$ = 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 $d(p^a) = a + 1$.
$\sigma(p^a) = 1 + p + p^2 + \ldots p^a = (p^{a+1} - 1)/(p - 1)$.
Writing $n = p_1^{n_1} \ldots p_k^{n_k}$ (prime power factorization),
$d(n) = (n_1 + 1) \ldots (n_k + 1)$ and

$$\sigma(n) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{n_k+1} - 1}{p_k - 1}.$$

4 marks. From lectures.

(ii) $d(n) = 15 = 3 \cdot 5$, so n must be of the form p^{14} or $p^2 q^3$ for primes p, q. The minimal possibilities for n are $2^{14}, 2^2 \cdot 3^4, 3^2 \cdot 2^4$ and clearly the smallest of these is $3^2 \cdot 2^4 = 144$.

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 72 and so are irrelevant.

$a \downarrow$ $p \rightarrow$	2	3	5	7	11	13	17	...	23	...	71
1	3	4	6	8	12	14	18	...	24	...	72
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 72 as a product of entries in different columns of the table: 72 or $6 \cdot 12$ or $4 \cdot 18$ or $3 \cdot 24$ or $3 \cdot 4 \cdot 6$. These give
$n = 71$ or $5 \cdot 11$ or $3 \cdot 17$ or $2 \cdot 23$ or $2 \cdot 3 \cdot 5$.
That is: $n = 71$ or 55 or 51 or 46 or 30.
8 marks. Seen similar in exercises.

(iii) $n = 2^3 \cdot p \cdot q$ where p and q are odd primes with $p < q$.
So $\sigma(n) = 15 \cdot (p + 1) \cdot (q + 1)$, the three factors of n being coprime in pairs.
Thus $\sigma(n) = 3n$ gives $15(p + 1)(q + 1) = 24pq$, i.e.
$15(p + q + 1) = 9pq$, i.e. $5(p + q + 1) = 3pq$.
Now comes the key step: 5 divides the l.h.s. of this equation, so must divide the r.h.s. But p and q are primes, so this implies $p = 5$ or $q = 5$. Putting $p = 5$ gives $5(q+6) = 15q$ so $q = 3 < p$, so in fact we must have $q = 5$, giving $p = 3$.

Note that it is *not* enough to 'spot the solution' $p = 3, q = 5$; the question asks it to be shown that this is the *only* solution, which is what is done above.
8 marks. Unseen.

8.
(i) Draw the following table, using the given formulae.

k	P_k	Q_k	x_k	a_k
0	0	1	$\sqrt{n}$	d
1	d	2	$\frac{d+\sqrt{n}}{2}$	d
2	d	1	$d + \sqrt{n}$	$2d$

5 marks

Justification of a_0, a_1, a_2 as follows.

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

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

$a_3 = [d+\sqrt{n}] = d + [\sqrt{n}] = d + d = 2d$.

3 marks

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

1 mark

The recurrence relations for p_k, q_k are:

$p_{k+1} = a_{k+1}p_k + p_{k-1}; q_{k+1} = a_{k+1}q_k + q_{k-1}$

which, together with the initial values:

$p_0 = a_0, q_0 = 1, p_1 = a_0a_1 + 1, q_1 = a_1$

defines all p_k, q_k, for $k \geq 0$.

2 marks

Taking $d = 5$ gives $n = 27$ i.e. $\sqrt{27} = [5, \overline{5, 10}]$.

k	a_k	p_k	q_k
0	5	5	1
1	5	26	5
2	10	265	51
3	5	1351	260

Using the identity $p_k^2 - nq_k^2 = (-1)^{k+1}Q_{k+1}$, we get two solutions: $x = 26, y = 5$ and $x = 1351, y = 260$.

4 marks

(ii) Draw the table:

k	P_k	Q_k	x_k	a_k
0	0	1	$\sqrt{m}$	$d-1$
1	$d-1$	$2d-2$	$\frac{d-1+\sqrt{m}}{2d-2}$	1
2	$d-1$	1	$d-1+\sqrt{m}$	$2d-2$

Justification of a_0, a_1, a_2 as follows.

$a_0 = [\sqrt{m}]$. But, for all $d \geq 2$, we have $d-1 \geq 1$ and so: $(d-1)^2 = d^2 - 2d + 1 = d^2 - 1 - 2(d-1) < d^2 - 1 < d^2$, giving: $d - 1 < \sqrt{d^2-1} < d$, so that $[\sqrt{m}] = d-1$, i.e. $a_0 = d-1$.

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

$a_3 = [d-1+\sqrt{m}] = d-1+[\sqrt{m}] = (d-1)+(d-1) = 2d-2$.

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

5 marks. Whole question similar to one in exercises.