Full Solutions
MATH437 December 2006

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

Solution. By the fundamental theorem of arithmetic, let $z^2 = \prod_{i=1}^{n} p_i^{2\alpha_i}$ be the prime factorization. Suppose that $p_i \mid x$ for any i. Then since x and y are coprime, this means that $p_i \nmid y$. Thus, we must have that $p_i^{2\alpha_i} \parallel x$.
If one of x or y (or both) has no prime factors, then since these numbers are positive, they must be equal to 1 which is a square.
Repeating this argument for all such i and noticing that this argument is symmetric in x and y, we see that

$$x = \prod_{p_i \mid x} p_i^{2\alpha_i} = \left(\prod_{p_i \mid x} p_i^{\alpha_i} \right)^2 = u^2$$

and

$$y = \prod_{p_i \mid y} p_i^{2\alpha_i} = \left(\prod_{p_i \mid y} p_i^{\alpha_i} \right)^2 = v^2$$

completing the proof.

Question 2

Solution. Clearly $0^6 \equiv 0 \mod 31$ and $(\pm 1)^6 \equiv 1 \mod 31$ so throughout we suppose that both x is greater than 1 but less than 30. This leaves 28 such values left to be computed. We begin by computing at powers of two. Since
$(\pm 2)^6 \equiv (\pm 1)^6 \cdot 2^5 \cdot 2 \equiv 2 \mod 31$
we see that a equals 2 is an admissable value. Further, we immediately get that
$(2^b)^6 \equiv (2^6)^b \equiv 2^b \mod 31$
and so for b ranging from 1 to 4 we see that a can take on the values 2,4,8 or 16. This covers the x values $x = \pm 2, \pm 4, \pm 8, \pm 16$.
Next for x equals ± 3, notice that
$(\pm 3)^6 \equiv (3^3)^2 \equiv (27)^2 \equiv (-4)^2 \equiv 16 \mod 31$
which gives us an already chosen a value. Using these facts, we can clearly see that
Further at x equals ± 5,
$(\pm 5)^6 \equiv (5^2)^3 \equiv (-6)^3 \equiv -6 \cdot 36 \equiv -6 \cdot 5 \equiv 1$
and this value was also an already chosen a value. I claim that these values are enough to show that all admissable values of a have already been found. To see this, notice for example that
$(\pm 6)^6 \equiv 3^6 \cdot 2^6 \mod 31$
and the right hand side was already shown to be a power of 2. Similarly
$(\pm 7)^6 \equiv (\pm 1)^6 (7)^6 \equiv (-7)^6 \equiv (24)^6 \equiv (2^3)^6 \cdot 3^6 \mod 31$
is also a power of 2. Crunching through the remaining cases, we have
$(\pm 9)^6 \equiv (3^6)^2 \mod 31$
$(\pm 10)^6 \equiv 2^6 \cdot 5^6 \mod 31$
$(\pm 11)^6 \equiv (\pm 1)^6 (11)^6 \equiv (-11)^6 \equiv 20^6 \mod 31$
$(\pm 12)^6 \equiv 4^6 \cdot 3^6 \mod 31$
$(\pm 13)^6 \equiv (\pm 1)^6 (13)^6 \equiv (-13)^6 \equiv (18)^6 \equiv\equiv 2^6 \cdot 9^6 \mod 31$
$(\pm 14)^6 \equiv 2^6 \cdot 7^6 \mod 31$
and in all these cases, we have already shown the right hand side to be a power of 2. Thus the admissable values for a are given by $a \in \{0, 1, 2, 4, 8, 16\}$.

Question 3

Solution. Euler's Criterion states that

$$1 = \left(\frac{a}{p} \right) \equiv a^{(p-1)/2} = a^{(8n+5-1)/2} = a^{4n+2} \mod p$$

Thus, we must have that $a^{2n+1} \equiv \pm 1 \mod p$ (since it squares to one and ± 1 are the two unique solutions to $x^2 \equiv 1 \mod p$ where uniqueness is due to the fact that p is a prime).
Case 1: $a^{2n+1} \equiv 1 \mod p$. In this case, we have
$(\pm a^{n+1})^2 \equiv a^{2n+2} \equiv a \cdot a^{2n+1} \equiv a \mod p$
Case 2: $a^{2n+1} \equiv -1 \mod p$. In this case, recall that $p \equiv 5 \mod 8$ and so a subcase of quadratic reciprocity says that (along with Euler's criterion again)
$-1 = \left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} = 2^{4n+2} \mod p.$
Using this, we have
$(\pm 2^{2n+1} a^{n+1})^2 \equiv 2^{4n+2} a^{2n+2} \equiv (-1) \cdot a \cdot a^{2n+1} \equiv (-1)a(-1) \equiv a \mod p$
and this completes the proof.

Question 4

SOLUTION. (a) Since $6! = 2^4 \cdot 3^2 \cdot 5$, Fermat's theorem says that in case (a) we must have a solution. (The curiously minded person should note that as $1^2 + 2^2 = 5$ then multiplying both sides by 12^2 gives $12^2 + 24^2 = 6!$).
(b) As $11 \parallel 12!$ and $11 \equiv 3 \mod 4$, this case has no solutions.
(c) As $23 \parallel 24!$ and $23 \equiv 3 \mod 4$, this case has no solutions.
(d) As $47 \parallel 48!$ and $47 \equiv 3 \mod 4$, this case has no solutions.

Question 5

SOLUTION. We proceed as in the hints. Suppose that in fact d was of the form $4n+3$. Then since
$(4k+1)(4m+1) = 4(4km + k + m) + 1$
we know that there must be a prime p of the form $p = 4j + 3$ that divides d. Reducing modulo p gives
$x^2 \equiv -1 \mod p$
This means that $\left(\frac{-1}{p}\right) = 1$. However, Euler's criterion tells us that $1 = \left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} = (-1)^{2j+1} = -1 \mod p$ and this is a contradiction.

Question 6

SOLUTION. Proceeding as in the hints, we see it suffices to show that the period of $\sqrt{4k^2+k}$ is even. First notice that
$(2k)^2 < 4k^2 + k < 4k^2 + 4k + 1 = (2k+1)^2$
and thus $\left\lfloor \sqrt{4k^2+k} \right\rfloor = 2k = a_0$ in the continued fraction expansion. As
$$\sqrt{4k^2+k} = a_0 + \frac{1}{a_1 + \ldots} = 2k + \frac{1}{a_1 + \ldots}$$
we see that after cross multiplying that

$$\begin{aligned}
a_1 &= \left\lfloor \frac{1}{\sqrt{4k^2+k}-2k} \right\rfloor \\
&= \left\lfloor \frac{\sqrt{4k^2+k}+2k}{(\sqrt{4k^2+k}+2k)(\sqrt{4k^2+k}-2k)} \right\rfloor \\
&= \left\lfloor \frac{\sqrt{4k^2+k}+2k}{4k^2+k-4k^2} \right\rfloor \\
&= \left\lfloor \frac{\sqrt{4k^2+k}+2k}{k} \right\rfloor \\
&= \left\lfloor \sqrt{4+1/k}+2 \right\rfloor \\
&= 4
\end{aligned}$$

As
$\sqrt{4k^2+k}-2k = \dfrac{1}{a_1+\frac{1}{a_2+\ldots}}$
cross multiplying gives us that
$a_1 + \dfrac{1}{a_2+\ldots} = \dfrac{1}{\sqrt{4k^2+k}-2k} = \sqrt{4+1/k}+2$
and thus as we know $a_1 = 4$,

$$\begin{aligned}
a_2 &= \left\lfloor \frac{1}{\sqrt{4+1/k}+2-a_1} \right\rfloor \\
&= \left\lfloor \frac{1}{\sqrt{4+1/k}+2-4} \right\rfloor \\
&= \left\lfloor \frac{1}{\sqrt{4+1/k}-2} \right\rfloor \\
&= \left\lfloor \frac{\sqrt{4+1/k}+2}{(\sqrt{4+1/k}+2)(\sqrt{4+1/k}-2)} \right\rfloor \\
&= \left\lfloor \frac{\sqrt{4+1/k}+2}{4+1/k-4} \right\rfloor \\
&= \left\lfloor k(\sqrt{4+1/k}+2) \right\rfloor \\
&= \left\lfloor \sqrt{4k^2+k}+2k \right\rfloor \\
&= 4k
\end{aligned}$$

Here we reduce back to the case of a_1. Hence, the continued fraction expansion is given by $\sqrt{4k^2+k} = [2k; \overline{4, 4k}]$. Thus the period of the continued fraction expansion is even and the theory of Pell equations states that the equation $x^2 - dy^2 = -1$ has no solution.

Question 7

SOLUTION. We proceed as in the hints. We factor the left hand side in $\mathbb{Q}(\sqrt{-11})$ as $(y+\sqrt{-11})(y-\sqrt{-11}) = x^3$.
Since $-11 \equiv 1 \mod 4$, the ring of integers here is given by $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ which is a unique factorization domain. We compute the greatest common divisor of the terms on the left hand side.

Let $I = (y + \sqrt{-11}, y - \sqrt{-11})$, the ideal generated by these two elements. Now notice that in the equation $y^2 = x^3 - 11$, if x is even, then modulo 8 considerations show that $y^2 \equiv 5 \mod 8$ and this is a contradiction since the only odd square is 1 modulo 8. Thus, x is odd and so y is even.
We may further suppose that these factors are coprime for otherwise, if a prime p divides both x and y, then it must divide 11 and hence must equal 11. Rewriting the equation would then give
$(11y')^2 + 11 = (11x')^3$
or simplified
$11(y')^2 + 1 = 121(x')^3$
and hence 11 divides 1 which is a contradiction. So y is even and x and y are coprime. Further, we have that
$(y + \sqrt{-11})(y - \sqrt{-11}) = x^3 \in I$
and that
$y + \sqrt{-11} + y - \sqrt{-11} = 2y \in I$
Hence $1 = \gcd(x, y) \in I$ and thus, the two elements $y + \sqrt{-11}, y - \sqrt{-11}$ are coprime. Thus, we may write

$$y + \sqrt{-11} = \pm \left(\frac{\alpha' + \beta'\sqrt{-11}}{2} \right)^3 = \left(\frac{\alpha + \beta\sqrt{-11}}{2} \right)^3$$

where above, the right hand side absorbs the units since $\pm 1 = (\pm 1)^3$ (and we relabeled the α', β' values) where $\alpha, \beta \in \mathbb{Z}$.
Expanding and comparing coefficients yields

$$\begin{aligned} 8y &= \alpha^3 - 33\alpha\beta^2 \\ 8\sqrt{-11} &= (3\alpha^2\beta - 11\beta^3)\sqrt{-11} \end{aligned}$$

or simplified

$$\begin{aligned} 8y &= \alpha^3 - 33\alpha\beta^2 \\ 8 &= \beta(3\alpha^2 - 11\beta^2) \end{aligned}$$

The second equation tells us that $\beta \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$ since it must be a factor of 8. Checking these 8 values shows that only $\beta = -1$ or $\beta = 2$ gives admissable values. This leads to the points
$(\alpha, \beta) = (\pm 1, -1)$ or $(\alpha, \beta) = (\pm 4, 2)$
The first point gives $y = \mp 4$ and the second point yields $y = \mp 29$. These correspond to the given points and thus complete the problem.

Question 8

SOLUTION. Note that $2^n + 1$ is odd for all values of n so the smallest prime factor must be odd. Then further, $2^{p-1} \equiv 1 \mod p$ by Fermat's Little Theorem. From the given, we know that $2^n \equiv -1 \mod p$ and thus
$2^{2n} \equiv (2^n)^2 \equiv (-1)^2 \equiv 1 \mod p$
Hence the order of 2 must be a divisor of $d = \gcd(2n, p-1)$ (you can see this by using the Euclidean algorithm to find an a and a b so that $a(p-1) + bn = d$ and then noting that $2^d = 2^{a(p-1)+bn} \equiv 1 \mod p$). As p is the smallest prime factor of n and as noted it is odd, we see that $\gcd(2n, p-1) = 2$. Since clearly $2 \equiv 1 \mod p$ is false, we see that $4 = 2^2 \equiv 1 \mod p$ which happens only when $p = 3$ as required.

Good Luck for your exams!