Full Solutions
MATH312 December 2010

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

Solution. Proceed by contradiction. Suppose that there exist integers x and y such that $px = 8n+3$ and $py = 5n+2$. Multiplying the first by 5 and the second equation by 8 gives

$$5px = 40n + 15$$
$$8py = 40n + 16$$

subtracting the two equations gives $p(8y - 5x) = 1$ and as p is prime, it divides the left hand side but not the right hand side which is a contradiction. Hence no such prime number can exist.

Question 2

Solution. Proceeding as stated in the hint, notice that the sum of the digits of a is
$(8+5)n = 13 \cdot 3^{100}$
and this is clearly divisible by 9. Thus a is divisible by 9. Further, the alternating sum of the digits is
$(8-5)n = 3 \cdot 3^{100} = 3^{101}$
and this is clearly not divisible by 11. Thus a is not divisible by 11.

Question 3

Solution. We proceed as in the hints. Modulo 8, we have that if a is even, then the residue of this number is 0 modulo 8. If it is odd, then Euler's Theorem tells us that since $\phi(8) = 8(1-1/2) = 4$, we have
$a^{100} = (a^4)^{25} = (a^{\phi(8)})^{25} \equiv 1^{25} \equiv 1 \mod 8$
Similarly, modulo 125 we have that if 5 divides a, then the residue is 0 and otherwise, Euler's Theorem tells us that since $\phi(125) = 5^3(1-1/5) = 100$, we have
$a^{100} = a^{\phi(125)} \equiv 1 \mod 125$
This gives us four possible systems. Either

$$\begin{aligned}
a^{100} &\equiv 0 \mod 8 \quad \text{and} \quad a^{100} \equiv 0 \mod 125 \\
a^{100} &\equiv 1 \mod 8 \quad \text{and} \quad a^{100} \equiv 0 \mod 125 \\
a^{100} &\equiv 0 \mod 8 \quad \text{and} \quad a^{100} \equiv 1 \mod 125 \\
a^{100} &\equiv 1 \mod 8 \quad \text{and} \quad a^{100} \equiv 1 \mod 125
\end{aligned}$$

As 8 and 125 are coprime, we have via the Chinese Remainder Theorem that there exists a unique solution to each of these system of equations modulo 1000 (the product of 8 and 125). We break this down into cases.
Case 1: $a^{100} \equiv 0 \mod 8$ and $a^{100} \equiv 0 \mod 125$. This case occurs when 10 divides a. In this case, by inspection, we can see that the last three digits here are given by 000 since 0 is the unique solution to this system.
Case 2: $a^{100} \equiv 1 \mod 8$ and $a^{100} \equiv 0 \mod 125$. This occurs when a is odd and divisible by 5. In this case, we have that $a^{100} = 1 + 8s$ and so $1 + 8s \equiv 0 \mod 125$. The inverse of 8 modulo 125 is given by the Euclidean algorithm:

$$\begin{aligned}
125 &= 8(15) + 5 \\
8 &= 5(1) + 3 \\
5 &= 3(1) + 2 \\
3 &= 2(1) + 1
\end{aligned}$$

and back substituting gives

$$
\begin{aligned}
1 &= 3 - 2(1) \\
1 &= 3 - (5 - 3(1))(1) \\
1 &= 3(2) - 5(1) \\
1 &= (8 - 5(1))(2) - 5(1) \\
1 &= 8(2) - 5(3) \\
1 &= 8(2) - (125 - 8(15))(3) \\
1 &= 8(47) - 125(3)
\end{aligned}
$$

so the inverse is 47. Thus

$$
\begin{aligned}
8s &\equiv -1 \mod 125 \\
8(47)s &\equiv -47 \mod 125 \\
s &\equiv 125 - 47 \mod 125 \\
s &\equiv 78 \mod 125
\end{aligned}
$$

so $s = 78 + 125t$. Thus recalling that $a^{100} = 1 + 8s$ we have that
$a^{100} = 1 + 8(78 + 125t) = 1 + 624 + 1000t = 625 + 1000t$
and so the last 3 digits are 625 in this case.
Case 3: $a^{100} \equiv 0 \mod 8$ and $a^{100} \equiv 1 \mod 125$. This occurs when a is even and not divisible by 5. In this case, we have that $a^{100} = 8s$ and so $8s \equiv 1 \mod 125$. The inverse of 8 modulo 125 as computed above is 47. Thus $s \equiv 47 \mod 125$ and hence $s = 47 + 125t$. Thus recalling that $a^{100} = 8s$ we have that
$a^{100} = 8s = 8(47 + 125t) = 376 + 1000t$
and so the last 3 digits are 376 in this case.
Case 4: $a^{100} \equiv 1 \mod 8$ and $a^{100} \equiv 1 \mod 125$. This occurs when a is odd and not divisible by 5. In this case, we have that $a^{100} = 1 + 8s$ and so $1 + 8s \equiv 1 \mod 125$. The inverse of 8 modulo 125 as computed above is 47. Thus $s \equiv 0 \mod 125$ and hence $s = 0 + 125t$. Thus recalling that $a^{100} = 1 + 8s$ we have that
$a^{100} = 1 + 8s = 1 + 8(0 + 125t) = 1 + 1000t$
and so the last 3 digits are 001 in this case. This completes all cases.

Question 4

SOLUTION. Start off by using the Fundamental Theorem of Arithmetic to write
$n = \prod_{i=1}^{n} p_i^{\alpha_i}$
Then the number of divisors of n is
$d = \prod_{i=1}^{n} (\alpha_i + 1)$
To see this, notice that each prime factor has $\alpha_i + 1$ choices of occurring in the divisor of n (either you do not select the divisor or you select the divisor and some power of it). As d is given to be 77, and 77 has only the prime factors 7 and 11, we see that there can only be two nontrivial terms in the expansion of d. Thus only two of these divisors can be prime.

Question 5

SOLUTION. We begin by noting that
$2 \cdot 11 = 22 = \phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \frac{p-1}{p} = \prod_{p_i^{\alpha_i} \| n} p_i^{\alpha_i - 1}(p-1)$

where above we used the Fundamental Theorem of Arithmetic to write (recall that $\|$ means *fully divides*) $n = \prod_{p_i^{\alpha_i} \| n} p_i^{\alpha_i}$.
Our *main equation* of discussion will be
$2 \cdot 11 = \prod_{p_i^{\alpha_i} \| n} p_i^{\alpha_i - 1}(p_i - 1)$.
We proceed in cases. First we discuss the powers of 2 in n.
Case 1

$$8 \mid n$$

. In this case, notice that 4 divides the right hand side of the main equation but only 2 divides the left hand side. This is a contradiction.
Case 2

$$4 \| n$$

. In this case, notice that 2 divides the right hand side of the main equation and 2 divides the left hand side. However, if another odd prime divides n, then the right hand side is divisible by an extra power of 2 which is a contradiction. The remaining subcase in this case is if no odd primes divde n, that is, $n = 4$. But since also $\phi(4) = 2 \neq 22$ this case cannot occur.
"'Case 3

$$2 \| n$$

or n is odd"'. In either of these cases, since ϕ is multiplicative and as $\phi(2) = 1$, we have that either of these cases can occur, that is, if $\phi(n) = 22$, then $\phi(2n) = 22$. Therefore, without loss of generality, we suppose 2 does not divide n.
Now we deal with the odd primes. Notice that for each odd prime, we get a factor of 2 on the right hand side of the main equation. Thus only exactly one odd prime can occur. Thus $n = p^{\alpha}$. Since only 2 and 11 occur as prime factors on the left hand side of the equation, we know that we must have that $\alpha \leq 2$ (the right hand side of the main equation has an $p^{\alpha-1}$ term so the factor could be 2). If $\alpha = 2$, then the prime p in question must be 11 since p divides the right hand side. So $n = 11^2$ but this is inadmissable since $\phi(11^2) \neq 22$. Thus n is a prime. For primes, we have that $\phi(p) = p - 1$. This value we know is 22 and so $n = 23$.
Thus combining the two discussions shows us that either $n = 23$ or $n = 46$ completing the question.

Question 6

SOLUTION. For part (a), we seek to solve the system of congruences given by

$$\begin{aligned} 5 &\equiv 4a + b \mod 26 \\ 6 &\equiv 19a + b \mod 26 \end{aligned}$$

Subtracting the two equations yields

$$1 \equiv 15a \mod 26$$

Thus we need to find the inverse of 15 modulo 26. To do this we use the Euclidean Algorithm.

$$\begin{aligned} 26 &= 15(1) + 11 \\ 15 &= 11(1) + 4 \\ 11 &= 4(2) + 3 \\ 4 &= 3(1) + 1 \end{aligned}$$

and back substituting gives

$$\begin{aligned}
1 &= 4 - 3(1) \\
1 &= 4 - (11 - 4(2))(1) \\
1 &= 4(3) - 11(1) \\
1 &= (15 - 11(1))(3) - 11(1) \\
1 &= 15(3) - 11(4) \\
1 &= 15(3) - (26 - 15(1))(4) \\
1 &= 15(7) - 26(4)
\end{aligned}$$

and so an inverse of 15 modulo 26 is given by 7. Thus as $1 \equiv 15a \mod 26$, we have that $7 \equiv a \mod 26$. Plugging back into the original equation gives $5 \equiv 4a + b \equiv 4(7) + b \mod 26$ and isolating for b gives the value of 3 and so the encryption key is $K_E = (26, 7, 3)$
For part (b), we seek to solve

$$\begin{aligned}
4 &\equiv 5c + d \mod 26 \\
19 &\equiv 6c + d \mod 26
\end{aligned}$$

Subtracting these two equations gives $15 \equiv c \mod 26$. Thus as $4 \equiv 5c + d \equiv 5(15) + d \equiv 75 + d \equiv -3 + d \mod 26$ (so d is 7), we have that the decryption key is given by $K_D = (26, 15, 7)$.

Question 7

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

As stated in the hint, we seek to find a value of d such that
$ed \equiv 1 \mod \phi(n)$
Notice that $\phi(n) = \phi(85) = \phi(5 \cdot 17) = \phi(5)\phi(17) = 4(16) = 64$. So we need to solve
$7d \equiv 1 \mod 64$.
To do this, we use the Euclidean Algorithm.

$$64 = 7(9) + 1$$

Here we are immediately done and so multiplying both sides above by -9 yields $d \equiv -9 \equiv 55 \mod 64$.

Question 8

Solution. By Fermat's Little Theorem, we have that
$x^{52578} \equiv 1 \mod 52579$.
The given problem tells us that
$x^5 \equiv 1 \mod 52579$
Using the Euclidean Algorithm, we can find integers a and b such that
$5a + 52578b = \gcd(52578, 5) = 1$.
Thus we have that
$x \equiv x^{5a+52578b} \equiv x^{5a}x^{52578b} \equiv (x^5)^a(x^{52578})^b \equiv 1 \mod 52579$
and this completes the proof. The other property that we used about 52579 is that 52578 and 5 are coprime.

Good Luck for your exams!

