Full Solutions
MATH312 December 2005

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.

Question 1

SOLUTION. The answer is **true**.
Suppose that n has at least two distinct positive divisors p and q. Then it has at least 4 prime divisors given by $1, p, q, pq$. Thus n must only have one prime divisor. Then if $n = p^{\alpha}$, then n has $\alpha + 1$ prime divisors. Thus if $\alpha + 1 = 3$ we have that $\alpha = 2$ which is as claimed in the question.

Question 2

SOLUTION. The claims is **false**.
Let $2 \equiv -4 \mod 6$ so $a = 8$ and $b = 20$.
Further, let $8 \equiv 20 \mod 6$ so $c = 2$ and $d = -4$.
So $c \mid a$ and $d \mid b$. Then
$\frac{a}{c} = 4$ and $\frac{b}{d} = -5$ and so
$\frac{a}{c} \equiv 4 \mod 6$ and $\frac{b}{d} \equiv -5 \equiv 1 \mod 6$
These two values are not equivalent and thus this gives a counter example.

Question 3

SOLUTION. The answer is $\mathbf{d = 42}$
We use the multiplicativity of the phi function to see that
$\phi(98) = \phi(2 \cdot 49) = \phi(2 \cdot 7^2) = \phi(2)\phi(7^2) = 7(7-1) = 42$
As the phi function computes the number of primitive roots modulo n, we are done.

Question 4

SOLUTION. The answer is $\mathbf{a = 0}$
The number of primitive roots modulo n is equal to $\phi(n)$ provided that $n \in \{2, 4, p^k, 2p^k\}$ for some odd prime p. As $n = 3^2 \cdot 11$, we see that n does not take this form and so there are no primitive roots.

Question 5

SOLUTION. The correct answer is $\mathbf{c = 37}$.
Following the hints, we seek to count the number of factors of 10 in the number 153!. To do this we count the number of 5s occuring in its expansion. The number of 5s occurring in the expansion of $n!$ is given by
$\left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + ... + \left\lfloor \frac{n}{5^{\lfloor \log_5(n) \rfloor}} \right\rfloor$
This is true since you get a factor of 5 every 5 integers. You get another factor of 5 every 25 integers and so on. Counting this, we see that
$\left\lfloor \frac{153}{5} \right\rfloor + \left\lfloor \frac{153}{5^2} \right\rfloor + \left\lfloor \frac{153}{5^3} \right\rfloor = 30 + 6 + 1 = 37.$

Question 6

SOLUTION. The answer is $\mathbf{d =}$ **Wednesday**
Proceeding as in the hints, we need to compute
$10^{200000000000} \equiv 3^{200000000000} \mod 7$
We use Euler's formula which states that
$3^{\phi(7)} = 3^6 \equiv 1 \mod 7$

Next, notice that 200000000000 is not divisible by 6 (the sum of the digits is not divisible by 3 so the number is not divisible by 3). However 200000000004 is divisible by 6 and thus, $200000000004 - 6 = 199999999998 = 6s$ is divisible by 6 (here we let s be an integer). Hence

$$\begin{aligned} 10^{200000000000} &\equiv 3^{200000000000} \mod 7 \\ &\equiv 3^2 \cdot 3^{199999999998} \mod 7 \\ &\equiv 2 \cdot (3^6)^s \mod 7 \\ &\equiv 2 \mod 7 \end{aligned}$$

and thus, two days from Monday is a Wednesday.

Question 7

SOLUTION 1. The answer is $\mathbf{b = 2}$.
The quickest solution is to note that adding one egg to the basket gives a multiple of 2,3,4,5 and 6 and is congruent to 1 modulo 7. Since $\text{lcm}(2, 3, 4, 5, 6) = 60$ we are simply looking for multiples of 60 that are congruent to 1 modulo 7. Notice that $60 \equiv 4 \mod 7$ and $120 \equiv 1 \mod 7$. Hence the answer is $120 - 1 = 119$. reducing modulo 13 gives $119 \equiv 2 \mod 13$

SOLUTION 2. The correct answer is $\mathbf{b = 2}$
The slower, albeit more constructive way, to solve this is to set up a system of equations consisting of the following

$$\begin{aligned} n &\equiv 1 \mod 2 \quad n \equiv 2 \mod 3 \quad n \equiv 3 \mod 4 \\ n &\equiv 4 \mod 5 \quad n \equiv 5 \mod 6 \quad n \equiv 0 \mod 7 \end{aligned}$$

Now we just crunch condition by condition. Notice that some of these equations are redundant. In fact the cases modulo 2 and modulo 6 can be reduced from the cases modulo 4 and from combining the modulo 2 and 3 cases respectively. Hence we need only consider the equations

$$n \equiv 2 \mod 3 \quad n \equiv 3 \mod 4 \quad n \equiv 4 \mod 5 \quad n \equiv 0 \mod 7$$

For the remaining steps, let k_i be integers for each $i = 1..4$ as needed. The first equation tells us that

$$n = 2 + 3k_1$$

Plugging into the second yields $2+3k_1 \equiv 3 \mod 4$ which implies that $k_1 \equiv 3 \mod 4$. This says $k_1 = 3+4k_2$. Plugging into the equation above yields

$$n = 2 + 3k_1 = 2 + 3(3 + 4k_2) = 11 + 12k_2$$

Next, into the third equation yields $11 + 12k_2 \equiv 4 \mod 5$ which implies that $k_2 \equiv 4 \mod 5$. This says $k_2 = 4 + 5k_3$. Hence, plugging into the equation above yields

$$n = 11 + 12k_2 = 11 + 12(4 + 5k_3) = 59 + 60k_3$$

Lastly, into the fourth equation yields $59 + 60k_3 \equiv 0 \mod 7$ which implies that $k_3 \equiv 1 \mod 7$. This says $k_3 = 1 + 7k_4$. Hence, plugging into the equation above yields

$$n = 59 + 60k_3 = 59 + 60(1 + 7k_4) = 119 + 420k_4$$

Thus, in order for all these conditions to be satisfied, we need n to be congruent to 119 modulo 420. The minimum such number is 119. Modulo 13, we see that the answer is 2.

Question 8

SOLUTION. The statement is **true**.
We use the hint and proceed by proving the contrapositive. Suppose that n is not squarefree. Then there is a prime p such that $p^2 \mid n$. Now, in this case, we have
$p \mid \phi(p^k) = p^{k-1}(p-1)$
where $k \geq 2$. Further, write $n = p^k m$ where m is coprime to p. Then
$\phi(p^k) \mid \phi(p^k)\phi(m) = \phi(p^k m) = \phi(n)$.
Hence
$p \mid \phi(n)$.
However $p \nmid n-1$ since $n \equiv 0 \mod p$. Thus, $\phi(n) \nmid n-1$ since they do not share the factor of p. This is precisely what we wanted to show.

Question 9

SOLUTION. Assume towards a contradiction that $-r$ is not a primitive root. Then $(-r)^s \equiv 1 \mod p$ for some s smaller than $p-1$. Now, we have that $r^s \equiv (-1)^s \mod p$ (multiply both sides of the previous congruence by $(-1)^s$. As r is a primitive root, we have that $r^{p-1} \equiv 1 \mod p$ and that $r^{(p-1)/2} \equiv -1 \mod p$. As these are the only possible values for a power of r to be equivalent to a power of -1, we must have that either $s = p-1$ or $s = (p-1)/2$.
Suppose towards a contradiction that $s = (p-1)/2$. Then we have that by the above that
$-1 \equiv r^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv 1 \mod p$
valid since $(p-1)/2$ is even. This is a contradiction and hence $s = p-1$ making $-r$ a primitive root.

Question 10

SOLUTION. Use the Fundamental Theorem of Arithmetic to write
$a = \prod_{i=1}^{n} p_i^{e_i}$
and
$b = \prod_{i=1}^{m} p_i^{f_i}$
where we use all the same primes above in the two expansions so we will allow the possibility of e_i or f_i to be 0 (but of course not both). Then
$\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min(e_i, f_i)}$
and
$\mathrm{lcm}(a, b) = \prod_{i=1}^{n} p_i^{\max(e_i, f_i)}$.
Now, we have

$$\begin{aligned}
\gcd(a,b)\mathrm{lcm}(a,b) &= \prod_{i=1}^{n} p_i^{\min(e_i,f_i)} \prod_{i=1}^{n} p_i^{\max(e_i,f_i)} \\
&= \prod_{i=1}^{n} p_i^{\min(e_i,f_i)+\max(e_i,f_i)}
\end{aligned}$$

As
$\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$
we have that

$$\begin{aligned}
\gcd(a,b)\mathrm{lcm}(a,b) &= \prod_{i=1}^{n} p_i^{\min(e_i,f_i)} \prod_{i=1}^{n} p_i^{\max(e_i,f_i)} \\
&= \prod_{i=1}^{n} p_i^{\min(e_i,f_i)+\max(e_i,f_i)} \\
&= \prod_{i=1}^{n} p_i^{e_i+f_i} \\
&= \prod_{i=1}^{n} p_i^{e_i} \prod_{i=1}^{n} p_i^{f_i} \\
&= ab
\end{aligned}$$

completing the proof.

Question 11

SOLUTION 1. We proceed by induction. The case $N = 1$ is easy. For $N = 2$, we have
$(1+a)^2 = 1 + 2a + a^2 \equiv 1 + 2a \mod a^2$
Suppose the claim holds for N. Then for $N + 1$, we have
$(1+a)^{N+1} \equiv (1+a)^N(1+a) \equiv (1+Na)(1+a) \equiv (1+(N+1)a+Na^2) \equiv 1+(N+1)a \mod a^2$
and so by mathematical induction we are done.

SOLUTION 2. We can use the binomial theorem to see that
$(1+a)^N = \sum_{i=0}^{N} \binom{N}{a} a^i (1)^{N-i} \equiv \binom{N}{0} + \binom{N}{1} a + \sum_{i=2}^{N} \binom{N}{a} a^i (1)^{N-i} \equiv 1 + Na \mod a^2$
where all the terms in the right most summation are divisible by a^2.

Good Luck for your exams!