MT216.03: Introduction to Abstract Mathematics
Examination 3
Answers

1. (*20 points*) Let $f(x), g(x) \in \mathbf{F}_7[x]$, with $f(x) = 5x^2 + x + 2$ and $g(x) = 2x + 3$. Compute the monic greatest common divisor $d(x)$ of f and g, and find polynomials $a(x), b(x) \in \mathbf{F}_7[x]$ so that $d(x) = a(x)f(x) + b(x)g(x)$.

Answer: We start with long division:

$$\begin{array}{r|l} & 6x \ \ +2 \\ \hline 2x+3 & 5x^2 + \ \ x + 2 \\ & \underline{5x^2 + 4x} \\ & \qquad 4x + 2 \\ & \qquad \underline{4x + 6} \\ & \qquad\qquad 3 \end{array}$$

Therefore, $f(x) = (6x+2)g(x) + 3$, and so $3 = f(x) - (6x+2)g(x) = f(x) + (x+5)g(x)$. Multiply by 5, and we have $1 = 5f(x) + (5x+4)g(x)$.

2. (*10 points*) What is the remainder when 3^{75} is divided by 36?

Answer: We know that $3^{75} \equiv 0 \pmod 9$. We can use Euler's Theorem to see that $3^{\phi(4)} \equiv 1 \pmod 4$. Because $\phi(4) = 2$, we know that $3^2 \equiv 1 \pmod 4$, and therefore $3^{75} \equiv 3^{74}3 \equiv 3 \pmod 4$. We now have a Chinese Remainder Theorem problem:

$$3^{75} \equiv 0 \pmod 9$$
$$3^{75} \equiv 3 \pmod 4$$

You can either solve this systematically, or else just observe after trial and error (trying multiples of 9) that a solution is $3^{75} \equiv 27$. Therefore, the remainder is 27.

3. (*10 points*) Give an example of a degree 6 polynomial which you can show is irreducible by using Eisenstein's Criterion. Be sure to explain your answer.

Answer: Take $p = 2$, and take the polynomial $x^6 + 2$. We see that 2 does not divided the highest coefficient, and 2 divides every other coefficient, and 2^2 does not divide the constant term.

4. (*20 points*) Suppose that $f(x), g(x) \in \mathbf{C}[x]$ and we know that

- $\deg(f) = \deg(g) = n$, with $n \geq 1$.
- $f(1) = g(1)$, $f(2) = g(2)$, $\ldots$, $f(n) = g(n)$.
- $f'(1) = g'(1)$.

Prove or give a counterexample: $f(x) = g(x)$.

Answer: This statement is true.

Let $h(x) = f(x) - g(x)$, and then if $h(x) \neq 0$, we have $\deg(h) \leq n$. We know that $h(1) = h(2) = \cdots = h(n)$, and so h must be divisible by $(x-1)(x-2)\cdots(x-n)$. That is not yet a contradiction.

However, if $h(1) = h'(1) = 0$, we know that $(x-1)^2$ must divide $h(x)$, and so in fact $(x-1)^2(x-2)\cdots(x-n)|h(x)$. Now, a polynomial of degree $n+1$ cannot divide a polynomial of degree n. The only resolution is to conclude that $h(x) = 0$, and then $f(x) = g(x)$.

5. (*20 points*) List all eight cubic polynomials in $\mathbf{F}_2[x]$, and indicate which of them are irreducible in $\mathbf{F}_2[x]$. Be sure to explain your answer fully.

Answer: To see if a cubic polynomial in $\mathbf{F}_2[x]$ is irreducible, it suffices to see if it has a root in $\mathbf{F}_2$, which amounts to substituting $x = 0$ and $x = 1$ into the polynomial and evaluating. The results are:

Polynomial	$f(0)$	$f(1)$	Irreducible?
x^3	0	1	N
$x^3 + 1$	1	0	N
$x^3 + x$	0	0	N
$x^3 + x + 1$	1	1	Y
$x^3 + x^2$	0	0	N
$x^3 + x^2 + 1$	1	1	Y
$x^3 + x^2 + x$	0	1	N
$x^3 + x^2 + x + 1$	1	0	N

There are two irreducible cubic polynomials in $\mathbf{F}_2[x]$: $x^3 + x + 1$ and $x^3 + x^2 + 1$.

6. (*20 points*) Let $f : \mathbf{Z} \to \mathbf{Q}$ be defined by the formula $f(n) = \dfrac{n}{2n^2 - 1}$.
   (*a*) Is f a surjective function?
   (*b*) Is f an injective function?

Answer: (*a*) The function f is not surjective. To see this, we try to solve $f(n) = 2$, and we are led to the equation $n = 4n^2 - 2$, or $4n^2 - n - 2 = 0$. The solutions are $n = \dfrac{1 \pm \sqrt{33}}{2}$. Because the two roots are not elements of $\mathbf{Z}$, we see that the function is not surjective.

(*b*) This function is injective. Suppose that $f(n) = f(m)$, with $n, m \in \mathbf{Z}$, and $n \neq m$. We have

$$\begin{aligned}
\frac{n}{2n^2 - 1} &= \frac{m}{2m^2 - 1} \\
2nm^2 - n &= 2mn^2 - m \\
2nm^2 - 2mn^2 &= n - m \\
2mn(m - n) &= n - m \\
2mn &= -1
\end{aligned}$$

This equation has no solutions with $m, n \in \mathbf{Z}$, and therefore the function is injective.

Grade	Number of people
79	1
77	1
73	1
70	1
57	1
55	1
51	1
50	1
47	1
46	1
42	1
38	1
35	1

Mean: 55.38
Standard deviation: 14.29