

Lecture 10

Instructor: Sruthi Sekar

Scribe: Advay Sant

1 Lecture Overview

- Introduction to Fields.
- Some number-theoretic results on generation of primes.
- Construction of Finite Fields, including Fields of non-prime order.
- An application to communication complexity.

2 Fields

Definition 1 (Field). A **field** is a set F equipped with two binary operations: $+$ ('addition') and $\cdot$ ('multiplication') such that for all $a, b, c \in F$, the following hold:

- F is closed under $+$ and $\cdot$.
- Associativity: $a + (b + c) = (a + b) + c$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Commutativity: $a + b = b + a$, $a \cdot b = b \cdot a$.
- Distributivity: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- Existence of additive and multiplicative identities: There exist distinct elements $0, 1 \in F$ such that $0 + a = a$ and $1 \cdot a = a$.
- Existence of additive and multiplicative inverses: There exists an element $(-a) \in F$ such that $a + (-a) = 0$. If $a \neq 0$, there exists $a^{-1} \in F$ such that $a \cdot (a^{-1}) = 1$.

Definition 2 (Finite Field). A **finite field** is a field with a finite number of elements.

The following are some examples and counterexamples:

- $\mathbb{F}_p$: The finite field containing p elements where p is a prime i.e. the integers modulo p .
- For every prime p and positive integer n there exists a finite field of size p^n . **Any finite field must have order equal to a prime power.**
- Consider the ring of polynomials over a field $\mathbb{F}$ in n variables: $\mathbb{F}[X_1, \dots, X_n]$. This is not a field! (What would be the inverse of say, X_1 ?)

Theorem 3. For prime p , the set of integers modulo p (we will denote this by $\mathbb{F}_p$ with addition and multiplication modulo p) is a field.

Proof. Most of the properties are clear; we will prove the existence of multiplicative inverses.

Given any $a \in \mathbb{F}_p$ such that a is nonzero, $\gcd(a, p) = 1$ since p is prime. Therefore, by Bezout's theorem (more on this later), there exist integers x, y such that $ax + py = 1$. Therefore $ax \equiv 1 \pmod{p}$. Thus, we have found the multiplicative inverse of a which is $x \pmod{p}$. $\square$

Bezout's theorem states that given 2 integers a and b , $\gcd(a, b) = d$, there exist integers x, y such that $ax + by = d$. The case of $d = 1$ was useful to us in the previous theorem. However, is there a way to find the particular inverse? And in general, how do you find integers x, y satisfying the above identity?

This brings us to the **Extended Euclidean Algorithm**. This is an algorithm which takes any two integers a, b as input and returns 3 integers: $\gcd(a, b), x, y$ where $ax + by = \gcd(a, b)$.

Algorithm 1 ExtendedEuclidean

Input: a, b with $b > a > 0$

```

1 if  $a \mid b$  then
2    $q \leftarrow b/a$  return  $(a, 1, -q)$ 
3 else
4    $q \leftarrow \lfloor b/a \rfloor$   $r \leftarrow b - a q$  return ExtendedEuclidean( $a, r$ )

```

3 Some Number Theory

Now that we know that finite fields are only of the order of a prime power, it is not surprising that the generation of primes is also incredibly important. More specifically: How do you pick a prime p of n bits? Of course, this can be achieved by a pretty simple algorithm: Pick a random n -bit number, and use a primality test to check if it is prime. (Note that existence of an n -bit prime follows from Bertrand's postulate) The primality test could be deterministic in nature, like the AKS test, which runs in $\tilde{O}(n^6)$ time (which, although polylog, is pretty slow!). For a faster test, we can turn to the probabilistic Miller-Rabin test, which is not deterministic, but has a high rate of success, i.e. it will verify the primality of primes correctly, and output a composite number as prime with a very small probability, of the order of 10^{-4} .

Thus, finding an efficient deterministic algorithm for picking n -bit primes is still an issue.

Remark: There is no known deterministic efficient algorithm for picking n -bit primes among

$$2^n, \quad 2^n + 1, \quad 2^n + 2, \quad \dots$$

Conjecture (open problem, by Cramér): You will hit a prime by time $2^n + O(n^2)$.

Best provably known:

$$2^n + O(2^{0.535n})$$

Probability that a random n -bit number is prime:

$$\Pr[a \text{ is prime} \mid a \text{ is an } n\text{-bit number}] = \frac{\#n\text{-bit primes}}{2^n} \quad (\text{i.e., fraction of } n\text{-bit prime numbers})$$

Theorem 4. *Prime Number Theorem:*

$$\Pi(N) := \#primes \leq N$$

$$\Pi(N) \sim \frac{N}{\log N}$$

We can use this theorem to prove that the fraction of n -bit primes is approximately $\frac{1}{(2 \ln 2)^n}$. Therefore, the number of times you repeat to find a prime is $O(n)$. The algorithm gives an n -bit prime with high probability.

Note: You may not output anything!

4 Non-prime fields

Now, back to fields. As mentioned earlier, the following is the ring of univariate polynomials over a field $\mathbb{F}$:

$$\mathbb{F}[X] = \{c_0 + c_1X + \cdots + c_dX^d \mid c_i \in \mathbb{F}, d \geq 0\}$$

Univariate Polynomial Division

Given polynomials $A(X), B(X) \in \mathbb{F}[X]$ with $0 \leq \deg(B(X)) \leq \deg(A(X))$, there exist unique polynomials $q(X), r(X) \in \mathbb{F}[X]$ such that:

$$A(X) = B(X)q(X) + r(X)$$

Irreducible Polynomials

A polynomial $p(X)$ with $\deg(p(X)) \geq 2$ is called **irreducible** if it cannot be factored as a product of two lower-degree polynomials over $\mathbb{F}$.

Theorem 5. $\mathbb{F}[X]$ modulo $p(X)$ is a field of size $|\mathbb{F}|^{\deg(p)}$ **if and only if** $p(X)$ is irreducible.

Proof. Let $\deg(p) = d$. We proceed in three steps:

1. Every element has a unique remainder representative.

By the Division Algorithm for polynomials, each $f(X) \in \mathbb{F}[X]$ can be written uniquely as

$$f(X) = q(X)p(X) + r(X),$$

where $\deg r < d$. We declare two polynomials “equal in R ” exactly when their remainders agree. Thus

$$R = \{r(X) : \deg r < d\}$$

captures all possible elements, and addition/multiplication in R means

$$[r_1(X)] + [r_2(X)] = [r_1(X) + r_2(X)], \quad [r_1(X)] \cdot [r_2(X)] = [r_1(X)r_2(X)],$$

always followed by replacing by the remainder on division by $p(X)$.

2. Invertibility of nonzero elements.

Take any nonzero class $[r(X)] \in R$, so $\deg r < d$ but $p \nmid r$. Since p is irreducible, the only monic common divisors of r and p are constants, hence

$$\gcd(r(X), p(X)) = 1.$$

By the Extended Euclidean Algorithm for polynomials, there exist $u(X), v(X) \in \mathbb{F}[X]$ such that

$$u(X)r(X) + v(X)p(X) = 1.$$

Reducing both sides modulo $p(X)$ gives

$$u(X)r(X) \equiv 1 \text{ in } R,$$

so $[u(X)]$ is the multiplicative inverse of $[r(X)]$. Hence every nonzero element of R is invertible, proving R is a field.

3. Counting elements.

By construction, each element of R is uniquely represented by a polynomial of degree $< d$. There are $|\mathbb{F}|$ choices for each coefficient, and d coefficients, so

$$|R| = |\mathbb{F}|^d.$$

□

Fact: For every n , there exists an irreducible polynomial $p(X)$ of degree n over $\mathbb{F}$, so we can construct a field of size p^n , where $|\mathbb{F}| = p$.

Examples

1. $X^2 + 1 \in \mathbb{F}_3[X]$

Is it irreducible? **Yes!** Since it has no roots in $\mathbb{F}_3$ and is quadratic, it is irreducible.

2. $X^2 + 1 \in \mathbb{F}_5[X]$

Reducible: $X^2 + 1 = (X + 2)(X + 3)$ in $\mathbb{F}_5$

Therefore,

$$\mathbb{F}_3[X]/\langle X^2 + 1 \rangle = \{a + bX \mid a, b \in \mathbb{F}_3\}$$

is a field of order 9!

Finding Irreducible Polynomials of Degree n over $\mathbb{F}_p$

Randomized Algorithm

To find an irreducible polynomial $p(X) \in \mathbb{F}_p[X]$ of degree n :

1. Pick a random polynomial

$$p(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0,$$

where $c_i \in \mathbb{F}_p$ are chosen at random.

2. Check if $p(X)$ is irreducible.
3. If not, repeat.

Analysis

- Probability that a randomly chosen degree- n polynomial is irreducible is approximately

$$\Pr[p(X) \text{ is irreducible}] \sim \frac{1}{n}.$$

- Checking irreducibility is known to be doable in $\text{poly}(n \log p)$ time.
- Therefore, the algorithm runs in expected $O(n)$ tries, with high probability.

Deterministic Algorithm

There exists a deterministic algorithm that runs in time $\text{poly}(n, p)$ to produce an irreducible polynomial of degree n in $\mathbb{F}_p[X]$.

In particular, for $\mathbb{F}_{2^m}$ (i.e., $p = 2$), the runtime is polynomial in n .

5 An application to communication complexity

Theorem 6. *Fundamental Theorem of Algebra (Finite Field Version): Every non-zero univariate polynomial of degree $\leq d$ over a field has at most d roots.*

Setup

- Alice has a string $a = (a_0, \dots, a_{n-1}) \in \{0, 1\}^n$
- Bob has a string $b = (b_0, \dots, b_{n-1}) \in \{0, 1\}^n$
- They want to determine whether $a = b$ with as little communication as possible.

Deterministic protocols: Require $\Omega(n)$ bits (cannot do better).

Randomized Protocol (Fingerprinting)

- Choose a finite field $\mathbb{F}_q$ where q is large enough, say $q > n$.
- Alice and Bob interpret their strings as coefficients of degree- $(n-1)$ polynomials:

$$P_a(x) = a_1x + \dots + a_nx^n$$

$$P_b(x) = b_1x + \dots + b_nx^n$$

- They agree on a random $r \in \mathbb{F}_q$.
- Alice sends $P_a(r)$ to Bob.
- Bob compares with $P_b(r)$:

If $P_a(r) = P_b(r)$, output "equal"; else, "not equal"

Analysis:

- If $a = b$, then $P_a = P_b$ and they always agree.
- If $a \neq b$, then $P_a - P_b \neq 0$, so it is a degree- $\leq n$ non-zero polynomial. It has at most n roots.
- Therefore, over a random $r \in \mathbb{F}_q$, the probability of false positive is:

$$\Pr[P_a(r) = P_b(r) \mid a \neq b] \leq \frac{n}{q}$$

Conclusion:

- Only $O(\log n)$ bits need to be sent.
- For a large enough q , the probability of a false positive is reasonably small.

This setup is used to study the minimum communication needed to determine whether two parties have the same input.

References

- [1] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2008.