Full Solutions
MATH312 December 2012

April 16, 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. We seek to solve the system of congruences given by

$$\begin{aligned} x &\equiv 3 \mod 5 \\ x &\equiv 4 \mod 7 \end{aligned}$$

The first equality says that $x = 3+5s$. Plugging into the second yields $3+5s \equiv 4 \mod 7$. Simplifying yields $5s \equiv 1 \mod 7$.
We can find the inverse of 5 by using the Euclidean algorithm however since we are modulo 7, there is only 6 possible candidates so it is faster to just try them all. Since $5 \cdot 3 \equiv 15 \equiv 1 \mod 7$, we see that $s \equiv 3 \mod 7$. This is the same as $s = 3+7t$. Back substituting gives $x = 3+5(3+7t) = 18+35t$. So two possible answers are given by 18 and 53.

Question 1 (b)

Solution. As stated in the hint, the given problem is equivalent to
$999 \equiv 0 \mod m$
Thus m must be a divisor of 999. We can factor 999 as
$999 = 3^2 \cdot 111 = 3^3 37$.
Thus, the divisors are $1, 3, 9, 27, 37, 111, 333, 999$ and these are the potential m values.

Question 1 (c)

Solution. From the hint, we immediately see that

$$\begin{aligned} 1!+2!+3!+4!+5!+\ldots+100! &\equiv 1!+2!+3!+4! \mod 10 \\ &\equiv 1+2+6+24 \mod 10 \\ &\equiv 3 \mod 10 \end{aligned}$$

Question 1 (d)

Solution. Following the hint, we compute
$8-1+2-9+4-3+5-8+X = X-2$
and thus if X is 2, this sum will be 0 and hence the number will be divisible by 11. Next, we see that
$8+1+2+9+4+3+5+8+X = 40+X$
and thus if X is 5, this sum will be divisible by 9 and hence so will the original number. Lastly, to be divisible by 4, we need the last two digits to be divisible by 4 so if X is one of 0,4, or 8, then this condition is satisfied and the number will be divisible by 4.

Question 1 (e)

Solution. Following the hint, we compute the inverse of 7 modulo 13. Then

$$\begin{aligned} 13 &= 7(1)+6 \\ 7 &= 6(1)+1 \end{aligned}$$

and back substituting gives $1 = 7 - 6(1) = 7 - (13 - 7(1)) = 7(2) - 13$.
Thus, the inverse of 7 modulo 13 is 2. Hence $x \equiv 2(7)x \equiv 2(4) \equiv 8 \mod 13$ which completes the question.

Question 1 (f)

Solution. A Carmichael number is a composite number n which satisfies
$b^{n-1} \equiv 1 \mod n$
for all integers with $\gcd(b, n) = 1$.
For 561, we use Korselt's criterion which states that for each prime dividing n, we must check that $(p-1) \mid (n-1)$. Since
$561 = 3 \cdot 11 \cdot 17$
we check that

$$(3-1) = 2 \mid 560$$
$$(11-1) = 10 \mid 560$$
$$(17-1) = 16 \mid 560$$

valid since $560 = 2^4 \cdot 5 \cdot 7$. Thus 561 is a Carmichael number.

Question 1 (g)

Solution. We proceed by the hint.

$$5^{16} \equiv (5^2)^8 \equiv 25^8 \equiv 2^8 \equiv 256 \equiv 26 \equiv 3 \mod 23$$

Question 2 (a)

Solution. The answer is **true**.
Suppose that n has at least two distinct prime divisors p and q. Then it has at least 4 positive divisors given by $1, p, q, pq$. Thus n must only have one prime divisor, so must be of the form $n = p^\alpha$. In this case, n has exactly $\alpha + 1$ positive divisors, namely, p^β for $\beta = 0, 1, 2, \ldots, \alpha$. Thus if $\alpha + 1 = 3$ we have that $\alpha = 2$ which is as claimed in the question.

Question 2 (b)

Solution 1. We compute directly
$5^7 \equiv 5 \cdot 5^6 \equiv 5 \cdot (25)^3 \equiv 5 \cdot 4^3 \equiv 5 \cdot 64 \equiv 5 \cdot (-12) \equiv -60 \equiv 16 \not\equiv 1 \mod 19$
and so 7 is not the order of 5.

Solution 2. We compute directly
$5^7 \equiv 5 \cdot 5^6 \equiv 5 \cdot (25)^3 \equiv 5 \cdot 4^3 \equiv (5 \cdot 4) \cdot 4^2 \equiv 20 \cdot 16 \equiv 1 \cdot 16 \not\equiv 1 \mod 19$
and so 7 is not the order of 5.

Question 2 (c)

Solution. The answer is **true**.

Recall that 7 passes Miller's test if
$7^d \equiv 1 \mod 25$
or the following holds for some r
$7^{2^r d} \equiv -1 \mod 25$
where $25 - 1 = 24 = 2^s d = 2^8 \cdot 3$ and $0 \leq r \leq s - 1$. If 7 passes the test, then 25 is a probable prime. If it fails the test, then the number is not prime.
So we check manually:

$$7^3 \equiv 49 \cdot 7 \equiv -1 \cdot 7 \not\equiv 1 \mod 25$$
$$7^{2 \cdot 3} \equiv 49^3 \equiv (-1)^3 \equiv -1 \mod 25$$

Thus, 7 passes Miller's test. (Note that 25 is not prime but still 7 passes Miller's test).

Question 2 (d)

Solution. The answer is **true**
From Fermat's Little Theorem, we have
$2^6 \equiv 1 \mod 7$
and hence
$2^{39} \equiv (2^6)^6 \cdot 2^3 \equiv (1)^6 \cdot 8 \equiv 8 \equiv 1 \mod 7$
Thus 7 divides $2^{39} - 1$.

Question 3

Solution. As displayed in the hints, it suffices to compute the values of n for which
$\left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + ... + \left\lfloor \frac{n}{5^{\lfloor \log_5(n) \rfloor}} \right\rfloor = 74.$
Clearly for $n = 400$, we have that the first term in the above sum is 80 so it suffices to look smaller than this value. This reduces the above sum to
$\left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + \left\lfloor \frac{n}{5^3} \right\rfloor = 74$
We start with the value $n = 200$.
$\left\lfloor \frac{200}{5} \right\rfloor + \left\lfloor \frac{200}{5^2} \right\rfloor + \left\lfloor \frac{200}{5^3} \right\rfloor = 40 + 8 + 1 = 49.$
Trying $n = 300$ yields
$\left\lfloor \frac{300}{5} \right\rfloor + \left\lfloor \frac{300}{5^2} \right\rfloor + \left\lfloor \frac{300}{5^3} \right\rfloor = 60 + 12 + 2 = 74.$
That is an exact match and further we know that $n = 299$ makes the above sum less than 74. Notice that increasing the above sum from 300 to 301,302,303 or 304 does not increment any of the terms but at 305, the first summand increases by 1. Thus the five possible values are
$n \in \{300, 301, 302, 303, 304\}$
completing the question.

Question 4

Solution. First,
$\sigma(n) = \sum_{d|n} d$
and
$\tau(n) = \sum_{d|n} 1$
gives the required definitions.

For the last part, we proceed by a contradiction and suppose that $\phi(n) = 14$ for some integer n.
As stated in the hint, we have
$\phi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right) = \prod_{p^\alpha \| n} p^{\alpha_p - 1}(p-1) = 14.$
where $n = \prod p^{\alpha_p}$. Now every odd prime present in the factorization of n contributes a power of two to $\phi(n)$ due to the $(p-1)$ factor. Thus, there can be at most one odd prime dividing n, say p.
If p occurs to a power of two, then because it divides the left hand side, it must divide 14 and so must be 7. The prime p cannot occur to a third power or higher since otherwise there are two factors of p on the left and at most one on the right. However $\phi(7^2) = 42 > 14$ and so the power must be 1. Thus $n = 2^\alpha p$ for some α. Notice that as the phi-function is multiplicative, we have that
$14 = \phi(n) = \phi(2^\alpha)\phi(p) = 2^{\alpha-1}(p-1)$
(or we have that $\phi(n) = p - 1$ if no power of 2 divides n)
Thus, as $p - 1$ is even, we have that $\alpha = 1$ (or n is odd) and further that $p = 15$ which is not a prime. This is a contradiction and hence this equation has no solution.

Question 5

SOLUTION. Euler's Theorem states that

$$a^{\phi(b)} \equiv 1 \mod b$$
$$b^{\phi(a)} \equiv 1 \mod a$$

Translating the above, there exist integers s and t such that

$$a^{\phi(b)} - 1 = bs$$
$$b^{\phi(a)} - 1 = at$$

Taking the products of the left hand sides of the equation and the right hand sides of the equation yields (below we have flipped the sides of the equations)

$$abst = (a^{\phi(b)} - 1)(b^{\phi(a)} - 1) = a^{\phi(b)}b^{\phi(a)} - a^{\phi(b)} - b^{\phi(a)} + 1$$

As $\phi(a)$ and $\phi(b)$ are at least one, we have that

$$0 \equiv -a^{\phi(b)} - b^{\phi(a)} + 1 \mod ab$$

and hence we get the required result. For the last part, we have
$5^8 \equiv (5^2)^4 \equiv 25^4 \equiv 9^4 \equiv (9^2)^2 \equiv 81^2 \equiv 1^2 \equiv 1 \mod 16$
(or easier, notice that $\phi(16) = 8$ so Euler's theorem gives the same result) Thus as the number is 1, its inverse it itself.

Good Luck for your exams!

Free under CC-BY-NC-SA by the Math Education Resources.