MATH 220

Discrete Mathematics and Cryptography

Tutorial 6 **Week starting 27 April 2020**

---

1. Let $f(x) = x^3 + 2x + 4$ and $g(x) = 3x + 2$ in $\mathbb{Z}_5[x]$. Find the quotient and remainder when $f(x)$ is divided by $g(x)$.

2. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$. Find the quotient and remainder when $f(x)$ is divided by $g(x)$.

3. Factor into irreducible polynomials the polynomial $x^{12} + x^{10} + x^7 + x^6 + 1$ in $\mathbb{Z}_2[x]$.

4. Find all irreducible quadratic and cubic *monic* polynomials in $\mathbb{Z}_3[x]$.

5. Find the possible values of a so that the polynomial $x^2 + ax + 1$ is *irreducible* in $\mathbb{Z}_5[x]$.

6. Suppose that $f(x)$ is a polynomial of degree n. Define $\bar{f}(x) = x^n f(\frac{1}{x})$. Find $\bar{f}(x)$ in each of the cases

(a) $f(x) = x^3 + x + 1$,

(b) $f(x) = x^5 + x + 1$, and

(c) $f(x) = x^4 + x^2 + 1$.

It can be shown that if $f(x)$ is irreducible, then so is $\bar{f}(x)$. Why?

7. Find all irreducible quartic polynomials in $\mathbb{Z}_2[x]$.

8. Consider the recursive formula

$$s_{n+1} = c\, s_n \mod 26$$

where c is a fixed integer. Show (treating examples if nothing else) that the largest possible period of a keystream generated by this recursion is 12.

9. Consider the recursive formula

$$s_{n+1} = 7s_n + 2 \mod 13$$

with seed $s_0 = 6$. What is the smallest index n such that s_n returns to the value 6? Does the length of the period depend on the seed? Find the single "bad" seed x_{bad} such that the keystream is constant with that value.

10. Find the period of the linear feedback shift register defined by

$$s_{n+1} = s_n + s_{n-1} + s_{n-2} + s_{n-3}$$

in $\mathbb{Z}_2$ with seed $(s_0, s_1, s_2, s_3) = (0, 1, 0, 0)$.

11. Consider a linear feedback shift register defined by

$$s_{n+1} = s_n - s_{n-1}$$

with *real* numbers s_i. Show that, for any choice of seed $s = (s_0, s_1)$, this gives a periodic keystream whose period is a divisor of 6.