Full Solutions
MATH312 December 2013

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.

Question 1 (a)

SOLUTION. **THIS QUESTION HAS NOT YET BEEN REVIEWED! THE SOLUTION BELOW MAY CONTAIN MISTAKES!**

The inverse of an integer a is defined as an integer a^{-1} such that $aa^{-1} \equiv 1 \mod m$. This integer turns out to be unique modulo m.

Question 1 (b)

SOLUTION. **THIS QUESTION HAS NOT YET BEEN REVIEWED! THE SOLUTION BELOW MAY CONTAIN MISTAKES!**

We proceed using the Euclidean algorithm. We notice that

$$\begin{aligned}19 &= 16(1) + 3\\16 &= 3(5) + 1\end{aligned}$$

Back substituting, we get

$$\begin{aligned}1 &= 16 + 3(-5)\\1 &= 16 + (19 + 16(-1))(-5)\\1 &= 16(6) + 19(-5)\end{aligned}$$

and so the inverse of 16 is 6. Using this, we have

$$\begin{aligned}16x &\equiv 2 \mod 19\\6(16)x &\equiv 6(2) \mod 19\\x &\equiv 12 \mod 19\end{aligned}$$

Question 2 (a)

SOLUTION. **THIS QUESTION HAS NOT YET BEEN REVIEWED! THE SOLUTION BELOW MAY CONTAIN MISTAKES!**

We follow the solution as outlined in the hints. Notice that reducing the given equation modulo 5 and 11 gives the system of congruences

$$\begin{aligned}x^2 &\equiv 1 \mod 5\\x^2 &\equiv 1 \mod 11\end{aligned}$$

Solving these gives

$$\begin{aligned}x &\equiv 1, 4 \mod 5\\x &\equiv 1, 10 \mod 11\end{aligned}$$

As 5 and 11 are coprime, we may apply the Chinese remainder theorem. The above congruences can be solved as follows. For the case

$$x \equiv 1 \mod 5$$

we see that there is an integer m such that $x = 1 + 5m$. If we further suppose that

$$x \equiv 1 \mod 11$$

we can see by combining these two equations that $1 \equiv x \equiv 1 + 5m \mod 11$ and so we see that $m \equiv 0 \mod 11$. Writing $m = 11n$ for some integer n, we have that
$x = 1 + 5m = 1 + 5(11n) = 1 + 55n$
and reducing modulo 55 yields $x \equiv 1 \mod 55$. If instead in the second congruence we suppose that

$$x \equiv 10 \mod 11$$

we have that $10 \equiv x \equiv 1 + 5m \mod 11$ and so we see that $5m \equiv 9 \mod 11$. Multiplying both sides by *-2* gives $m \equiv -10m = -18 \equiv 4 \mod 11$ and so $m = 4 + 11n$ for some integer n. Hence, we have that
$x = 1 + 5m = 1 + 5(4 + 11n) = 21 + 55n$
and reducing modulo 55 yields $x \equiv 21 \mod 55$.
Now we go back to the first congruence and use instead the congruence given by

$$x \equiv 4 \mod 5$$

we see that there is an integer m such that $x = 4 + 5m$. If we further suppose that

$$x \equiv 1 \mod 11$$

we can see by combining these two equations that $1 \equiv x \equiv 4 + 5m \mod 11$ and so we see that $5m \equiv 8 \mod 11$. Multiplying by -2 on both sides yields $m \equiv -10m \equiv -16 \equiv 6 \mod 11$. Writing $m = 6 + 11n$ for some integer n, we have that
$x = 4 + 5m = 4 + 5(6 + 11n) = 34 + 55n$
and reducing modulo 55 yields $x \equiv 34 \mod 55$. If instead in the second congruence we suppose that

$$x \equiv 10 \mod 11$$

we have that $10 \equiv x \equiv 4 + 5m \mod 11$ and so we see that $5m \equiv 6 \mod 11$. Multiplying both sides by *-2* gives $m \equiv -10m = -12 \equiv 10 \mod 11$ and so $m = 10 + 11n$ for some integer n. Hence, we have that
$x = 4 + 5m = 4 + 5(10 + 11n) = 54 + 55n$
and reducing modulo 55 yields $x \equiv 21 \mod 55$. Thus, the complete set of solutions is given by
$x \equiv 1, 21, 34, 54 \mod 55$

Question 2 (b)

SOLUTION. No content found.

Question 3 (a)

SOLUTION. **THIS QUESTION HAS NOT YET BEEN REVIEWED! THE SOLUTION BELOW MAY CONTAIN MISTAKES!**

The Euler $\phi(n)$ function counts the number of coprime integers to the parameter n from 1 to the parameter n. Remember that here two integers m and n are coprime if $\gcd(m, n) = 1$.

Question 3 (b)

SOLUTION. No content found.

Question 4 (a)

SOLUTION. No content found.

Question 4 (b)

SOLUTION. No content found.

Question 5 (a)

SOLUTION. No content found.

Question 5 (b)

SOLUTION. **THIS QUESTION HAS NOT YET BEEN REVIEWED! THE SOLUTION BELOW MAY CONTAIN MISTAKES!**

Assume towards a contradiction that such an x exists. Order of x is 4. FLT states that $x^{p-1} \equiv 1 \mod p$. GCD of elements is 2. Thus $x^2 \equiv 1 \mod p$ which is a contradiction.

Question 6 (a)

SOLUTION. No content found.

Question 6 (b)

SOLUTION. No content found.

Question 7 (a)

SOLUTION. No content found.

Question 7 (b)

SOLUTION. No content found.

Good Luck for your exams!