HW 9

Charles Liu

Elementary Modern Algebra - Dr. Ben Clark

April 15th, 2025

---

1. How many zeros does $x^2 + 3x + 2$ have in $\mathbb{Z}_6$? How about $\mathbb{Z}_7$?

In $\mathbb{Z}_6$

$x^2 + 3x + 2 = (x + 2)(x + 1)$

So the zeros are 4 and 5, so two zeroes.

In $\mathbb{Z}_7$

The zeroes are $5, 6$, so also two zeroes.

---

2. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ be polynomials in $\mathbb{Z}_7[x]$. Determine the quotient and remainder upon dividing $f(x)$ by $g(x)$.

$$\begin{array}{rl}
 & 4x^2 + 3x + 6 \\
 & \text{-----------} \\
3x^2 + 2x + 1 & | \; 5x^4 + 3x^3 + 1 \\
 & 5x^4 + x^3 + 4x^2 \\
 & \qquad 2x^3 + 3x^2 + 1 \\
 & \qquad 2x^3 + 6x^2 + 3x \\
 & \qquad\qquad 4x^2 + 4x + 1 \\
 & \qquad\qquad 4x^2 + 5x + 6 \\
 & \qquad\qquad\qquad 6x + 2
\end{array}$$

Quotient: $4x^2 + 3x + 6$

Remainder: $6x + 2$

---

3. Show that $2x + 1$ has a multiplicative inverse in $\mathbb{Z}_4$.

Consider $a, b \in \mathbb{Z}_4$.
$(2x+1)(ax+b) = 1 \implies 2ax^2 + 2bx + ax + b = 1$
So, $b = 1, a = 2$.
Thus, $2x + 1$ has a multiplicative inverse, $2x + 1$, which is in $\mathbb{Z}_4$.

---

4. Find a polynomial with integer coefficients that has 1/2 and −1/3 as zeros.

First consider the polynomial $(x - 1/2)(x + 1/3) = 0$
This doesn't have integer coefficients, so we scale the first left component by 2 and the second by 3
$2(x - 1/2)3(x + 1/3) = (2x - 1)(3x + 1) = 0.$

So a polynomial is $(2x - 1)(3x + 1) = 6x^2 - x - 1 = 0$

---

5. Find infinitely many polynomials $f(x)$ in, $\mathbb{Z}_3[x]$ such that $f(a) = 0$ for all $a \in \mathbb{Z}_3$.

We want the polynomial to have the zeroes $0, 1, 2$, or all the elements in $\mathbb{Z}_3$.

Consider the polynomial
$(x-0)(x-1)(x-2) = x^2 - 3x + 2$
Convert this to a polynomial in $\mathbb{Z}_3[x]$, and we get
$g(x) = x^2 + 2.$
From its construction, $0, 1, 2$ must be zeroes of the polynomial.

Also consider that $f(x) = x^n g(x) = x^{2+n} + 2x^n \ \forall\ n \geq 0, n \in \mathbb{Z}$ has the zeroes $0, 1, 2$. Since there are infinite such polynomials, any polynomial of that form will satisfy $f(a) = 0$ for all $a \in \mathbb{Z}_3$.

---

6. Prove that the ideal $\langle x \rangle$ in $\mathbb{Q}[x]$ is maximal.

Proof:
If $\langle x \rangle$ is an ideal in $Q[x]$, then if $\langle x \rangle \subseteq I \subseteq \mathbb{Q}[x]$, either $\langle x \rangle = I$ or $I = \mathbb{Q}[x]$.

Assume $\langle x \rangle \subsetneq I$. Then there must be some element, $f(x) \notin \langle x \rangle$, where $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ where $a_0 \neq 0$ and $a_1, \ldots, a_n \in \mathbb{Q}$. Also consider $g(x) = a_1 x + a_2 x^2 + \ldots + a_n x^n \in \langle x \rangle \subset I$. Then $f(x) - g(x) = a_0 \in I$. Since $a_0 \neq 0$, a_0^{-1} exists and is in $\mathbb{Q}[x]$. Thus $a_0 a_0^{-1} = 1 \in I$, so $I = \mathbb{Q}[x]$.

---

7. Prove that $(50!)^2 \bmod 101 = -1 \bmod 101$.

Proof:

We can solve that

$(50!)^2 \bmod 101 = 50! \times (-51 \times -52 \times \ldots -100) \bmod 101 = 100! \bmod 101 = -1$

(By Wilson's Theorem).