Full Solutions
MATH312 December 2009

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 Educational 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 Exam 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 Educational Resources.

Question 1 (a)

Solution 1. The problem is equivalent to showing that 6^n divides $(3n)!$. So we must show that $(3n)!$ contains n copies of both 2 and 3. Now, notice that in $(2n)! < (3n)!$ we have that $(2n)!$ contains $2n$ consecutive numbers of which n are even. Hence $2^n \mid (2n)! \mid (3n)!$. Now, notice that $(3n)!$ contains $3n$ consecutive numbers and so n of these must be divisible by 3 (one in every 3 consecutive numbers is divisible by 3. Hence $3^n \mid (3n)!$ and combining these results (since 2 and 3 are coprime) gives us our result.

Solution 2. For a proof by induction, notice that $(3!)^1 = 6 \mid 6 = (3n)!$. Assume that $6^n = (3!)^n \mid (3n)!$. For $n+1$, we have
$(3!)^{n+1} = 6 \cdot 6^n$.
Now, $6^n \mid (3n)!$ and $(3(n+1))! = (3n+3)! = (3n+3)(3n+2)(3n+1)(3n)!$. Thus, it suffices to show that $6 \mid (3n+3)(3n+2)(3n+1)$. Clearly $3 \mid (3n+3)$ and since this a product of three consecutive numbers, one must be even and so 2 also divides this product. Thus $6^{n+1} \mid (3n+3)!$ and this completes the proof.

Question 1 (b)

Solution. Using long division, we see that
$a^2 + b^2 = (a+b)(a-b) + 2b^2$
and thus, the Euclidean algorithm states that
$\gcd(a^2+b^2, a+b) = (a+b, 2b^2)$.
Now, as a and b are coprime, we see that
$\gcd(a^2+b^2, a+b) = (a+b, 2b^2) = (a+b, 2)$. If this were not true then some factor of b would divide $a+b$ and that means that this factor would also divide a which means that the factor must have been 1 since a and b were coprime. Finally, it's clear that $(a+b, 2)$ is 1 or 2. This completes the proof.

Question 2 (a)

Solution. Recall that 2 passes Miller's test if
$2^d \equiv 1 \mod 209$
or for some value r
$2^{2^r d} \equiv -1 \mod 209$
where $209 - 1 = 208 = 2^s d$ and $0 \leq r \leq s-1$. If 2 fails the test, then 209 is not prime. For us, we see that $208 = 2^3(26) = 2^4 \cdot 13$ and so d is 13 and r is 4. We compute manually.
$2^{13} \equiv 2^8 \cdot 2^5 \equiv (256)(32) \equiv (47)(32) \equiv 1504 \equiv 41 \not\equiv \pm 1 \mod 209$
and for the powers of 2,
$2^{2 \cdot 13} \equiv 41^2 \equiv 1681 \equiv 9 \not\equiv \pm 1 \mod 209$
$2^{4 \cdot 13} \equiv 9^2 \equiv 81 \not\equiv \pm 1 \mod 209$
$2^{8 \cdot 13} \equiv 81^2 \equiv (2 \cdot 41 - 1)^2 \equiv 4 \cdot 41^2 - 4 \cdot 41 + 1 \equiv 4 \cdot 9 - 164 + 1 \equiv 36 + 45 + 1 \equiv 82 \not\equiv \pm 1 \mod 209$
$2^{16 \cdot 13} \equiv 82^2 \equiv (81+1)^2 \equiv 81^2 + 162 + 1 \equiv 82 + 162 + 1 \equiv 36 \not\equiv \pm 1 \mod 209$
and so the number 209 is not prime and 2 fails Miller's test. Thus 209 is composite. In fact $209 = 11 \cdot 19$.

Question 2 (b)

Solution. We follow the hints above (especially hint 2) which suggests we should use Korselt's Criterion. We first factor the number as
$2821 = 7 \cdot 403 = 7 \cdot 13 \cdot 31$
We check that $(p-1) \mid (n-1)$ for each prime factor. Notice that

$$(7-1) = 6 \mid 2820$$
$$(13-1) = 12 \mid 2820$$
$$(31-1) = 30 \mid 2820$$

We can see these are true by factoring
$2820 = 10 \cdot 282 = 2 \cdot 5 \cdot 2 \cdot 141 = 2^2 \cdot 5 \cdot 3 \cdot 47 = 2^2 \cdot 3 \cdot 5 \cdot 47$.
Hence 2821 is a Carmichael number.

Question 3 (a)

SOLUTION. Since considering a number modulo 1000 gives the last 3 digits, it suffices to consider this number modulo 1000. Now
$\phi(1000) = \phi(2^3 \cdot 5^3) = \phi(8)\phi(125) = (4)(100) = 400$
Euler's Theorem (valid throughout since $\gcd(7, 1000) = 1$) states that
$7^{400} \equiv 7^{\phi(1000)} \equiv 1 \mod 1000$
and so we have

$$\begin{aligned} 7^{999} &\equiv 7^{400} \cdot 7^{400} \cdot 7^{199} \mod 1000 \\ &\equiv 7^{199} \mod 1000 \end{aligned}$$

Let's examine 7^{200}. Notice that
$\phi(8) = 4 \quad \text{and} \quad \phi(125) = 100$
and so by Euler's Theorem, we have
$7^{200} \equiv (7^4)^{50} \equiv 1 \mod 8$.
Thus $7^{200} = 1 + 8s$ for some integer s. Further,
$1 + 8s \equiv 7^{200} \equiv (7^{100})^2 \equiv 1 \mod 125$
and so $8s \equiv 0 \mod 125$ giving $s = 125t$ for some integer t. Thus, $7^{200} = 1 + 8s = 1 + 1000t$. So $7^{200} \equiv 1 \mod 1000$. Hence
$7^{199} \equiv 7^{-1} \mod 1000$.
To complete the proof, we need to find the inverse of 7 modulo 1000. We can do this via the Euclidean algorithm.

$$\begin{aligned} 1000 &= 7(142) + 6 \\ 7 &= 6(1) + 1 \end{aligned}$$

and back substituting gives

$$\begin{aligned} 1 &= 7 - 6(1) \\ 1 &= 7 - (1000 - 7(142))(1) \\ 1 &= 7(143) - 1000(1) \end{aligned}$$

and so the inverse of 7 modulo 1000 is 143. Hence
$7^{999} \equiv 7^{199} \equiv 7^{-1} \equiv 143 \mod 1000$
completing the question.

Question 3 (b)

SOLUTION. We use the square multiply algorithm to solve this problem. We compute 9^{2a} for a up to 4 to compute this value. We see that

$$\begin{aligned}
9 &\equiv 9 \mod 31 \\
9^2 &\equiv 81 \equiv 19 \mod 31 \\
9^4 &\equiv (9^2)^2 \equiv 19^2 \equiv 361 \equiv 51 \equiv 20 \mod 31 \\
9^8 &\equiv (9^4)^2 \equiv 20^2 \equiv 400 \equiv 90 \equiv 28 \equiv -3 \mod 31 \\
9^{16} &\equiv (9^8)^2 \equiv (-3)^2 \equiv 9 \mod 31
\end{aligned}$$

Now, we have that

$$\begin{aligned}
9^{23} &\equiv 9^{16} \cdot 9^4 \cdot 9^2 \cdot 9^1 \mod 31 \\
&\equiv 9 \cdot 20 \cdot 19 \cdot 9 \mod 31 \\
&\equiv 9 \cdot 9 \cdot 19 \cdot 20 \mod 31 \\
&\equiv 9^2 \cdot 19 \cdot 20 \mod 31 \\
&\equiv 19 \cdot 19 \cdot 20 \mod 31 \\
&\equiv 19^2 \cdot 20 \mod 31 \\
&\equiv 20 \cdot 20 \mod 31 \\
&\equiv 28 \mod 31
\end{aligned}$$

Question 4 (a)

SOLUTION. First, we isolate for P in the given formula. To do this we need to compute the inverse of 7 modulo 26. We use the Euclidean algorithm to do this.

$$\begin{aligned}
26 &= 7(3) + 5 \\
7 &= 5(1) + 2 \\
5 &= 2(2) + 1
\end{aligned}$$

and back substituting

$$\begin{aligned}
1 &= 5 - 2(2) \\
1 &= 5 - (7 - 5(1))(2) \\
1 &= 5(3) - 7(2) \\
1 &= (26 - 7(3))(3) - 7(2) \\
1 &= 26(3) - 7(11)
\end{aligned}$$

and so the inverse of 7 modulo 26 is (-11) which is equal to 15 modulo 26. Hence
$P = 15(7P) = 15(C - 11) \mod 26$
We plug in the four values of C given by $OAPB = (14)(0)(15)(1)$ and see that

$$\begin{aligned}
P_1 &\equiv 15(14 - 11) \equiv 15(3) \equiv 45 \equiv 19 \equiv T \mod 26 \\
P_2 &\equiv 15(0 - 11) \equiv 15(-11) \equiv -165 \equiv 17 \equiv R \mod 26 \\
P_3 &\equiv 15(15 - 11) \equiv 15(4) \equiv 60 \equiv 8 \equiv I \mod 26 \\
P_4 &\equiv 15(1 - 11) \equiv 15(-10) \equiv -150 \equiv 6 \equiv G \mod 26
\end{aligned}$$

Thus, the plaintext was the word TRIG.

Question 4 (b)

Solution. We begin by multiplying the product by $(-1)^{p-1} \equiv 1 \mod p$. This gives
$1^2 \cdot 3^2 \cdot 5^2 \cdot ... \cdot (p-2)^2 \equiv 1^2 \cdot 3^2 \cdot 5^2 \cdot ... \cdot (p-2)^2 \cdot (-1)^{p-1} \mod p$
Now, rewrite each square as $a^2 = a \cdot a$ and for each value of a, distribute a power of -1. Notice that we have $(p-1)/2$ terms in our product. So we need to take a factor of $(-1)^{(p-1)/2}$ to accomplish this. This gives

$$\begin{aligned} &1^2 \cdot 3^2 \cdot 5^2 \cdot ... \cdot (p-2)^2 \cdot (-1)^{p-1} \\ &\quad \equiv (1)(-1)(3)(-3)(5)(-5)...(p-2)(-(p-2)) \cdot (-1)^{(p-1)/2} \mod p \end{aligned}$$

Now for each negative term, we add p to get.

$$\begin{aligned} &(1)(-1)(3)(-3)(5)(-5)...(p-2)(-(p-2)) \cdot (-1)^{(p-1)/2} \\ &\quad \equiv (1)(p-1)(3)(p-3)(5)(p-5)...(p-2)(2) \cdot (-1)^{(p-1)/2} \mod p \end{aligned}$$

After rearranging the right hand side above, we see that

$$\begin{aligned} &(1)(p-1)(3)(p-3)(5)(p-5)...(p-2)(2) \cdot (-1)^{(p-1)/2} \\ &\quad \equiv (p-1)! \cdot (-1)^{(p-1)/2} \mod p \end{aligned}$$

By Wilson's Theorem and combining the above, we have

$$\begin{aligned} &1^2 \cdot 3^2 \cdot 5^2 \cdot ... \cdot (p-2)^2 \\ &\quad \equiv (p-1)! \cdot (-1)^{(p-1)/2} \mod p \\ &\quad \equiv (-1) \cdot (-1)^{(p-1)/2} \mod p \\ &\quad \equiv (-1)^{(p+1)/2} \mod p \end{aligned}$$

and this was what we wanted to show.

Question 5 (a)

Solution. First we show that the Mobius function is multiplicative. Let m and n be coprime integers. Then let
$m = \prod_{i=1}^{M} p_i^{\alpha_i}$
and
$n = \prod_{j=1}^{N} q_j^{\beta_j}$.
We wish to show that $\mu(mn) = \mu(m)\mu(n)$. Clearly, if m or n contains a square prime factor, then both sides evaluate to 0 so without loss of generality, suppose that each $\alpha_i, \beta_j = 1$. We break into cases based on the number of prime factors.
Case 1: M and N are both odd or both even.. In these cases, $\mu(mn) = 1$. Now, since the number of prime factors are both odd or both even, we have that $\mu(m) = \mu(n)$ and since these are now either plus or minus 1 (we've eliminated the case when the Mobius function is 0 on either side), we have
$\mu(mn) = 1 = \mu(m)^2 = \mu(m)\mu(n)$

Case 2: M and N are of opposite parity.. Suppose that M is even (the argument is symmetric). In this case $\mu(mn) = -1$ since we have an odd number of factors. Now, we have that $\mu(m) = -1$ and $\mu(n) = 1$. Thus,
$\mu(mn) = -1 = \mu(m)\mu(n)$
Hence the Mobius function is multiplicative.
Now, let $S(n) = \sum_{d|n} \mu(d)$. I claim that this function is also multiplicative. For this, again let m and n be coprime integers (notice that $S(1) = 1$). We see that
$$S(m)S(n) = \sum_{d|m} \mu(d) \sum_{e|n} \mu(e) = \sum_{d|m} \sum_{e|n} \mu(d)\mu(e) = \sum_{d|m} \sum_{e|n} \mu(de)$$
Now as m and n are coprime, we see that for any divisor $h \mid mn$, we can write h uniquely of the form $h = de$ where $d \mid m$ and $e \mid n$ and vice versa. Thus, we have
$$S(m)S(n) = \sum_{d|m} \sum_{e|n} \mu(de) = \sum_{h|mn} \mu(h) = S(mn)$$
showing that this function is also multiplicative. So, by multiplicativity, it suffices to show that
$S(p^a) = 0$ where p is a prime and a is an integer. Here, we have
$$S(p^a) = \sum_{d|p^a} \mu(d) = \sum_{i=0}^{a} \mu(p^i) = \mu(1) + \mu(p) + \sum_{i=2}^{a} \mu(p^i).$$
Notice that the last sum might be non-existent if a is 1. In any case, the last sum evaluates to 0 since all the terms contain a p^2 factor. Notice that $\mu(1) + \mu(p) = 1 - 1 = 0$ and so $S(p^a) = 0$ so long as a is not 0 (which is allowed since n was an integer greater than 1). Thus we have a multiplicative function which evaluates to 0 on all prime powers, hence it must be zero for all values greater than 1 since
$$S(n) = S\left(\prod_{j=1}^{N} q_j\right) = \prod_{j=1}^{N} S\left(q_j\right) = 0.$$
This completes the proof.

Question 5 (b)

SOLUTION. A convergent is given by
$$[a_0; a_1, a_2, ..., a_n] = \frac{h_n}{k_n}$$
where we also have the recurrence relations

$$h_n = a_n h_{n-1} + h_{n-2}$$
$$k_n = a_n k_{n-1} + k_{n-2}$$

subject to the initial conditions $h_{-1} = 1, h_{-2} = 0, k_{-1} = 0, k_{-2} = 1$.
Plugging in our values, we see that

$$h_0 = a_0 h_{0-1} + h_{0-2} = (0)(1) + 0 = 0$$
$$k_0 = a_0 k_{0-1} + k_{0-2} = (0)(0) + 1 = 1$$
$$h_1 = a_1 h_{1-1} + h_{1-2} = (1)(0) + 1 = 1$$
$$k_1 = a_1 k_{1-1} + k_{1-2} = (1)(1) + 0 = 1$$
$$h_2 = a_2 h_{2-1} + h_{2-2} = (2)(1) + 0 = 2$$
$$k_2 = a_2 k_{2-1} + k_{2-2} = (2)(1) + 1 = 3$$
$$h_3 = a_3 h_{3-1} + h_{3-2} = (3)(2) + 1 = 7$$
$$k_3 = a_3 k_{3-1} + k_{3-2} = (3)(3) + 1 = 10$$
$$h_4 = a_4 h_{4-1} + h_{4-2} = (4)(7) + 2 = 30$$
$$k_4 = a_4 k_{4-1} + k_{4-2} = (4)(10) + 3 = 43$$

Thus the convergents are
$\left\{0, 1, \frac{2}{3}, \frac{7}{10}, \frac{30}{43}\right\}$

Question 6 (a)

SOLUTION. Assume towards a contradiction that
$\sqrt{3} + \sqrt{2} = \frac{p}{q}$
where $\gcd(p, q) = 1$. Now, squaring both sides yields
$3 + 2\sqrt{6} + 2 = \frac{p^2}{q^2}$
and isolating for the radical yields
$\sqrt{6} = \frac{p^2 - 5q^2}{2q^2}$
Now the right hand side is rational so now it suffices to show that $\sqrt{6}$ is irrational (this will simplify the computations to treat this as its own case). Suppose that
$\sqrt{6} = \frac{a}{b}$
where $\gcd(a, b) = 1$. Squaring both sides and cross multiplying yields
$6b^2 = a^2$
Now, 2 divides the left hand side so $2 \mid a$ writing $a = 2A$ and substituting yields
$6b^2 = 4A^2$.
Dividing by 2 yields
$3b^2 = 2A^2$.
Now, 2 divides the right hand side so $2 \mid b$. This contradicts the fact that $\gcd(a, b) = 1$ since 2 divides both numbers. Thus $\sqrt{6}$ is irrational and hence so is $\sqrt{3} + \sqrt{2}$ by the above argument as required.

Question 6 (b)

SOLUTION. The stated problem is equivalent to showing that $0 \equiv a^{4n+1} - a \mod 10$ which is equivalent to showing that 10 divides $a(a^{4n} - 1)$.
To do this, we break this into cases. Since we are looking modulo 10, we only have to discuss the cases when $a \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ since all numbers reduce to one of these modulo 10. We proceed as suggested by the hints.
Case 1

$$a = 0$$

. This case clearly satisfies $a \equiv a^{4n+1} \mod 10$ by a simple substitution. We suppose that a is positive.
Case 2

$$2 \mid a$$

. In this case, notice that clearly 2 divides $a(a^{4n} - 1)$ so it suffices to show that 5 divides $a^{4n} - 1$. Notice that 5 does not divide a and so $\gcd(a, 5) = 1$. Thus Euler's Theorem applies giving us that
$1 \equiv a^{\phi(5)} \equiv a^4 \mod 5$.
Hence
$a^{4n} - 1 \equiv (a^4)^n - 1 \equiv 1^n - 1 \equiv 0 \mod 5$
Thus, 5 divides $a^{4n} - 1$ and so 10 divides $a(a^{4n} - 1)$.
Case 3

$$a = 5$$

. In this case, notice that clearly 5 divides $a(a^{4n} - 1)$ so it suffices to show that 2 divides $a^{4n} - 1$. This last number is even since $a^{4n} = 5^{4n}$ is odd. Thus 10 divides $a(a^{4n} - 1)$.

Case 4

$$2 \nmid a$$

and $a \neq 5$. In this case, $\gcd(a, 10) = 1$. Thus Euler's Theorem applies giving us that
$1 \equiv a^{\phi(10)} \equiv a^{\phi(2)\phi(5)} \equiv a^{(1)(4)} \equiv a^4 \mod 10$.
Hence
$a(a^{4n} - 1) \equiv a((a^4)^n - 1) \equiv a(1^n - 1) \equiv 0 \mod 10$
Thus 10 divides $a(a^{4n} - 1)$ completing the proof.

Good Luck for your exams!