REU APPRENTICE CLASS #13

INSTRUCTOR: LÁSZLÓ BABAI
SCRIBE: MARKUS KLIEGL

Thursday, July 14, 2011

1. Cyclic Groups, The Fundamental Theorem of Arithmetic, Greatest Common Divisors of Polynomials

Recall the Division Theorem: If $a, b \in \mathbb{Z}$, then there exist $q, r \in \mathbb{Z}$ such that $a = q \cdot b + r$ and $0 \leq r < b$. This is the key ingredient for proving most of the results below.

Definition 1.1. d is a *g.c.d.* of a and b if (1) d is a common divisor of a and b (that is, $d \mid a$ and $d \mid b$), and (2) any common divisor of a and b divides d, that is $(\forall e)$(if $e \mid a$ and $e \mid b$ then $e \mid d$).

Theorem 1.2. *A g.c.d. of a and b always exists and can be written as $d = ax + by$.*

Definition 1.3. A group G is *cyclic* if $(\exists g \in G)(G = \langle g \rangle)$ where $\langle g \rangle$ denotes the subgroup generated by g. That is,

$$\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots\} = \{g^n \mid n \in \mathbb{Z}\}.$$

Observe that $|\langle g \rangle| = \mathrm{ord}(g)$. If $\mathrm{ord}(g) = t$ then $g^i = g^j \Leftrightarrow i \equiv j \pmod{t}$ (this means $t \mid i - j$). (Take $t = 0$ if $\mathrm{ord}(g) = \infty$.)

$(\mathbb{Z}, +)$ is a cyclic group: $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$. Observe that $\mathbb{Z} = \langle a, b \rangle$ if and only if $\gcd(a, b) = 1$. This is not entirely evident and we shall prove it.

Theorem 1.4. *All subgroups of $(\mathbb{Z}, +)$ are cyclic. That is, the subgroups of $(\mathbb{Z}, +)$ are precisely the groups*

$$d\mathbb{Z} := \{dn \mid n \in \mathbb{Z}\} = \textit{multiples of } d = \langle d \rangle = \langle -d \rangle \qquad (d \in \mathbb{Z}).$$

Convention 1.5. Observe that the g.c.d. of a and b is unique up to sign. When we write $\gcd(a, b)$, we mean the positive sign.

Theorem 1.6. $\gcd(ac, bc) = |c| \cdot \gcd(a, b)$.

Theorem 1.7. *If p is a prime then $(\forall a, b)$(if $p \mid ab$ then $p \mid a$ or $p \mid b$). This is called the* prime property.

(Note that 0 also has the prime property.) Note that the Fundamental Theorem of Arithmetic (unique prime factorization) immediately follows from Theorem 1.7.

Our next goal is to prove uniqueness of factorization of polynomials over a field F into irreducible polynomials.

For F a field, $F[x]$ is the set of polynomials over F. We can define the gcd as above; this time it will be unique up to nonzero constant factors.

Convention 1.8. When we write $\gcd(f, g)$ for $f, g \in F[x]$, we mean the gcd with leading coefficient 1 (so $\gcd(f, g)$ is a *monic* polynomial).

Theorem 1.9 (Existence of gcd)**.** *For all $f, g \in F[x]$, there exists $d \in F[x]$ such that*

(1) *$d \mid f$ and $d \mid g$,*
(2) *$(\forall e \in F[x])$(if $e \mid f$ and $e \mid g$ then $e \mid d$),*
(3) *$(\exists u, v \in F[x])(d = u \cdot f + v \cdot g)$.*

Problem 114. Prove Theorem 1.9.

Problem 115. Let $f \in \mathbb{Q}[x]$. Then f has a multiple root in $\mathbb{C}$ if and only if $\gcd(f, f') \neq 1$.

2. Euler-Fermat Congruence and Arithmetic Functions

Theorem 2.1 (Lagrange's Theorem)**.** *If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.*

Corollary 2.2. *If G is a finite group, then* $\operatorname{ord}(g)$ *divides $|G|$ for all $g \in G$.*

Recall that $\operatorname{ord}(g) = \min\{k \geq 1 \mid g^k = 1\}$. Observe that if $\operatorname{ord}(g) = t$, then $(\forall n \in \mathbb{Z})(q^n = 1 \Leftrightarrow t \mid n)$.

Applying Corollary 2.2 to $G = \mathbb{F}_q^\times$, we find that if $a \in \mathbb{F}_q$ and $a \neq 0$, then $a^{q-1} = 1$. Taking q to be prime, we get Fermat's Little Theorem.

Theorem 2.3 (Fermat's Little Theorem)**.** *For all $a \in \mathbb{Z}$, if a does not divide p, then $a^{p-1} \equiv 1 \pmod{p}$.*

Exercise 2.4. There exists $a^{-1} \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Problem 116. Prove that

$$\mathbb{Z}_m^\times := \{1 \leq a \leq m \mid \gcd(a, m) = 1\}$$

is a group under multiplication modulo m. Observe that $|\mathbb{Z}_m^\times| = \varphi(m)$.

Theorem 2.5 (Euler-Fermat congruence)**.** *If $\gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Observe that $\varphi(p^k) = p^{k-1}\left(1 - \frac{1}{p}\right)$.

Problem 117. If $\gcd(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.

Corollary 2.6. *If $n = p_1^{k_1} \cdots p_s^{k_s}$, then*

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_s^{k_s}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

Thus,

$$\frac{\varphi(n)}{n} = \prod_{p \mid n}\left(1 - \frac{1}{p}\right).$$

Problem 118. Show that $\inf\limits_{n \in \mathbb{N}} \dfrac{\varphi(n)}{n} = 0$.

Problem 119. Let $d(n)$ be the number of positive divisors of $n \in \mathbb{N}$. If $\gcd(a, b) = 1$, then $d(ab) = d(a)d(b)$.

Definition 2.7. $d(n)$ is called the *divisor function*.

Problem 120. Give an explicit formula for $d(n)$ given the prime factorization of n.

Definition 2.8. An *arithmetic function* is a function $f : \mathbb{N} \to \mathbb{C}$ (where $\mathbb{N} = \{1, 2, 3, \dots\}$).

Definition 2.9. f is *multiplicative* if whenever $\gcd(a, b) = 1$, we have $f(ab) = f(a)f(b)$.

Definition 2.10. The *Möbius function* is

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 \cdots p_r,\ p_i \neq p_j \text{ for } i \neq j, \\ 0 & \text{if } n \text{ is not square-free.} \end{cases}$$

Problem 121. Show the Möbius function is multiplicative: If $\gcd(a, b) = 1$, then $\mu(ab) = \mu(a)\mu(b)$.

Definition 2.11. $\omega \in \mathbb{C}$ is a primitive nth root of unity if $\operatorname{ord}(\omega) = n$.

Problem 122. (a) If $\omega \in G$ and $\operatorname{ord}(\omega) = n$, then for what j is $\operatorname{ord}(\omega^j) = n$ if and only if $\gcd(j, n) = 1$?

(b) If $\omega \in G$, then $\operatorname{ord}(\omega^j) = \frac{\operatorname{ord}(\omega)}{\gcd(j,n)}$.

Problem 123. Let S_n denote the sum of the primitive nth roots of unity. Show that $S_n = \mu(n)$.

Problem 124. Show that $\sum\limits_{d \mid n} \varphi(d) = n$.

Problem 125. If f is multiplicative, then so is $g(n) = \sum\limits_{d \mid n} f(d)$.

Problem 126 (Möbius inversion)**.** Show that

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

for all $f : \mathbb{N} \to \mathbb{C}$ and $g(n) = \sum_{d|n} f(d)$.

Problem 127. (a) $\sum_{\text{primes}} 1/p = \infty$.
(b) $\sum_{p \le n} 1/p = \ln \ln n + \theta_n^*$ with $|\theta_n^*|$ bounded.

3. Functions of Matrices

Definition 3.1. If $A \in M_n(F)$ and $f(x) = a_0 + a_1 x + \cdots + a_k x^k \in F[x]$, then

$$f(A) := a_0 I + a_1 A + \cdots + a_k A^k.$$

Exercise 3.2. $(\exists f \neq 0)(f(A) = 0)$.

This amounts to showing there is k such that $\{I, A, ..., A^k\}$ are linearly dependent in $M_n(\mathbb{F})$. Indeed, we can take $k = n^2$ since $\{I, A, ..., A^{n^2}\}$ are $n^2 + 1$ vectors and $\dim(M_n) = n^2$.

Theorem 3.3 (Cayley-Hamilton)**.** *Let f_A be the characteristic polynomial of A. Then $f_A(A) = 0$.*

Problem 128. Prove the Cayley-Hamilton theorem ($f_A(A) = 0$) for diagonalizable matrices.

Problem 129. If λ is an eigenvalue of A and $f \in F[x]$, then $f(\lambda)$ is an eigenvalue of $f(A)$. (Is the converse true?)

Problem 130. For $a \in M_n(\mathbb{R})$, (a) define e^A, and (b) prove that if λ is an eigenvalue of A, then e^λ is an eigenvalue of e^A. (Is the converse true?)