

Mathematics 323: Algebra and Applications

Lecture 14

Prime Factorization in Euclidean Domains

The Euler Product and Möbius Inversion

Existence of Finite Fields

Euclid Since $\gcd(s, t) = \gcd(s, t - s)$ one can find the gcd of two numbers by continually subtracting the smaller from the larger until the two numbers are equal, at which point the common value is the gcd.

$$\gcd(t^m - 1, t^n - 1) = t^{\gcd(n,m)} - 1$$

Proposition: Let t be any element in a Euclidean domain. If m and n are positive integers then $\gcd(t^m - 1, t^n - 1) = t^{\gcd(n,m)} - 1$

Proof: Induction on $\max(m, n)$

Result is evident if $\max(m, n) = 1$ or $m = n$, so assume $m < n$

$$t^n - 1 - t^{n-m}(t^m - 1) = t^{n-m} - 1$$

Now apply induction and Euclid

$$\begin{aligned} \gcd(t^n - 1, t^m - 1) &= \gcd(t^m - 1, t^{n-m} - 1) && \text{(Euclid)} \\ &= t^{\gcd(m, n-m)} - 1 && \text{(Induction)} \\ &= t^{\gcd(n, m)} - 1 && \text{(Euclid) } \square \end{aligned}$$

Corollary: $x^{q^d} - x \mid x^{q^n} - x$ if and only if $d \mid n$

The Structure of Euclidean Domains

cancellation law: if $ab = ac$ and $a \neq 0$, then $b = c$

division with remainder: if $b \neq 0$, then $g(a) \leq g(ab)$ for all $a \in D$. For all nonzero elements $a, b \in D$ there exist $q, r \in D$ such that $a = bq + r$, with $r = 0$ or $g(r) < g(b)$.

Identifying Units: u is a unit if and only if $g(u) = g(1)$

Proof: For any element $a \in D$, $g(a) = g(a \times 1) \geq g(1)$

If u is a unit, then $uv = 1$ for some v and

$$g(1) = g(uv) \geq g(u)$$

Conversely suppose $g(u) = g(1)$, and write $1 = uv + r$

If $r \neq 0$, then $g(r) < g(u) = g(1)$ which is not possible

Hence $uv = 1$ and u is a unit. \square

Factorization into Primes

Theorem: In a Euclidean Domain every irreducible is prime.

Proof: If $p|ab$ and p does not divide a then $\gcd(p, a) = 1$.

There exist $s, t \in D$ such that $ps + at = 1$

Now $b = bps + (ab)t$ and $p|b$ as required. \square

Proposition: If $a = bc$, where b, c are not units, then $g(a) > g(b), g(c)$

Proof: Write $b = aq + r$ where $g(r) < g(a)$

Now $r = b - aq = b(1 - cq)$ and $1 - cq \neq 0$

It follows that $g(b) \leq g(r) < g(a)$ as required. \square

Proposition: If $a \in D$ is not a unit, then a can be written as a product of finitely many irreducibles.

Proof: Induction on $g(a)$

Uniqueness of Factorization into Primes

Proof (cont): If a is irreducible then we are done.

Otherwise $a = bc$ where neither b nor c is a unit. Now $g(b), g(c) < g(a)$ and each of b, c can be written as a finite product of irreducibles. \square

Theorem: Given two ways to write $a \in D$ as a product of irreducibles

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

then $r = s$, and after appropriate reordering there exist units u_i such that $q_i = u_i p_i$

Proof: Induction on $g(a)$

p_1 must divide one of the irreducibles q_i ; say $q_1 = u_1 p_1$ for some unit u_1 . Apply the cancellation law

$$a/p_1 = p_2 \cdots p_r = (u_1 q_2) q_3 \cdots q_s$$

Now $g(a/p_1) < g(a)$, so apply induction. \square

Monic Irreducible Polynomials of Degree n over \mathbb{Z}_p

Existence implies there is a finite field of size p^n .

Finite field F of size q : $F[x]$ is a Euclidean Domain and $x^{q^n} - x$ factors uniquely as a product of monic irreducibles.

Theorem: $x^{q^n} - x = \prod_{d|n} v_d(x)$

where $v_d(x)$ is the product of all monic irreducibles of degree d .

Corollary: $q^n = \sum_{d|n} dI_d$

where I_d is the number of distinct monic irreducibles of degree d .

Example Here F is the binary field \mathbb{Z}_2

$$x^{16} + x = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1)x$$

$$v_1(x) = x(x + 1), v_2(x) = x^2 + x + 1, v_4(x) = x^{12} + x^9 + x^6 + x^3 + 1$$

The Euler product $q^n = \sum_{d|n} dI_d$

Claim:

$$\frac{1}{1 - qz} = \prod_{d=1}^{\infty} \left(\frac{1}{(1 - z^d)^{I_d}} \right)$$

Left Side coefficient of z^n is q^n - counts monic polynomials of degree n .

Right Side there are I_d terms $1/(1 - z^d)$ - contribution of z^{dl} counts monic irreducible polynomial of degree d occurring with multiplicity l in the factorization of a monic polynomial of degree n .

Equality follows from unique factorization in $F[x]$.

Now take logs, differentiate and multiply by z

$$\frac{qz}{1 - qz} = \sum_{d=1}^{\infty} I_d \frac{dz^d}{1 - z^d}$$

Equate coefficients of z^n to obtain the Euler Product.

$$\boxed{x^{q^n} - x = \prod_{d|n} v_d(x)}$$

Proof: Let $d|n$ and let $f(x)$ be a monic irreducible polynomial of degree d . The field $F[x]/(f(x))$ has q^d elements and the multiplicative order of each element divides $q^d - 1$

$$f(x) \mid x^{q^d} - x \text{ and since } d|n \text{ we have } f(x) \mid x^{q^n} - x$$

Every monic irreducible polynomial with degree $d|n$ must divide $x^{q^d} - x$

Conversely, let $f(x)$ be a monic irreducible divisor of $x^{q^n} - x$ with degree d .

Then $f(x) \mid \gcd(x^{q^n} - x, x^{q^d} - x) = x^{q^e} - x$, where $e = \gcd(n, d)$

We show that $e \geq d$ by finding q^d solutions to $x^{q^e} - x$

If α is a root of $f(x)$, then $\alpha^{q^e} = \alpha$, since $f(x) \mid x^{q^e} - x$

Every element of the field $K = F[x]/(f(x))$ is a polynomial in α of degree $\leq d - 1$.

$$\boxed{x^{q^n} - x = \prod_{d|n} v_d(x) \text{ (contd)}}$$

$$\beta = A_0 + A_1\alpha + \dots + A_{d-1}\alpha^{d-1}$$

Then

$$\beta^{q^e} = \sum_{j=0}^{d-1} A_j^{q^e} \alpha^{jq^e} = \sum_{j=0}^{d-1} A_j \alpha^j = \beta$$

so every element of K satisfies $x^{q^e} - x = 0$.

The equation $x^{q^e} - x = 0$ has at most q^e solutions so $e \geq d$.
However $e = \gcd(n, d)$ divides d , so $d = e$ and d divides n .

We have shown that every irreducible divisor of $x^{q^n} - x$ has degree dividing n .

To complete the proof we need to show $x^{q^e} - x$ has no repeated factors. The formal derivative of a polynomial

$$p(x) = p_0 + p_1x + \dots + p_mx^m \text{ is } p'(x) = p_1 + 2p_2x + \dots + mp_mx^{m-1}.$$

$p(x)$ has no repeated roots if and only if $\gcd(p(x), p'(x)) = 1$

Since $(x^{q^n} - x)' = -1$ it follows that $x^{q^n} - x$ has no repeated factors.

Möbius Inversion

Given elements $a(j), b(j)$ from a commutative group G (written additively) with

$$a(n) = \sum_{d|n} b(d)$$

how to express $b(j)$ in terms of the $a(k)$'s

Example Here $G = \mathbb{Z}$, $a(n) = q^n$ and $b(n) = nI_n$ where I_n is the number of distinct monic irreducible polynomials of degree n over a field F of size q .

Example Here G is the multiplicative group $F^*[x]$, $a(n) = x^{q^n} - x$ and $b(n) = V_n(x)$ the product of all monic irreducible polynomials of degree n in $F[x]$.

Note that the sequence $b(n)$ is determined by the sequence $a(n)$

$$b(n) = a(n) - \sum_{d|n, d \neq n} b(d).$$

The Möbius Function

We show that if we can invert $a(n) = \sum_{d|n} b(d)$ in the special case $a(n) = (1, 0, \dots)$ then we can invert any sequence.

Möbius Function μ

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Proposition:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof: If $n = 1$, then $d = 1$ is the only divisor and $\mu(1) = 1$. For $n > 1$, write $n = p_1^{e_1} \dots p_r^{e_r}$ and set $n^* = p_1 \dots p_r$

$$\sum_{d|n} \mu(d) = \sum_{d|n^*} \mu(d) = 1 - r + \binom{r}{2} - \dots = (1 - 1)^r = 0$$

The Inversion Formula

Theorem:

$$b(n) = \sum_{d|n} \mu(d) a(n/d)$$

Proof:

$$\begin{aligned} a(n/d) &= \sum_{d'|(n/d)} b(d') \\ \sum_{d|n} \mu(d) a(n/d) &= \sum_{d|n} \mu(d) \sum_{d'|(n/d)} b(d') \\ &= \sum_{d'|n} b(d') \sum_{d|(n/d')} \mu(d) \\ &= b(n) \end{aligned}$$

Theorem: For every n , there is a monic irreducible polynomial of degree m with coefficients in \mathbb{Z}_p

Proof:

$$I_m = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d} > \frac{1}{n} (p^n - \sum_{j=0}^{n/2} p^j) > 0$$