Final answers script in beta

Final Answers
MATH312 December 2008

April 16, 2015

How to use this resource

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

Tips for Using Previous Exams to Study: Work through problems

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

1. **How to use the final answer:** *The final answer is not a substitution for the full solution!* The final answer alone will not give you full marks. The final answer is provided so that you can check the correctness of your work without spoiling the full solution.
   - To answer each question, only use what you could also use in the exam. Download the raw exam here.
   - If you found an answer, how could you verify that it is correct from your work only? E.g. check if the units make sense, etc. Only then compare with our result.
   - If your answer is correct: good job! Move on to the next question.
   - Otherwise, go back to your work and check it for improvements. Is there another approach you could try? If you still can't get to the right answer, you can check the full solution on the Math Education Resources.
2. **Reflect on your work:** Generally, reflect on how you solved the problem. Don't just focus on the final answer, but whether your mental process was correct. If you were stuck at any point, what helped you to go forward? What made you confident that your answer was correct? What can you take away from this so that, next time, you can complete a similar question without any help?
3. **Plan further studying:** Once 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. Once you are ready to tackle a full exam, follow the advice for the full exam (click here).

Please note that all final answers were extracted automatically from the full solution. It is possible that the final answer shown here is not complete, or it may be missing entirely. In such a case, please notify `mer-wiki@math.ubc.ca`. Your feedback helps us improve.

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 that turn their desire to improve education into practice. You may use this material under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International licence.

Question 1 (a)

FINAL ANSWER. Then $a \mid (b+c)$ but $a \nmid b$ or c.

Question 1 (b)

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

Question 1 (c)

FINAL ANSWER. Since $\gcd(a,2)=1$, we have that $\phi(2a)=\phi(a)$ completing the proof.

Question 1 (d)

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

Question 1 (e)

FINAL ANSWER. $a \equiv a^{s\phi(b)+(b-1)t} = (a^{\phi(b)})^s (a^{b-1})^t \equiv 1 \mod b$which would be a contradiction.This is what we did above.

Question 1 (f)

FINAL ANSWER. $\phi(a)\phi(b)\phi(c) = 1 \neq 2$and thus this is a counter example.

Question 2 (a) iii

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

Question 2 (a) ii

FINAL ANSWER. $\frac{59!}{30!} \equiv (59)(58)...(31) \equiv 0 \mod 31$

Question 2 (a) i

FINAL ANSWER. $30^{-1} \equiv (-1)^{-1} \equiv -1 \mod 31$.

Question 2 (a) iv

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

$x \equiv 1 \mod 17$(notice that we didn't need to compute this inverse, though if we wanted to the inverse is 2).

Question 2 (b)

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

$2009^{2012} \equiv 9^{1202} \equiv (9^{400})^3 9^2 \equiv 81 \mod 1000$and so the last three digits are 081.

Question 3 (a)

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

$x \equiv 32, 69, 106 \mod 111$seen by adding multiples of 37 to 32.

Question 3 (b)

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

$x \equiv 999998999 \mod 999999000$

Question 3 (c)

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

$x \equiv 21 \mod 30$.

Question 4 (a)

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

$b^n \equiv b \mod n$.

Question 4 (b)

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

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

Question 4 (c)

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

$(2^{18})^2 \equiv 2^{36} \equiv 1 \mod 1729$and this is a contradiction.Hence 1729 is not prime.

Question 5 (a)

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

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)

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

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

Question 5 (c)

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

This is computable since Alice has both C and d available to her.This completes the proof.

Question 6 (a)

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

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)

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

$p_i^{e_i} \mid p_i^{m-\phi(m)} \mid a^{m-\phi(m)}$.

Question 6 (c)

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

$p_i^{e_i} \mid (a^m - a^{m-\phi(m)})$.

Question 6 (d)

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

$m = \prod_{i=1}^{k} p_i^{e_i} \mid (a^m - a^{m-\phi(m)})$and this completes the proof.