Full Solutions
MATH312 December 2008

April 4, 2015

How to use this resource

- When you feel reasonably confident, simulate a full exam and grade your solutions. This document provides full solutions that you can use to grade your work.
- If you're not quite ready to simulate a full exam, we suggest you thoroughly and slowly work through each problem. To check if your answer is correct, without spoiling the full solution, we provide a pdf with the final answers only. Download the document with the final answers here.
- Should you need more help, check out the hints and video lecture on the Math Education Resources.

Tips for Using Previous Exams to Study: Exam Simulation

Resist the temptation to read any of the solutions below before completing each question by yourself first! We recommend you follow the guide below.

1. **Exam Simulation:** When you've studied enough that you feel reasonably confident, print the raw exam (click here) without looking at any of the questions right away. Find a quiet space, such as the library, and set a timer for the real length of the exam (usually 2.5 hours). Write the exam as though it is the real deal.
2. **Reflect on your writing:** Generally, reflect on how you wrote the exam. For example, if you were to write it again, what would you do differently? What would you do the same? In what order did you write your solutions? What did you do when you got stuck?
3. **Grade your exam:** Use the solutions in this pdf to grade your exam. Use the point values as shown in the original exam.
4. **Reflect on your solutions:** Now that you have graded the exam, reflect again on your solutions. How did your solutions compare with our solutions? What can you learn from your mistakes?
5. **Plan further studying:** Use your mock exam grades to help determine which content areas to focus on and plan your study time accordingly. Brush up on the topics that need work:
   - Re-do related homework and webwork questions.
   - The Math Education Resources offers mini video lectures on each topic.
   - Work through more previous exam questions thoroughly without using anything that you couldn't use in the real exam. Try to work on each problem until your answer agrees with our final result.
   - Do as many exam simulations as possible.

   Whenever you feel confident enough with a particular topic, move on to topics that need more work. Focus on questions that you find challenging, not on those that are easy for you. Always try to complete each question by yourself first.

This pdf was created for your convenience when you study Math and prepare for your final exams. All the content here, and much more, is freely available on the Math Education Resources.

This is a free resource put together by the Math Education Resources, a group of volunteers with a desire to improve higher education. You may use this material under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International licence.

Question 1 (a)

Solution. The answer is **false**. Let $a = 2, b = 1, c = 1$. Then $a \mid (b + c)$ but $a \nmid b$ or c.

Question 1 (b)

Solution. The answer is **false**. The number 2 is an even prime (the only even prime).

Question 1 (c)

Solution. The answer is **true**. Since $\gcd(a, 2) = 1$, we have that $\phi(2a) = \phi(2)\phi(a) = \phi(a)$ completing the proof.

Question 1 (d)

Solution 1. The answer is **false**
We try each combination for a

$$\begin{aligned}
4(0) &\equiv 0 \mod 10 \\
4(1) &\equiv 4 \mod 10 \\
4(2) &\equiv 8 \mod 10 \\
4(3) &\equiv 2 \mod 10 \\
4(4) &\equiv 6 \mod 10 \\
4(5) &\equiv 0 \mod 10 \\
4(6) &\equiv 4 \mod 10 \\
4(7) &\equiv 8 \mod 10 \\
4(8) &\equiv 2 \mod 10 \\
4(9) &\equiv 6 \mod 10
\end{aligned}$$

As we can see, we have two solutions given by $a \equiv 4, 9 \mod 10$ and so the statement is false.

Solution 2. The answer is **false**.
We isolate for 0 giving
$4a - 6 \equiv 2(2a - 3) \equiv 0 \mod 10$
Thus, we have that 10 divides $2(2a - 3)$ and so we are looking for a value of a such that $5 \mid (2a - 3)$. We quickly see that $a \equiv 4 \mod 5$ works. This lifts to two solutions modulo 10, namely $a \equiv 4, 9 \mod 10$ and this gives a contradiction.

Question 1 (e)

Solution. The statement is **false**
We seek a counter example and we take the smallest composite number for b, namely $b = 4$. We then take $a = 3$. Then
$3^{4-1} \equiv 3^3 \equiv 27 \equiv 3 \not\equiv 1 \mod 4$.
For a more enlightening proof, recall that by Euler's Theorem
$a^{\phi(b)} \equiv 1 \mod b$
Thus if we find a value of b where $\gcd(\phi(b), b-1) = 1$ we would be able to construct a counter example since in this case there are integers s and t such that
$s\phi(b) + (b - 1)t = 1$

and so choosing an a coprime to b between 2 and b-1 would give us that
$a \equiv a^{s\phi(b)+(b-1)t} = (a^{\phi(b)})^s(a^{b-1})^t \equiv 1 \mod b$
which would be a contradiction. This is what we did above.

Question 1 (f)

Solution. The answer is **false**.
Let $a = b = 2$ and $c = 1$. Then $\gcd(a, b, c) = \gcd(2, 2, 1) = 1$ and further
$\phi(abc) = \phi((2)(2)(1)) = \phi(4) = 2$.
However
$\phi(a)\phi(b)\phi(c) = \phi(2)\phi(2)\phi(1) = (1)(1)(1) = 1 \neq 2$
and thus this is a counter example.

Question 2 (a) i

Solution. We proceed directly.

$$\begin{aligned}
\frac{60!}{31!} &\equiv (60)(59)...(32) \mod 31 \\
&\equiv (29)(28)...(1) \mod 31 \\
&\equiv 29! \mod 31 \\
&\equiv 30! \cdot 30^{-1} \mod 31 \\
&\equiv (31-1)! \cdot (-1) \mod 31 \\
&\equiv (-1)(-1) \mod 31 \\
&\equiv 1 \mod 31
\end{aligned}$$

where in the second last line we used Wilson's Theorem. We also used the fact that
$30^{-1} \equiv (-1)^{-1} \equiv -1 \mod 31$.

Question 2 (a) ii

Solution. Immediately, we have
$\frac{59!}{30!} \equiv (59)(58)...(31) \equiv 0 \mod 31$

Question 2 (a) iii

Solution. The given problem is equivalent to $x^2 \equiv 4 \mod 5$. Testing all points gives

$$\begin{aligned}
0^2 &\equiv 0 \mod 5 \\
1^2 &\equiv 1 \mod 5 \\
2^2 &\equiv 4 \mod 5 \\
3^2 &\equiv 4 \mod 5 \\
4^2 &\equiv 1 \mod 5
\end{aligned}$$

and so the smallest admissible integer is $x \equiv 2 \mod 5$

Question 2 (a) iv

Solution. We first reduce the right hand side using Euler's Formula (or Fermat's Little Theorem). As $\gcd(3, 17) = 1$ and
$3^{\phi(17)} \equiv 3^{17-1} \equiv 3^{16} \equiv 1 \mod 17$
and hence

$$3^{162} \equiv 3^{160} \cdot 3^2 \equiv 9 \mod 17$$

Now, we have
$9x \equiv 9 \mod 17$
and thus, multiplying both sides by the inverse of 9 gives
$x \equiv 1 \mod 17$
(notice that we didn't need to compute this inverse, though if we wanted to the inverse is 2).

Question 2 (b)

Solution. Euler's theorem tells us that if $\gcd(a, 1000) = 1$ then
$a^{\phi(1000)} \equiv a^{\phi(8)\phi(125)} \equiv a^{4\cdot 100} \equiv a^{400} \equiv 1 \mod 1000$.
Thus, we have
$2009^{2012} \equiv 9^{1202} \equiv (9^{400})^3 9^2 \equiv 81 \mod 1000$
and so the last three digits are 081.

Question 3 (a)

Solution. Proceeding as suggested in the hint, we have
$3(7x - 2) \equiv 0 \mod 111$
Now, as $111 = 3 \cdot 37$, we see that we must have
$7x - 2 \equiv 0 \mod 37$
if the above congruence is to hold. Now, isolating gives
$7x \equiv 2 \mod 37$
We can crunch through the Euclidean algorithm to find the inverse of 7 but here I will use a clever time saving trick. The right hand side is equivalent to
$7x \equiv -35 \mod 37$
Thus, multiplying by the inverse of 7 on both sides yields
$x \equiv -5 \equiv 32 \mod 37$.
Thus, modulo 111, the solutions are
$x \equiv 32, 69, 106 \mod 111$
seen by adding multiples of 37 to 32.

Question 3 (b)

Solution. Proceeding as in the hints yields

$$\begin{aligned} x &\equiv -1 \mod 999 \\ x &\equiv -1 \mod 1000 \\ x &\equiv -1 \mod 1001 \end{aligned}$$

As

$$999 = 3^3 \cdot 37$$
$$1000 = 2^3 \cdot 5^3$$
$$1001 = 7 \cdot 11 \cdot 13$$

we see that all these moduli are coprime. Hence by the Chinese remainder theorem, we have that a unique solution is given by
$x \equiv -1 \mod 999 \cdot 1000 \cdot 1001$
or expanded and made positive
$x \equiv 999998999 \mod 999999000$

Question 3 (c)

SOLUTION. The conditions

$$x \equiv 3 \mod 6$$
$$x \equiv 1 \mod 10$$

give us that there is a positive integer s such that

$$x = 3 + 6s.$$

Substituting into the second equation yields

$$3 + 6s \equiv 1 \mod 10.$$

Isolating for 0 gives

$$2(3s + 1) \equiv 0 \mod 10.$$

Hence, we have that 5 must divide the term in the bracket, that is

$$3s + 1 \equiv 0 \mod 5$$

This gives

$$3s \equiv -1 \mod 5.$$

Multiplying both sides by 2 gives

$$s \equiv -2 \equiv 3 \mod 5.$$

Hence $s = 3 + 5t$ for some integer t. Thus,

$$x = 3 + 6s = 3 + 6(3 + 5t) = 3 + 18 + 30t = 21 + 30t$$

and hence all solutions are given by

$x \equiv 21 \mod 30$.

Question 4 (a)

Solution. We say that n is a pseudoprime to the base b if n is a composite integer and $b^n \equiv b \mod n$.

Question 4 (b)

Solution. We proceed using the hints. Clearly 1729 is square free so it suffices to check that for each prime divisor, we have that $(p-1) \mid (n-1)$. We proceed mechanically

$$\begin{aligned}(7-1) = 6 \mid 1728\\ (13-1) = 12 \mid 1728\\ (19-1) = 18 \mid 1728\end{aligned}$$

And all of these are true since $1728 = 12^3 = 2^6 3^3$. Hence 1729 is a Carmichael number.

Question 4 (c)

Solution. Assume towards a contradiction that 1729 is prime. Look at
$x^2 \equiv 1 \mod 1729$
If this were prime, we would have that the only two solutions to this equation are given by $x \equiv 1 \mod 1729$ and $x \equiv -1 \mod 1729$ (if you haven't seen this before, isolate for 0, factor and argue that because we've assumed that 1729 is prime, it has to divide one of the factors). However, notice that from the given congruences, we have that $2^{18} \not\equiv \pm 1 \mod 1729$ but
$(2^{18})^2 \equiv 2^{36} \equiv 1 \mod 1729$
and this is a contradiction. Hence 1729 is not prime.

Question 5 (a)

Solution. To compute the ciphertext given the plain text, one must compute
$P^e \mod n$
and in this case, we have
$101^{1189} \equiv 35 \mod 1271$
so the value of the ciphertext is $C = 35$. Note: You do not need to actually perform the above computation. It is given to us.

Question 5 (b)

Solution. We use the Euclidean algorithm to find an inverse. We do this with the numbers 1189 and $\phi(n) = \phi(1271) = \phi(31)\phi(41) = 30 \cdot 40 = 1200$.
This gives

$$\begin{aligned}1200 = 1189(1) + 11\\ 1189 = 11(108) + 1\end{aligned}$$

and back substituting gives

$$1 = 1189 - 11(108)$$
$$1 = 1189 - (1200 - 1189(1))(108)$$
$$1 = 1189(109) - 1200(108)$$

Hence the value of d can be chosen to be $d = 109$ since $1189(109) \equiv 1 \mod \phi(1271)$.

Question 5 (c)

Solution. Recall up to this point that Bob computed $C \equiv P^e \mod n$ and you've computed a d such that $ed \equiv 1 \mod \phi(n)$ so in fact, we have $ed = 1 + \phi(n)s$ for some integer s. Using Euler's Theorem, we can compute P back if we compute
$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+\phi(n)s} \equiv P(P^{\phi(n)})^s \equiv P \mod n$.
This is computable since Alice has both C and d available to her. This completes the proof.

Question 6 (a)

Solution. Proceed as in the hint given in the problem. Notice that
$$\phi(m) = \phi\left(\prod_{i=1}^{k} p_i^{e_i}\right) = \prod_{i=1}^{k} \phi\left(p_i^{e_i}\right)$$
holding since ϕ is multiplicative. Hence
$\phi(p_i^{e_i}) \mid \phi(m)$ and for simplicity, say $\phi(m) = \phi(p_i^{e_i})s$ for some integer s. Thus
$a^{\phi(m)} \equiv (a^{\phi(p_i^{e_i})})^s \equiv 1 \mod p_i^{e_i}$
where the last line holds by Euler's theorem since we are given in this question that $p_i \nmid a$ so $\gcd(a, p_i^{e_i}) = 1$.

Question 6 (b)

Solution. We prove the sub claims as outlines in the question.
Prove that $p_i^{e_i} \mid (m - \phi(m))$.
For this, we use the property of the phi function to see
$\phi(p_i^{e_i}) = p_i^{e_i}(1 - 1/p_i) = p_i^{e_i - 1}(p_i - 1)$
and thus by the multiplicativity of the phi function, we have
$$m - \phi(m) = \prod_{j=1}^{k} p_j^{e_j} - \prod_{j=1}^{k} p_j^{e_j - 1}(p_j - 1) = \prod_{j=1}^{k} p_j^{e_j - 1}(p_j - (p_j - 1)) = \prod_{j=1}^{k} p_j^{e_j - 1}$$
and hence $p_i^{e_i} \mid (m - \phi(m))$.
Prove that $m - \phi(m) \geq p_i^{e_i - 1}$.
The above shows that $m - \phi(m) = \prod_{j=1}^{k} p_j^{e_j - 1} \geq p_i^{e_i - 1}$ and this completes the proof.
Prove that $p_i^{e_i} \mid p_i^{m - \phi(m)}$ (here you may use without proof that $p_i^{e_i - 1} \geq e_i$.)
We have that
$p_i^{m-\phi(m)} \geq p_i^{p_i^{e_i - 1}} \geq p_i^{e_i}$.
Therefore,
$p_i^{e_i} \mid p_i^{m-\phi(m)}$.
We finish off this problem by noticing that
$p_i^{e_i} \mid p_i^{m-\phi(m)} \mid a^{m-\phi(m)}$.

Question 6 (c)

SOLUTION. We proceed in cases.
Case 1

$$p_i \nmid a$$

.
In this case, part (a) states that
$a^{\phi(m)} \equiv 1 \mod p_i^{e_i}$.
Since $\gcd(a, p_i^{e_i}) = 1$, the element above has an inverse showing that
$a^{-\phi(m)} \equiv 1 \mod p_i^{e_i}$.
Multiplying both sides by a^m yields
$a^{m-\phi(m)} \equiv a^m \mod p_i^{e_i}$.
which is what we wanted to show in this case.
Case 2

$$p_i \mid a$$

.
In part (b), we showed that
$p_i^{e_i} \mid a^{m-\phi(m)}$
Since
$a^{m-\phi(m)} \mid a^m$
We also have that
$p_i^{e_i} \mid a^m$
and hence that
$p_i^{e_i} \mid (a^m - a^{m-\phi(m)})$.

Question 6 (d)

SOLUTION. Notice that parts (a) to (c) held for an arbitrary prime factor of m. We repeat the above for each such prime factor. Since they are all distinct primes, the fact that
$p_i^{e_i} \mid (a^m - a^{m-\phi(m)})$
holds for each $i \in \{1, .., k\}$ will together imply that via the Chinese Remainder Theorem
$m = \prod_{i=1}^{k} p_i^{e_i} \mid (a^m - a^{m-\phi(m)})$
and this completes the proof.

Good Luck for your exams!