Math 580/780I Notes 11

Polynomial Basics:

• Irreducible polynomials. A non-zero polynomial $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv \pm 1$ is *irreducible* (over $\mathbb{Z}$ or in $\mathbb{Z}[x]$) if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ implies either $g(x) \equiv \pm 1$ or $h(x) \equiv \pm 1$. A non-zero polynomial $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv \pm 1$ is *reducible* if $f(x)$ is not irreducible. A non-constant polynomial $f(x) \in \mathbb{Q}[x]$ is *irreducible over* $\mathbb{Q}$ (or in $\mathbb{Q}[x]$) if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Q}[x]$ implies either $g(x)$ or $h(x)$ is a constant. A non-constant polynomial $f(x) \in \mathbb{Q}[x]$ is *reducible over* $\mathbb{Q}$ if $f(x)$ is not irreducible over $\mathbb{Q}$.

• **Examples.** The polynomial $x^2 + 1$ is irreducible over $\mathbb{Z}$ and over $\mathbb{Q}$. The polynomial $2x^2 + 2$ is reducible over $\mathbb{Z}$ and irreducible over $\mathbb{Q}$.

• **Comment:** Suppose $f(x) \in \mathbb{Z}[x]$ and the greatest common divisor of the coefficients of $f(x)$ is 1. Then $f(x)$ is irreducible over the integers if and only if $f(x)$ is irreducible over the rationals.

• Unique factorization in $\mathbb{Z}[x]$. It exists.

• Division algorithm for polynomials. Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ with $g(x) \not\equiv 0$, there are unique polynomials $q(x)$ and $r(x)$ in $\mathbb{Q}[x]$ such that $f(x) = q(x)g(x) + r(x)$ and either $r(x) \equiv 0$ or $\deg r(x) < \deg g(x)$. In the case where $g(x)$ is monic, the polynomials $q(x)$ and $r(x)$ will be in $\mathbb{Z}[x]$.

• **Examples.** If $f(x) = x^3 + 2x + 1$ and $g(x) = x^2 + 2$, then $q(x) = x$ and $r(x) = 1$. If $f(x) = x^4 + 4$ and $g(x) = 2x^3 - 3x^2 + 2$, then $q(x) = \dfrac{1}{2}x + \dfrac{3}{4}$ and $r(x) = \dfrac{9}{4}x^2 - x + \dfrac{5}{2}$.

• The Euclidean Algorithm. Illustrate by computing $\gcd(x^9 + 1, x^8 + x^4 + 1)$. Note that this example is not meant to be typical; in general the coefficients might not be integral. If we want $\gcd(f(x), g(x))$ to be monic, then division by a constant may be necessary after performing the Euclidean algorithm.

• Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, not both $\equiv 0$, there exist polynomials $u(x)$ and $v(x)$ in $\mathbb{Q}[x]$ such that

$$f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x)).$$

The Euclidean algorithm can be used to compute such $u(x)$ and $v(x)$.

• The Remainder Theorem. The remainder when a polynomial $f(x)$ is divided by $x - a$ is $f(a)$. Observe that the division algorithm for polynomials implies that there is a polynomial $q(x) \in \mathbb{Q}[x]$ and a rational number r such that $f(x) = (x - a)q(x) + r$; the remainder theorem follows by letting $x = a$. As a corollary, we note that $(x - a)|f(x)$ if and only if $f(a) = 0$.

• The Fundamental Theorem of Algebra. A non-zero polynomial $f(x) \in \mathbb{C}[x]$ of degree n has exactly n complex roots when counted to their multiplicity. In other words, if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x]$ is a non-zero polynomial with roots (counted to their multiplicity) $\alpha_1, \alpha_2, \ldots, \alpha_n$, then

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

• Elementary Symmetric Functions. Expanding the above factorization of $f(x)$ in terms of its roots, we deduce that

$$f(x) = a_n\big(x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n\big)$$

where

$$\sigma_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_n,\ \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n,\ \ldots,\ \sigma_n = \alpha_1\alpha_2\cdots\alpha_n$$

(in general, σ_j is the sum of the roots of $f(x)$ taken j at a time). We deduce the formula $\sigma_j = (-1)^j a_{n-j}/a_n$ for each $j \in \{1, 2, \ldots, n\}$. Any rational symmetric function of $\alpha_1, \alpha_2, \ldots, \alpha_n$ can be written in terms of the *elementary* symmetric functions σ_j.

• **Examples.** Discuss the values of σ_j when $f(x) = x^2 - 3x + 2 = (x-1)(x-2)$. Also, given $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are the roots of $f(x) = x^4 + 2x^3 - 3x + 5$, compute the value of $(1/\alpha_1) + (1/\alpha_2) + (1/\alpha_3) + (1/\alpha_4)$.

• Congruences Modulo Polynomials. Is $x^{18} - 3x^{15} + x^6 - x^4 + 2x^3 - x^2 - 2$ divisible by $x^2 + x + 1$? If not, what's the remainder? Discuss the answer(s).

Homework:

(1) Calculate $\gcd(x^5 - 3x^4 + 3x^3 - 6x^2 + 2x - 3, x^4 - 3x^3 + 2x^2 - 3x + 1)$.

(2) Using your computations from Homework (1) above, find $u(x)$ and $v(x)$ satisfying

$$\begin{aligned}(x^5 - 3x^4 + 3x^3 - 6x^2 + 2x - 3)u(x) + (x^4 - 3x^3 + 2x^2 - 3x + 1)v(x)\\ = \gcd(x^5 - 3x^4 + 3x^3 - 6x^2 + 2x - 3, x^4 - 3x^3 + 2x^2 - 3x + 1).\end{aligned}$$

(3) For each given $f(x)$ and $g(x)$ below, determine whether $f(x)$ is divisible by $g(x)$?

(a) $f(x) = x^{2010} - 3x^{276} + 2$ and $g(x) = x + 1$

(b) $f(x) = x^{2010} - 3x^{276} + 2$ and $g(x) = x - 1$

(c) $f(x) = x^6 - 3x^4 - x^3 - 5x + 2$ and $g(x) = x - 2$

(4) Determine whether $x^4 + 1$ is a factor of $x^{25} + 2x^{23} + x^{17} + x^{13} + x^7 + x^3 + 1$ using arithmetic modulo $x^4 + 1$.

(5) Let α_1, α_2, and α_3 be the roots of $x^3 + x + 1 = 0$. Calculate

$$S_k = \sum_{j=1}^{3} \alpha_j^k \quad \text{for } k = 1, 2, 3, 4 \text{ and } 5.$$

(6) Consider all lines which meet the graph on $y = 2x^4 + 7x^3 + 3x - 5$ in four distinct points, say $(x_i, y_i), i = 1, 2, 3, 4$. Show that $(x_1 + x_2 + x_3 + x_4)/4$ is independent of the line and find its value.

Challenge Problem:

In Homework (6), do the following as well.

(a) Show that the average of the x_j^2's is independent of the line and find its value.

(b) Determine whether the average of the y_j's is independent of the line. Justify your answer.