MT216.03: Introduction to Abstract Mathematics
Final Examination
Answers

1. (*10 points*) Use the Euclidean algorithm to find the smallest positive integer n so that

$$31n \equiv 4 \pmod{43}$$

or prove that there are no solutions.

Answer: We have

$$\begin{aligned}
43 &= 1 \cdot 31 + 12 \\
31 &= 2 \cdot 12 + \ \ 7 \\
12 &= 1 \cdot \ \ 7 + \ \ 5 \\
7 &= 1 \cdot \ \ 5 + \ \ 2 \\
5 &= 2 \cdot \ \ 2 + \ \ 1
\end{aligned}$$

Therefore,

$$\begin{aligned}
1 &= 1 \cdot 5 &&+ (-2)(2) \\
&= 1 \cdot 5 &&+ (-2)(7-5) \\
&= 3 \cdot 5 &&+ (-2)(7) \\
&= 3 \cdot (12-7) &&+ (-2)(7) \\
&= 3 \cdot 12 &&+ (-5)(7) \\
&= 3 \cdot 12 &&+ (-5)(31 - 2 \cdot 12) \\
&= 13 \cdot 12 &&+ (-5)(31) \\
&= 13 \cdot 12 &&+ (-5)(31) \\
&= 13 \cdot (43 - 31) &&+ (-5)(31) \\
&= 13 \cdot 43 &&+ (-18)(31)
\end{aligned}$$

Therefore, $31(-18) \equiv 1 \pmod{43}$, and so $31(-72) \equiv 4 \pmod{43}$. However, the problem asks for the smallest positive integer solving the congruence, so we need to note that $-72 \equiv 14 \pmod{43}$.

2. (*5 points*) Find a non-constant monic sixth degree polynomial $f(x) \in \mathbf{Z}[x]$ so that:

- $f(3) = f'(3) = 0$
- $f(5) = f'(5) = f''(5) = 0$
- $f(6) = 0$

or prove that no such polynomial exists. You can state your answer as a product of irreducible polynomials.

Answer: $f(x) = (x-3)^2(x-5)^3(x-6)$.

3. (*5 points*) On my calculator, I can compute that

$$\begin{aligned}
2^{8910} &\equiv 1 \pmod{8911} \\
3^{8910} &\equiv 1 \pmod{8911} \\
(2, 8911) &= 1 \\
(3, 8911) &= 1
\end{aligned}$$

Based on these computations, which of the following conclusions can be drawn?

(*a*) 8911 is definitely composite.
(*b*) 8911 is definitely prime.
(*c*) 8911 could be either prime or composite.

Be sure to explain your answer.

Answer: If 8911 were prime, then Fermat's Little Theorem tells us that $a^{8910} \equiv 1 \pmod{8911}$ for $a = 1, 2, \ldots, 8910$. However, the given information is the converse of the theorem, and so the correct answer based on these congruences is (*c*). In fact, $7 \cdot 19 \cdot 67$.

4. (*10 points*) A horde of 12 Mongol invaders has raided a castle, and found a treasure trove of gold coins. The invaders attempt to divide the pile of coins evenly, and find that there are 3 remaining. A mêlée ensues, and 5 of the invaders die. The remaining 7 members of the horde try again to divide the coins evenly, and now there are 4 coins left over. Another fight ensues, and 2 more invaders die. The remaining 5 marauders now divide the pile evenly.

What is the smallest number of coins that could be in the trove?

Answer: We need to solve the congruences

$$\begin{aligned} n &\equiv 3 \pmod{12} \\ n &\equiv 4 \pmod{7} \\ n &\equiv 0 \pmod{5} \end{aligned}$$

The first congruence tells us that $n = 12k + 3$. Substitution into the second congruence yields $12k + 3 \equiv 4 \pmod 7$, or $5k \equiv 1 \pmod 7$. This congruence has solution $k \equiv 3 \pmod 7$, so $k = 7j + 3$. Therefore, $n = 12(7j + 3) + 3 = 84j + 39$.

We now solve $84j + 39 \equiv 0 \pmod 5$. That simplifies to $4j \equiv 1 \pmod 5$, with solution $j \equiv 4 \pmod 5$, so $j = 5m + 4$, and $n = 84(5m + 4) + 39 = 420m + 336 + 39 = 420m + 375$. Therefore, the smallest number of coins that could be in the trove is 375.

5. (*10 points*) Let n be a positive integer. Prove using induction that

$$\int_0^1 (1 - x^2)^n \, dx = \frac{2^{2n}(n!)^2}{(2n + 1)!}.$$

Hint: Use the identity $(1 - x^2)^n = (1 - x^2)^{n-1} - x^2(1 - x^2)^{n-1}$ and integrate by parts.

Answer: We first check that the formula is correct when $n = 1$. We have $\int_0^1 (1 - x^2)\, dx = x - x^3/3\Big|_0^1 = 2/3$, while $\dfrac{2^2(1!)^2}{3!} = 4/6$.

Now, assuming that $\int_0^1 (1 - x^2)^k \, dx = \dfrac{2^{2k}(k!)^2}{(2k + 1)!}$, we have

$$\begin{aligned} \int_0^1 (1 - x^2)^{k+1} \, dx &= \int_0^1 (1 - x^2)^k \, dx + \int_0^1 x(-x)(1 - x^2)^k \, dx \\ &= \frac{2^{2k}(k!)^2}{(2k + 1)!} + \int_0^1 x(-x)(1 - x^2)^k \, dx \end{aligned}$$

$\Big[u = x,\ du = dx,\ dv = (-x)(1 - x^2)^k,\ v = (1 - x^2)^{k+1}/(2k + 2)\Big]$

$$\begin{aligned} &= \frac{2^{2k}(k!)^2}{(2k + 1)!} + x\ \frac{(1 - x^2)^{k+1}}{2k + 2}\Bigg|_0^1 - \frac{1}{2k + 2} \int_0^1 (1 - x^2)^{k+1} \, dx \\ &= \frac{2^{2k}(k!)^2}{(2k + 1)!} - \frac{1}{2k + 2} \int_0^1 (1 - x^2)^{k+1} \, dx \\ \frac{2k + 3}{2k + 2} \int_0^1 (1 - x^2)^{k+1} \, dx &= \frac{2^{2k}(k!)^2}{(2k + 1)!} \\ \int_0^1 (1 - x^2)^{k+1} \, dx &= \left(\frac{2k + 2}{2k + 3}\right) \frac{2^{2k}(k!)^2}{(2k + 1)!} = \left(\frac{2k + 2}{2k + 3}\right)\left(\frac{2k + 2}{2k + 2}\right) \frac{2^{2k}(k!)^2}{(2k + 1)!} \\ &= \frac{2^{2k+2}((k + 1)!)^2}{(2k + 3)!}. \end{aligned}$$

This is the desired conclusion to establish the induction.

6. (*10 points*) Remember that the set μ_{1000} is defined by $\mu_{1000} = \{z \in \mathbf{C} \mid z^{1000} = 1\}$. Let j be a positive integer, and define $f : \mu_{1000} \to \mu_{1000}$ with the formula $f(x) = x^j$.

(*a*) If $(j, 1000) = 1$, prove that f is a bijection.

(*b*) If $(j, 1000) \neq 1$, prove that f is not a bijection.

Answer: (*a*) Suppose that $(j, 1000) = 1$. Find integers m and n so that $jm + 1000n = 1$. Let $g : \mu_{1000} \to \mu_{1000}$ be defined by the formula $g(x) = x^m$. Then $f(g(x)) = g(f(x)) = x^{mj} = x^{1-1000n} = x^1(x^{1000})^{-n} = x \cdot 1^{-n} = x$. Because $f \circ g$ and $g \circ f$ are both the identity, f is invertible, and therefore a bijection.

(*b*) This can be done in general, but it's a bit more enlightening to take advantage of numerical properties of 1000. Suppose that $(j, 1000) \neq 1$. Because $1000 = 2^3 5^3$, we can conclude that either $2 | j$ or $5 | j$.

Suppose first that $2|j$. In that case $f(-1) = (-1)^j = 1$ and $f(1) = 1^j = 1$, so f is not an injection.

On the other hand, if $5|j$, we have $f(e^{2\pi i/5}) = e^{2\pi ij/5} = 1$ and $f(1) = 1$, so again we see that f is not an injection.

7. (*10 points*) Define a sequence $\{x_n\}$ with the formulas

$$x_1 = 2$$
$$x_{n+1} = \sqrt{4 + x_n} \qquad n \geq 1$$

For example, $x_2 = \sqrt{6}$ and $x_3 = \sqrt{4 + \sqrt{6}}$.

Prove

(a) $x_n \leq 3$.

(b) $x_n \leq x_{n+1}$.

Answer: (a) We proceed by induction. When $n = 1$, we clearly have $x_n \leq 3$.

If we have $x_k \leq 3$, then $x_{k+1} = \sqrt{4 + x_k} \leq \sqrt{4 + 3} = \sqrt{7} \leq 3$. That establishes the induction.

(b) We proceed by induction. We have $x_1 = 2$ and $x_2 = \sqrt{6}$, so $x_1 \leq x_2$.

Now, assuming that $x_k \leq x_{k+1}$, we have $4 + x_k \leq 4 + x_{k+1}$. Therefore, $\sqrt{4 + x_k} \leq \sqrt{4 + x_{k+1}}$, and so $x_{k+1} \leq x_{k+2}$, establishing the induction.

8. (*5 points*) Find 3 complex numbers which solve the equation $z^3 = 7$. Write each of those numbers in the form $a + bi$, where a and b are real numbers expressed using radicals.

Answer: Write $z = re^{i\theta}$, so $z^3 = r^3 e^{3i\theta}$. We therefore have $r^3 = 7$, so $r = \sqrt[3]{7}$. We also have $e^{3i\theta} = 1$, with three possibilities:

$$3\theta = 0$$
$$3\theta = 2\pi$$
$$3\theta = 4\pi$$

In the first case, we have $\theta = 0$ and $z = \sqrt[3]{7}$. In the second, we have $\theta = 2\pi/3$, and $z = \sqrt[3]{7}e^{2\pi i/3} = \sqrt[3]{7}(\cos(2\pi/3) + i\sin(2\pi/3)) = \sqrt[3]{7}(-1/2 + i\sqrt{3}/2)$. In the third case, we conclude that $z = \sqrt[3]{7}(-1/2 - i\sqrt{3}/2)$. The three answers are

$$\sqrt[3]{7} + 0i \qquad -\frac{\sqrt[3]{7}}{2} + i\frac{\sqrt{3}\sqrt[3]{7}}{2} \qquad -\frac{\sqrt[3]{7}}{2} - i\frac{\sqrt{3}\sqrt[3]{7}}{2}$$

9. (*5 points*) There are 9 monic quadratic polynomials in $\mathbf{F}_3[x]$. List all 9 of these polynomials, and indicate which are irreducible.

Answer: To see if a quadratic polynomial is irreducible in $\mathbf{F}_3[x]$, it suffices to see if it has any roots in $\mathbf{F}_3$, which can be determined by computing $f(0)$, $f(1)$, and $f(2)$. We have

Polynomial	$f(0)$	$f(1)$	$f(2)$	Irreducible?
x^2	0	1	1	N
$x^2 + 1$	1	2	2	Y
$x^2 + 2$	2	0	0	N
$x^2 + x$	0	2	0	N
$x^2 + x + 1$	1	0	1	N
$x^2 + x + 2$	2	1	2	Y
$x^2 + 2x$	0	0	2	N
$x^2 + 2x + 1$	1	1	0	N
$x^2 + 2x + 2$	2	2	1	Y

Therefore, the irreducible polynomials are $x^2 + 1$, $x^2 + x + 2$, and $x^2 + 2x + 2$.

10. (*10 points*) As usual, define the Fibonacci numbers by $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Let $\alpha = \frac{1}{2}(1 + \sqrt{5})$ and $\beta = \frac{1}{2}(1 - \sqrt{5})$. You may use the facts that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$.

Prove using induction that

$$F_{n+1} = \alpha F_n + \beta^n$$

for $n \geq 1$.

Answer: We check that when $n = 1$, we get $F_2 = 1$, and $\alpha F_1 + \beta = \alpha + \beta = 1$. We also need to check the formula for $n = 2$, and then we have $F_3 = 2$, and $\alpha F_2 + \beta^2 = \alpha + \beta + 1 = 1 + 1 = 2$.

We now proceed using strong induction. We assume that the statement is true when $n = k - 2$ and $n = k - 1$, and add:

$$\begin{aligned} F_{k-1} &= \alpha F_{k-2} + \beta^{k-2} \\ F_k &= \alpha F_{k-1} + \beta^{k-1} \end{aligned}$$

Adding yields $F_{k+1} = \alpha(F_{k-2} + F_{k-2}) + \beta^{k-2} + \beta^{k-1} = \alpha F_k + \beta^{k-2}(1+\beta) = \alpha F_k + \beta^{k-2}\beta^2 = \alpha F_k + \beta^k$. This establishes the induction.

11. (*10 points*) Suppose that n and k are positive integers, with $n > k > 1$. Prove using the definition of binomial coefficient that

$$\binom{n-1}{k-1}\binom{n}{k+1}\binom{n+1}{k} = \binom{n-1}{k}\binom{n+1}{k+1}\binom{n}{k-1}.$$

Answer: We have

$$\begin{aligned} \binom{n-1}{k-1}\binom{n}{k+1}\binom{n+1}{k} &= \left(\frac{(n-1)!}{(n-k)!(k-1)!}\right)\left(\frac{n!}{(n-k-1)!(k+1)!}\right)\left(\frac{(n+1)!}{(n+1-k)!k!}\right) \\ &= \left(\frac{(n-1)!}{(n-1-k)!k!}\right)\left(\frac{(n+1)!}{(n-k)!(k+1)!}\right)\left(\frac{n!}{(k-1)!(n+1-k)!}\right) \\ &= \binom{n-1}{k}\binom{n+1}{k+1}\binom{n}{k-1}. \end{aligned}$$

12. (*10 points*) Suppose that F is a field, and $f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 \in F[x]$, with $n \geq 2$. Suppose that $\gamma_1, \gamma_2, \ldots, \gamma_n \in F$ are the n roots of $f(x)$. Prove that

$$c_0 = (-1)^n \gamma_1\gamma_2\cdots\gamma_n$$

and

$$c_{n-1} = -(\gamma_1 + \gamma_2 + \cdots + \gamma_n)$$

Answer: We know that $f(x) = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3)\cdots(x-\gamma_n)$. Substitution of $x = 0$ yields $c_0 = (-\gamma_1)(-\gamma_2)\cdots(-\gamma_n) = (-1)^n\gamma_1\gamma_2\cdots\gamma_n$.

We can also multiply out the factorization of $f(x)$, and look at the coefficient of x^{n-1}. The way to get x^{n-1} in the product is to have $n-1$ factors of x and one factor of $-\gamma_k$. We conclude that the x^{n-1} term looks like $(-\gamma_1 - \gamma_2 - \cdots - \gamma_n)x^{n-1}$. Because we know that the x^{n-1} term is also $c_{n-1}x^{n-1}$, we have $c_{n-1} = -\gamma_1 - \gamma_2 - \cdots - \gamma_n$.

Grade	Number of people
86	1
83	1
80	1
73	1
72	3
71	1
70	2
65	1
61	1
43	1

Mean: 70.62
Standard deviation: 10.29