# Full Solutions
# MATH437 December 2011

April 5, 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. Assume towards a contradiction that $n \mid (2^n - 1)$.
Let $p$ be the smallest prime dividing $n$. Notice that $2^n - 1$ is odd and so $p$ is not 2. Thus, we have that
$2^n \equiv 1 \mod p$
and by Fermat's Little Theorem, we also have that
$2^{p-1} \equiv 1 \mod p$.
Thus, we also have that (via the Euclidean Algorithm)
$2^{\gcd(n,p-1)} \equiv 1 \mod p$.
However $\gcd(n, p-1) = 1$ since $p$ was the smallest prime dividing $n$. This gives us that
$2 \equiv 1 \mod p$
which is a contradiction.

## Question 2

SOLUTION. First we show that $a_k = 1$. Let $\ell$ be an integer. Since our function is multiplicative, we know that
$f(10^\ell) = f(2^\ell)f(5^\ell)$.
Expanding gives

$$\begin{aligned} a_k 10^{\ell k} + a_{k-1}10^{\ell(k-1)} + ... + a_0 &= (a_k 2^{\ell k} + a_{k-1}2^{\ell(k-1)} + ... + a_0)(a_k 5^{\ell k} + a_{k-1}5^{\ell(k-1)} + ... + a_0) \\ &= a_k^2 10^{\ell k} + a_{k-1}10^{\ell(k-1)}((2+5)a_k + a_{k-1}) + .. + a_0^2 \end{aligned}$$

Isolating for $10^{\ell k}$ gives
$a_k(1-a_k)10^{\ell k} = a_{k-1}10^{\ell(k-1)}((2+5)a_k + a_{k-1} - 1) + ... + a_0^2 - a_0$
Dividing both sides by $10^{\ell k}$ gives
$a_k(1-a_k) = 10^{-\ell}(a_{k-1}((2+5)a_k + a_{k-1} - 1) + ... + (a_0^2 - a_0)10^{-\ell(k-1)})$
Making $\ell$ sufficiently large, we can see that the right hand side tends to 0. Since the left hand side is an integer, we see that the right hand side must in fact be 0 and hence so must the left hand side. Thus,
$a_k(1-a_k) = 0$
giving $a_k = 1$ since $a_k \neq 0$ as stated in the question.
Next, we show that all the other coefficients must be 0. Let $j$ be the largest index less that $k$ such that $a_j \neq 0$. We assume that $j$ exists and find a contradiction. Thus,
$f(n) = x^k + a_j x^j + ... + a_0$.
Let $m$ and $n$ be arbitrary nonzero, nonunital positive integers such that $\gcd(m,n) = 1$. Then, we see again that
$f((mn)^\ell) = f(m^\ell)f(n^\ell)$
and hence

$$\begin{aligned} (mn)^{\ell k} + a_j(mn)^{\ell j} + ... + a_0 &= (m^{\ell k} + a_j m^{\ell j} + ... + a_0)(n^{\ell k} + a_j n^{\ell j} + ... + a_0) \\ &= (mn)^{\ell k} + a_j(mn)^{\ell j}(m^{\ell(k-j)} + n^{\ell(k-j)} + a_j) + .. + a_0^2 \end{aligned}$$

Cancelling and isolating for $a_j$ yields

$$a_j(mn)^{\ell j}(1 - m^{\ell(k-j)} - n^{\ell(k-j)} - a_j) = \text{terms with order less than } (mn)^{\ell j}$$

As before dividing by $(mn)^{\ell j}$ and letting $\ell$ tend to infinity shows that the modified right hand side is 0 and thus, we have
$a_j(mn)^{\ell j}(1 - m^{\ell(k-j)} - n^{\ell(k-j)} - a_j) = 0$
Hence, either $a_j = 0$ or $a_j = 1 - m^{\ell(k-j)}n^{\ell(k-j)}$. However, $a_j$ is completely independent of $\ell$. Thus as $j$ is distinct from $k$ (so $k - j \neq 0$), we must have that $a_j = 0$ which shows that no such $j$ can exists. Hence each and every $a_j$ for $0 \leq j < k$ must in fact be 0. This completes the proof.

Keep in mind that $f(1) = 1$ and this holds with this polynomial. Also it is clear that $f(n) = n^k$ is multiplicative.

## Question 3

**Solution.** Let $m$ be an arbitrary integer.
The main idea uses the Chinese Remainder Theorem. Define a system of congruences by
$x \equiv p_i - i + 1 \mod p_i^2$ for $i \in \{1, .., m-1\}$
where $p_i$ is the $i$th prime number. So

$$x \equiv 2 - 1 + 1 \mod 4$$

$$x \equiv 3 - 2 + 1 \mod 9$$

$$x \equiv 5 - 3 + 1 \mod 25$$

and so on. Now look at the numbers $x, x+1, ..., x+m-1$. Notice that for any $x+(i-1)$ for $i \in \{1, .., m-1\}$, we have
$x + (i-1) \equiv p_i \mod p_i^2$
This means that $p_i \mid (x+i-1)$ however $p_i^2 \nmid (x+i-1)$. Thus, no entry in this list can be a power of a prime (though some entries themselves might be prime if $m$ is too small).

## Question 4

**Solution.** First, notice that
$\displaystyle\sum_{i=1}^{p-1} \frac{1}{i} = \frac{a}{b} = \frac{a\frac{(p-1)!}{b}}{(p-1)!}$.

Now, if we are to show that $p^2 \mid a$ then it suffices to show that $p^2 \mid a\frac{(p-1)!}{b}$ since the term given by $\displaystyle\frac{(p-1)!}{b}$ is corpime to $p$. Cross multiplying shows us that it suffices to show that
$\displaystyle p^2 \mid \sum_{i=1}^{p-1} \frac{(p-1)!}{i}$.

Let's now pair terms with their additive inverses:
$\displaystyle\sum_{i=1}^{p-1} \frac{(p-1)!}{i} = (p-1)! \sum_{i=1}^{(p-1)/2} \left(\frac{1}{i} + \frac{1}{p-i}\right) = (p-1)! \sum_{i=1}^{(p-1)/2} \left(\frac{p-i+i}{i(p-i)}\right) = p \sum_{i=1}^{(p-1)/2} \left(\frac{(p-1)!}{i(p-i)}\right)$
and thus it now suffices to show that the sum
$\displaystyle\sum_{i=1}^{(p-1)/2} \frac{(p-1)!}{i(p-i)} \equiv \sum_{i=1}^{(p-1)/2} (-i^2)^{-1}(p-1)! \equiv \sum_{i=1}^{(p-1)/2} -(-i^2)^{-1} \equiv \sum_{i=1}^{(p-1)/2} i^{-2} \mod p$
satisfies
$\displaystyle S := \sum_{i=1}^{(p-1)/2} i^{-2} \equiv 0 \mod p.$
To do this, we use the trick common in evaluating Gauss sums and looking at $2S = S + S$. this gives

$$\begin{aligned} S + S &= \sum_{i=1}^{(p-1)/2} i^{-2} + \sum_{i=1}^{(p-1)/2} i^{-2} \\ &= \sum_{i=1}^{(p-1)/2} i^{-2} + \sum_{i=1}^{(p-1)/2} (-i)^{-2} \end{aligned}$$

Now note that $\{1^{-1}, 2^{-1}, ..., (p-1)^{-1}\}$, $\{1, 2, ..., p-1\}$ and $\{\pm 1, \pm 2, ..., \pm(p-1)/2\}$ all form complete residue systems for $(\mathbb{Z}/p\mathbb{Z})^*$. Thus, the above sum is

$$\begin{aligned} S + S &= \sum_{i=1}^{(p-1)/2} i^{-2} + \sum_{i=1}^{-(p-1)/2} i^{-2} \\ &= \sum_{i=1}^{p-1} i^{-2} \\ &= \sum_{i=1}^{p-1} i^{2} \\ &= \frac{p(p-1)(2p-1)}{6} \end{aligned}$$

Here is where we use the fact that $p \geq 5$. Notice that as $p$ is odd, we have that $2 \mid (p-1)$. Further, we know that either $p \equiv 1 \mod 3$ or $p \equiv 2 \mod 3$. If $p \equiv 1 \mod 3$ then $3 \mid (p-1)$. If $p \equiv 2 \mod 3$ then $2p - 1 \equiv 2(2) - 1 \equiv 0 \mod 3$ and so $3 \mid (2p-1)$. In either case, we see that $\frac{(p-1)(2p-1)}{6} \in \mathbb{Z}$ and thus $\frac{p(p-1)(2p-1)}{6} \equiv p\left(\frac{(p-1)(2p-1)}{6}\right) \equiv 0 \mod p$. Hence, we see that $2S \equiv 0 \mod p$. Again as $p$ is odd, we have that $S \equiv 0 \mod p$.
This completes the proof.
For those of you wondering, this is also called Wolstenholme's Theorem.

## Question 5

SOLUTION. The claim is clearly true of one of $m$ or $n$ equals 1. Thus we suppose that both are strictly greater than 1.
In this case, the Fundamental Theorem of Arithmetic tells us that we may write

$$m = \prod_{i=1}^{k} p_i^{\alpha_i}$$

and

$$n = \prod_{j=1}^{\ell} q_j^{\beta_j}$$

where each of the exponents is a positive integer at least 1. The left hand side of the equation in question thus reduces to

$$m\phi(m) = \prod_{i=1}^{k} p_i^{\alpha_i} \left(\prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)\right) = \prod_{i=1}^{k} p_i^{2\alpha_i - 1}(p_i - 1)$$

and in total as we are given that $m\phi(m) = n\phi(n)$, we have

$$\prod_{i=1}^{k} p_i^{2\alpha_i - 1}(p_i - 1) = \prod_{j=1}^{\ell} q_j^{2\beta_j - 1}(q_j - 1)$$

Now, suppose that $m$ and $n$ are distinct. Let $p_0$ be the largest prime where they differ and without loss of generality, suppose that $p_0^{\alpha_0} \parallel m$ but $p_0^{\alpha_0} \nmid n$. Then we know that we must have that $p_0 \mid (q_{j_0} - 1)$ for some $j_0$. Thus $q_{j_0} > p_0$.
However, $p_0$ was chosen to be the largest such prime where $m$ and $n$ differ to any power. So $q_{j_0}^{\beta_{j_0}} = p_{i_0}^{\alpha_{i_0}}$ for some $i_0$ and thus $(q_{j_0} - 1) = (p_{i_0} - 1)$. Thus, we may cancel out these terms and repeat this argument to find another index $j_0$ and since there are only finitely many of these terms, we must eventually reach a contradiction.
Hence $m$ and $n$ have all the same prime factors to the same powers and thus are equal.
**Food for thought**: Is there an easier proof of this using the fact that
$n\phi(n) = 2\sum k$
where the above sum ranges over all integers $1 \leq k \leq n$ with $\gcd(k, n) = 1$?

## Question 6

SOLUTION. Let $n = 2^k m$ with $k$ at least 1. Further, let

$$\sigma(n) = \sum_{d|n} d$$

and recall that this function is multiplicative (the sum is over positive divisors of $n$). Since we are given that $n$ is an even perfect number, we know that

$$2n = \sigma(n).$$

Next, we use the multiplicativity of $\sigma$ and see that

$$2^{k+1}m = 2n = \sigma(n) = \sigma(2^k m) = \sigma(2^k)\sigma(m) = (1 + 2 + 2^2 + ... + 2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m).$$

Since $\gcd(2^{k+1}, 2^{k+1} - 1) = 1$, we see that $(2^{k+1} - 1) \mid m$. Let $M$ be an integer such that $m = (2^{k+1} - 1)M$.
Substituting this into the above yields
$2^{k+1}(2^{k+1} - 1)M = 2^{k+1}m = (2^{k+1} - 1)\sigma(m)$.
Cancelling on both sides yields
$2^{k+1}M = \sigma(m)$.
Using the fact that both $m$ and $M$ are divisors of $m$ (and hence are terms inside the expansion of $\sigma(m)$, we have that
$2^{k+1}M = \sigma(m) \geq m + M = (2^{k+1} - 1)M + M = 2^{k+1}M$.
Thus, the greater than sign is in fact an equality. This means that $\sigma(m)$ has only two factors, namely $m$ and $M$. Since $m > M$, we must have that $M = 1$ and so $m = (2^{k+1} - 1)M = 2^{k+1} - 1$. As $m$ has only two prime factors, we also know that $m = 2^{k+1} - 1$ is prime. This completes the proof.

## Question 7 (i)

SOLUTION. We first make some observations before beginning the formal proof.
Firstly, recall that the order of an odd element in $\mathbb{Z}/2^k\mathbb{Z}$ divides $\phi(2^k) = 2^{k-1}$ for any $k \geq 1$. This follows from Euler's theorem and using the Euclidean algorithm (for any element if $d^b \equiv 1 \mod m$ and $d^c \equiv 1 \mod m$ then $d^{\gcd(b,c)} \equiv 1 \mod m$). Thus the order of $a$ must be a power of 2.
Suppose that the order of $a$ is the value $r$. The above shows that $r$ is a power of 2. Moreover,

$$(a^r)^2 \equiv 1 \mod 2^{\alpha+2}$$

Thus, to show that $r$ is $2^\alpha$, it suffices to show that
$a^{2^{\alpha-1}} \not\equiv 1 \mod 2^\alpha$ and $a^{2^\alpha} \equiv 1 \mod 2^\alpha$.
Next, we will make use of this small lemma.
**Lemma** The solutions to $x^2 \equiv 1 \mod 2^e$ for $e$ a positive integer are given as follows:

1) If $e = 1$, then $x = 1$.

2) If $e = 2$, then $x = \pm 1$.

3) If $e \geq 3$, then $x \equiv \pm 1 \mod 2^e$ or $x = \pm 1 + 2^{e-1} \mod 2^e$.

**Proof of lemma** The first two cases are clear so let's suppose that $e$ is at least 3. Clearly the four $x$ values do give solutions so it suffices to show that these are the only ones. Factoring shows that
$(x-1)(x+1) \equiv 0 \mod 2^e$.
Notice that $\gcd(x+1, x-1) = \gcd(x+1, 2) = 2$. Thus, we must have that one of the following is true
$x - 1 \equiv 0 \mod 2^{e-1}$
or
$x + 1 \equiv 0 \mod 2^{e-1}$
These give one of $x = \pm 1 + 2^{e-1}k$ for some integer $k$. We break into cases.
**Case 1**

$$k = 2m + 1$$

**odd**. Then, we see that
$x = \pm 1 + 2^{e-1}(2m+1) = \pm 1 + 2^{e-1} + 2^e m \equiv \pm 1 + 2^{e-1} \mod 2^e$
**Case 2**

$$k = 2m$$

**even**. Then, we see that
$x = \pm 1 + 2^{e-1}(2m) = \pm 1 + 2^e m \equiv \pm 1 \mod 2^e$
and this is what was to be shown completing the proof of the **lemma**.
After all this we can begin the proof of the problem. The proof proceeds by induction.
Notice that the claim is trivial for $\alpha = 0$ or $\alpha = 1$. For $\alpha = 2$, we have that $a \equiv 5, 13 \mod 16$ and both of these elements can be checked to have order 4. Thus, we suppose that $\alpha \geq 3$ and that the claim holds for $\alpha - 1$.
To prove the claim for $\alpha$, we proceed in two parts as suggested by the preliminary discussion. **First** we show that

$$a^{2^{\alpha-1}} \not\equiv 1 \mod 2^{\alpha+2}.$$

Notice that the induction hypothesis gives us that

$$a^{2^{\alpha-1}} \equiv 1 \mod 2^{\alpha+1}$$

and $a^{2^{\alpha-2}} \not\equiv 1 \mod 2^{\alpha+1}$
Notice that the element $a^{2^{\alpha-2}}$ is a nontrivial solution to $x^2 \equiv 1 \mod 2^{\alpha+1}$. Thus, the lemma states that

$$a^{2^{\alpha-2}} \equiv \pm 1 + 2^\alpha \mod 2^{\alpha+1}$$

or $a^{2^{\alpha-2}} \equiv -1 \mod 2^{\alpha+1}$
(since the solution 1 is not consistent with the above information). Notice that for the two negative solutions, If we look at the equation modulo 4 (recalling that we assumed that $\alpha \geq 3$), we get that

$$1 \equiv a^{2^{\alpha-2}} \equiv -1 \mod 4$$

where we used the fact that $a \equiv 5 \mod 8$. This gives a contradiction and thus

$$a^{2^{\alpha-2}} \equiv \pm 1 + 2^{\alpha} \mod 2^{\alpha+1}.$$

Next, we assume that $a^{2^{\alpha-1}} \equiv 1 \mod 2^{\alpha+2}$ and try to reach a contradiction. From above, we saw that $a^{2^{\alpha-2}} \not\equiv 1 \mod 2^{\alpha+1}$ and thus, $a^{2^{\alpha-2}} \not\equiv 1 \mod 2^{\alpha+2}$. Once again, using the lemma and similar logic to the above, we see that

$$a^{2^{\alpha-2}} \equiv 1 + 2^{\alpha+1} \mod 2^{\alpha+2}.$$

This implies that $a^{2^{\alpha-2}} \equiv 1 \mod 2^{\alpha+1}$ which contradicts the above.
**Secondly**, we wish to show that $a^{2^{\alpha}} \equiv 1 \mod 2^{\alpha+2}$. Thankfully, this is much more straightforward. Using the induction hypothesis given by

$$a^{2^{\alpha-1}} \equiv 1 \mod 2^{\alpha+1}$$

we recast this information as

$$a^{2^{\alpha-1}} = 1 + 2^{\alpha+1}k$$

for some integer $k$. Squaring both sides yields

$$a^{2^{\alpha}} = (a^{2^{\alpha-1}})^2 = (1 + 2^{\alpha+1}k)^2 = 1 + 2^{\alpha+2}k + 2^{2\alpha+2}k^2 \equiv 1 \mod 2^{\alpha+2}$$

which completes what was required to show.

## Question 7 (ii)

Solution. Repeating the hint, part (i) shows us that the order of $a$ modulo $2^{\alpha+2}$ is equal to $2^{\alpha}$. Thus each of

$$a^j \mod 2^{\alpha+2}$$

are distinct odd numbers between 0 and $2^{\alpha+2}$ for $0 \le j \le 2^{\alpha} - 1$ and thus each of the

$$(-1)a^j \mod 2^{\alpha+2}$$

are also distinct odd numbers between 0 and $2^{\alpha+2}$. As there are $2^{\alpha-1}$ total odd numbers between 0 and $2^{\alpha+2}$, we know that provided all of the above numbers are distinct, we have found $2^{\alpha} + 2^{\alpha} = 2^{\alpha+1}$ total odd numbers and hence we can form a bijection. Hence it suffices to show that

$$(-1)a^k \not\equiv a^j \mod 2^{\alpha+2}$$

for any $0 \le j, k \le 2^{\alpha} - 1$. This shows the claim for all odd numbers since all odd numbers are equivalent modulo $2^{\alpha+2}$ to an odd number between 0 and $2^{\alpha+2}$.

Assume towards a contradiction that we found two such numbers:

$$(-1)a^k \equiv a^j \mod 2^{\alpha+2}$$

Without loss of generality, suppose that $k \geq j$. Then,

$$a^{k-j} \equiv -1 \mod 2^{\alpha+2}$$

Once again, modulo 4 arguments (recalling that $a \equiv 5 \mod 8$) show that the left hand side above is congruent to 1 modulo 4 and the right hand side is still congruent to -1 modulo 4. This is a contradiction. Thus any odd number can be expressed uniquely of the form

$$(-1)^i a^j$$

with $i \in \{0, 1\}$ and $0 \leq j \leq 2^\alpha - 1$ as required.

## Good Luck for your exams!