Fields and Polynomials
First, a little more
Number Theory
Bezout’s identity

Let $a, b$ be arbitrary positive integers. There exist integers $r$ and $s$ such that

$$r a + s b = \gcd(a, b)$$

A non-algorithmic proof:

- Consider the set $L$ of all positive integers that can be expressed as $r a + s b$ for some integers $r, s$.
- $L$ is non-empty (e.g. $a \in S$).
- So $L$ has a minimum element $d$ (well-ordering principle $\iff$ principle of induction)

**Claim:** $d = \gcd(a, b)$

Follows from Extended Euclid Algorithm
Claim: \( \gcd(a,b) = d \) (the minimum positive integer expressible as \( ra+sb \) )

1. \( \gcd(a,b) \) divides both \( a \) and \( b \), and hence also divides \( d \). So \( d \geq \gcd(a,b) \)

2. \( d \) divides both \( a \) and \( b \), and hence \( d \leq \gcd(a,b) \)

Let’s show \( d \mid a \).
Write \( a = qd + t \), with \( 0 \leq t < d \).
\( t = a – qd \) is also expressible as a combination \( r’ a + s’ b \).
Contradicts minimality of \( d \).
Lemma: If \( \gcd(a,b) = 1 \) and \( a \mid bc \), then \( a \mid c \).

Proof: Let \( r,s \) be such that \( ra + sb = 1 \)

\[
ra \cdot c + sb \cdot c = c
\]

\( a \mid bc \) and \( a \mid ra \cdot c \), so \( a \mid c \).

Corollary: If \( p \) is a prime and \( p \mid q_1 \cdot q_2 \cdots q_k \), then \( p \) must divide some \( q_i \).

If the \( q_i \)'s are also prime, then \( p = q_i \) for some \( i \).

Uniqueness of prime factorization follows from this!
Poll

Which of these numbers is congruent to 1 (mod 5), 6 (mod 7), and 8 (mod 9)?

- No such number exists
- 91
- 136
- 197
- 251
- 291
- None of the above
- Beats me
Chinese Remaindering

Chinese Remainder Theorem: Suppose positive integers \( n_1, n_2, \ldots, n_k \) are pairwise coprime. Then, for all integers \( b_1, b_2, \ldots, b_k \), there exists an integer \( x \) solving the below system of simultaneous congruences

\[
\begin{align*}
x &\equiv b_1 \pmod{n_1} \\
x &\equiv b_2 \pmod{n_2} \\
\vdots \\
x &\equiv b_k \pmod{n_k}.
\end{align*}
\]

Further, all solutions \( x \) are congruent to each other modulo \( N = \prod_{i=1}^{k} n_i \).

Uniqueness of solutions modulo \( N \)

If \( x, y \) are two solutions, then \( n_i \) divides \( x - y \), for \( i=1,2,\ldots,k \)

Since the \( n_i \) are pairwise coprime, this means the product \( N = n_1 \times n_2 \times \ldots \times n_k \) divides \( x - y \), thus \( x \equiv y \pmod{N} \)
Extended Euclid and Chinese Remaindering

Chinese Remainder Theorem: Suppose positive integers \( n_1, n_2, \ldots, n_k \) are pairwise coprime. Then, for all integers \( b_1, b_2, \ldots, b_k \), there exists an integer \( x \) solving the below system of simultaneous congruences

\[
\begin{align*}
x &\equiv b_1 \pmod{n_1} \\
x &\equiv b_2 \pmod{n_2} \\
& \quad \vdots \\
x &\equiv b_k \pmod{n_k}.
\end{align*}
\]

Further, all solutions \( x \) are congruent to each other modulo \( N = \prod_{i=1}^{k} n_i \).

Proof for \( k=2 \):

Take \( x = b_1 \left( n_2^{-1} \mod n_1 \right) n_2 + b_2 \left( n_1^{-1} \mod n_2 \right) n_1 \)

Divisible by \( n_2 \),
Remainder 1 mod \( n_1 \)

Divisible by \( n_1 \)
Remainder 1 mod \( n_2 \)

Can compute \( x \) efficiently (by computing modular inverses)
Chinese Remainder Theorem: Suppose positive integers \( n_1, n_2, \ldots, n_k \) are \textit{pairwise coprime}. Then, for all integers \( b_1, b_2, \ldots, b_k \), there exists an integer \( x \) solving the below system of simultaneous congruences

\[
\begin{align*}
x &\equiv b_1 \pmod{n_1} \\
x &\equiv b_2 \pmod{n_2} \\
& \vdots \\
x &\equiv b_k \pmod{n_k}.
\end{align*}
\]

Further, all solutions \( x \) are congruent to each other modulo \( N = \prod_{i=1}^{k} n_i \).

For arbitrary \( k \): Let \( m_i = N/n_i \)

Note \( \gcd(m_i, n_i) = 1 \)

\( n_i | m_j \) for \( j \neq i \)

Take \( x = b_1 \left( m_1^{-1} \mod n_1 \right) m_1 + b_2 \left( m_2^{-1} \mod n_2 \right) m_2 + \ldots + b_k \left( m_k^{-1} \mod n_k \right) m_k \)

First term contributes the remainder mod \( n_1 \) (rest are divisible by \( n_1 \)), \ldots, \( k'\)th term contributes the remainder mod \( n_k \)
Quick Recap:
Groups
Recap: Definition of a group

$G$ is a “group under operation $\bullet$” if:

0. [Closure] $G$ is closed under $\bullet$
   i.e., $a \bullet b \in G \quad \forall \ a,b\in G$

1. [Associativity] Operation $\bullet$ is associative:
   i.e., $a \bullet (b \bullet c) = (a \bullet b) \bullet c \quad \forall \ a,b,c\in G$

2. [Identity] There exists an element $e \in G$
   (called the “identity element”) such that
   $a \bullet e = a, \ e \bullet a = a \quad \forall \ a\in G$

3. [Inverse] For each $a \in G$ there is an element $a^{-1} \in G$
   (called the “inverse of $a$”) such that
   $a \bullet a^{-1} = e, \ a^{-1} \bullet a = e$
Symmetries of undirected cycle: dihedral group

\[ G = \{ \text{Id, } r_1, r_2, r_3, r_4, f_1, f_2, f_3, f_4, f_5 \} \]
Abelian groups

In a group we do NOT NECESSARILY have

\[ a \cdot b = b \cdot a \]

Definition:

“\( a,b \in G \) commute” means \( ab = ba \).

Definition:

A group is said to be abelian if all pairs \( a,b \in G \) commute.
Order of a group element

Let $G$ be a **finite** group. Let $a \in G$.

**Definition:** The order of $x$, denoted $\text{ord}(a)$, is the smallest $m \geq 1$ such that $a^m = 1$.

Note that $a, a^2, a^3, \ldots, a^{m-1}, a^m = 1$ all distinct.
Order Theorem: For every $a \in G$, \( \text{ord}(a) \) divides \(|G|\).

Corollary: $a^{|G|} = 1$ for all $a \in G$.

Corollary (Euler’s Theorem): For $a \in \mathbb{Z}_n^*$, $a^{\phi(n)} = 1$.
That is, if $\gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Corollary (Fermat’s little theorem): For prime $p$, if $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. 
Cyclic groups

A finite group $G$ of order $n$ is cyclic if $G = \{e, b, b^2, \ldots, b^{n-1}\}$ for some group element $b$.

In such a case, we say $b$ "generates" $G$, or $b$ is a "generator" of $G$.

Examples:

• $(\mathbb{Z}_n, +)$ (1 is a generator)

• $C_4$ (Rot$_{90}$ is a generator)

Non-examples: Mattress group; dihedral group; any non-abelian group.
Lagrange's Theorem: If $G$ is a finite group, and $H$ is a subgroup then $|H|$ divides $|G|$.

A useful corollary: If $G$ is a finite group and $H$ is a proper subgroup of $G$, then $|H| \leq |G|/2$.
Feature Presentation: Field Theory
Find out about the wonderful world of $\mathbb{F}_{2^k}$ where two equals zero, plus is minus, and squaring is a linear operator!

– Richard Schroeppel
A group is a set with a single binary operation.

Number-theoretic sets often have more than one operation defined on them.

For example, in \( \mathbb{Z} \), we can do both addition and multiplication.

Same in \( \mathbb{Z}_n \) (we can add and multiply modulo \( n \)).

For reals \( \mathbb{R} \) or rationals \( \mathbb{Q} \), we can also divide (inverse operation for multiplication).
Fields

Informally, it’s a place where you can add, subtract, multiply, and divide.

Examples: Real numbers $\mathbb{R}$
Rational numbers $\mathbb{Q}$
Complex numbers $\mathbb{C}$
Integers mod prime $\mathbb{Z}_p$ (Why?)

NON-examples: Integers $\mathbb{Z}$
Non-negative reals $\mathbb{R}^+$ division??
subtraction??
A field is a set $F$ with two binary operations, called $+$ and $\cdot$.

$(F, +)$ an abelian group, with identity element called $0$

$(F \setminus \{0\}, \cdot)$ an abelian group, identity element called $1$

Distributive Law holds:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

Example:

$$F_3 = \mathbb{Z}_3^*$$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\cdot$</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Fields: familiar examples

Real numbers \( \mathbb{R} \)
Rational numbers \( \mathbb{Q} \)
Complex numbers \( \mathbb{C} \)
Integers mod \textit{prime} \( \mathbb{Z}_p \)

The last one is a finite field
Example

Quadratic “number field”

\[ \mathbb{Q}(\sqrt{2}) = \{ a + b \sqrt{2} : a, b \in \mathbb{Q} \} \]

**Addition:** \((a + b \sqrt{2}) + (c + d \sqrt{2}) = (a+c) + (b+d) \sqrt{2}\)

**Multiplication:**
\[(a + b \sqrt{2}) \cdot (c + d \sqrt{2}) = (ac+2bd) + (ad+bc) \sqrt{2}\]

**Exercise:** Prove above defines a field.
Finite fields

Some familiar infinite fields: \( \mathbb{Q}, \mathbb{R}, \mathbb{C} \) (now \( \mathbb{Q}(\sqrt{2}) \))

Finite fields we know: \( \mathbb{Z}_p \) aka \( \mathbb{F}_p \) for \( p \) a prime

Is there a field with 2 elements? Yes
Is there a field with 3 elements? Yes
Is there a field with 4 elements? Yes

\[
\begin{array}{cccc}
+ & 0 & 1 & a & b \\
0 & 0 & 1 & a & b \\
1 & 1 & 0 & b & a \\
a & a & b & 0 & 1 \\
b & b & a & 1 & 0 \\
\end{array}
\]

\[
\begin{array}{cccc}
\cdot & 0 & 1 & a & b \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & a & b \\
a & a & b & 1 & a \\
b & 0 & b & 1 & a \\
\end{array}
\]
Evariste Galois (1811–1832) introduced the concept of a finite field (also known as a Galois Field in his honor)
<table>
<thead>
<tr>
<th>Finite fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a field with <strong>2</strong> elements?</td>
</tr>
<tr>
<td>Is there a field with <strong>3</strong> elements?</td>
</tr>
<tr>
<td>Is there a field with <strong>4</strong> elements?</td>
</tr>
<tr>
<td>Is there a field with <strong>5</strong> elements?</td>
</tr>
<tr>
<td>Is there a field with <strong>6</strong> elements?</td>
</tr>
<tr>
<td>Is there a field with <strong>7</strong> elements?</td>
</tr>
<tr>
<td>Is there a field with <strong>8</strong> elements?</td>
</tr>
<tr>
<td>Is there a field with <strong>9</strong> elements?</td>
</tr>
<tr>
<td>Is there a field with <strong>10</strong> elements?</td>
</tr>
</tbody>
</table>
Finite fields

Theorem (which we won’t prove):
There is a field with $q$ elements if and only if $q$ is a power of a prime.

Up to isomorphism, it is unique.

That is, all fields with $q$ elements have the same addition and multiplication tables, after renaming elements.

This field is denoted $\mathbb{F}_q$ (also $GF(q)$)
Finite fields

Question:

If $q$ is a prime power but not just a prime, what **are** the addition and multiplication tables of $\mathbb{F}_q$?

Answer:

It’s a bit hard to describe.

We’ll tell you later, but for 251’s purposes, you mainly only need to know about prime $q$. 
Polynomials
Polynomials

Informally, a polynomial is an expression that looks like this:

\[6x^3 - 2.3x^2 + 5x + 4.1\]

\(x\) is a symbol, called the variable (or indeterminate)

the ‘numbers’ standing next to powers of \(x\) are called the coefficients
Polynomials

Informally, a polynomial is an expression that looks like this:

$$6x^3 - 2.3x^2 + 5x + 4.1$$

Actually, coefficients can come from any field.

Can allow multiple variables, but we won’t.

Set of polynomials with variable $x$ and coefficients from field $F$ is denoted $F[x]$. 
Polynomials – formal definition

Let $F$ be a field and let $x$ be a variable symbol.

$F[x]$ is the set of polynomials over $F$, defined to be expressions of the form

$$c_d x^d + c_{d-1} x^{d-1} + \cdots + c_2 x^2 + c_1 x + c_0$$

where each $c_i$ is in $F$, and $c_d \neq 0$.

We call $d$ the degree of the polynomial.

Also, the expression $0$ is a polynomial.

(By convention, we call its degree $-\infty$.)
Adding and multiplying polynomials

You can add and multiply polynomials.

Example. Here are two polynomials in $\mathbb{F}_{11}[x]$

$$P(x) = x^2 + 5x - 1$$
$$Q(x) = 3x^3 + 10x$$

$$P(x) + Q(x) = 3x^3 + x^2 + 15x - 1$$
$$= 3x^3 + x^2 + 4x - 1$$
$$= 3x^3 + x^2 + 4x + 10$$
Adding and multiplying polynomials

You can add and multiply polynomials (they are a “ring” but we’ll skip a formal treatment of rings)

**Example.** Here are two polynomials in \( \mathbb{F}_{11}[x] \)

\[
\begin{align*}
P(x) &= x^2 + 5x - 1 \\
Q(x) &= 3x^3 + 10x
\end{align*}
\]

\[
P(x) \cdot Q(x) = (x^2 + 5x - 1)(3x^3 + 10x)
= 3x^5 + 15x^4 + 7x^3 + 50x^2 - 10x
= 3x^5 + 4x^4 + 7x^3 + 6x^2 + x
\]
Adding and multiplying polynomials

Polynomial addition is associative and commutative.
\[ 0 + P(x) = P(x) + 0 = P(x). \]
\[ P(x) + (-P(x)) = 0. \]
So \((F[x], +)\) is an abelian group!

Polynomial multiplication is associative and commutative.
\[ 1 \cdot P(x) = P(x) \cdot 1 = P(x). \]
Multiplication distributes over addition:
\[ P(x) \cdot (Q(x) + R(x)) = P(x) \cdot Q(x) + P(x) \cdot R(x) \]

If \(P(x) / Q(x)\) were always a polynomial, then \(F[x]\) would be a field! Alas…
Dividing polynomials?

P(x) / Q(x) is not necessarily a polynomial.

So \( F[x] \) is not quite a field.

(It’s a “ring”)

Same with \( \mathbb{Z} \), the integers:

it has everything except division.

Actually, there are many analogies between \( F[x] \) and \( \mathbb{Z} \).

• starting point for rich interplay between algebra, arithmetic, and geometry in mathematics
Dividing polynomials?

\( \mathbb{Z} \) has the concept of “division with remainder”:

Given \( a, b \in \mathbb{Z}, b \neq 0 \), can write

\[ a = q \cdot b + r, \]

where \( r \) is “smaller than” \( b \).

\( F[x] \) has the same concept:

Given \( A(x), B(x) \in F[x], B(x) \neq 0 \), can write

\[ A(x) = Q(x) \cdot B(x) + R(x), \]

where \( \deg(R(x)) < \deg(B(x)) \).
“Division with remainder” for polynomials

Example: Divide \(6x^4 + 8x + 1\) by \(2x^2 + 4\) in \(\mathbb{F}_{11}[x]\)

\[
\begin{array}{rcccl}
& & 3x^2 & + 5 \\
\hline
2x^2 + 4 & | & 6x^4 & + 8x & + 1 \\
- & - & 6x^4 & + x^2 \\
\hline
& & -x^2 & + 8x & + 1 \\
- & - & -x^2 & + 9 \\
\hline
& & & 8x & + 3
\end{array}
\]

Check:

\[
6x^4 + 8x + 1 = (3x^2 + 5)(2x^2 + 4) + (8x + 3)
\]

(in \(\mathbb{F}_{11}[x]\))
Integers $\mathbb{Z}$

“size” = absolute value

“division”:
$$a = qb + r, \quad |r| < |b|$$

can use Euclid’s Algorithm to find GCDs

$p$ is “prime”:
no nontrivial divisors

$\mathbb{Z}$ mod $p$:
a field iff $p$ is prime

Polynomials $F[x]$

“size” = degree

“division”:
$$A(x) = Q(x)B(x) + R(x), \quad \deg(R) < \deg(B)$$

can use Euclid’s Algorithm to find GCDs

$P(x)$ is “irreducible”:
no nontrivial divisors

$F[x]$ mod $P(x)$:
a field iff $P(x)$ is irreducible
(with $|F|^{\deg(P)}$ elements)
The field with 4 elements

Degree < 2 polynomials \{0,1,x,1+x\} \subseteq \mathbb{F}_2[x]

Addition and multiplication modulo 1+x+x^2

\[
\begin{array}{cccc}
+ & 0 & 1 & a \\
0 & 0 & 1 & a \\
1 & 1 & 0 & b \\
a & a & b & 0 \\
b & b & a & 1 \\
\end{array}
\]

\[
\begin{array}{cccc}
\cdot & 0 & 1 & a \\
0 & 0 & 0 & 0 \\
1 & 0 & 1 & a \\
a & 0 & a & b \\
b & 0 & b & 1 \\
\end{array}
\]

\[
\begin{array}{cccc}
a=x \\
b=1+x
\end{array}
\]
The field with \( p^d \) elements

Degree < d polynomials \( \subseteq \mathbb{F}_p[x] \)

Addition and multiplication modulo \( h(x) \), which is any degree d **irreducible** polynomial in \( \mathbb{F}_p[x] \)

- **Fact**: Irreducibles of every degree exist in \( \mathbb{F}_p[x] \)

Field with 9 elements: \( \mathbb{F}_3[x] \mod (x^2+1) \)

Field with 8 elements: \( \mathbb{F}_2[x] \mod (x^3+x+1) \)
Enough algebraic theory.

Let’s play with polynomials!
Evaluating polynomials

Given a polynomial $P(x) \in F[x]$, $P(a)$ means its evaluation at element $a$.

E.g., if $P(x) = x^2 + 3x + 5$ in $\mathbb{F}_{11}[x]$

$P(6) = 6^2 + 3 \cdot 6 + 5 = 36 + 18 + 5 = 59 = 4$

$P(4) = 4^2 + 3 \cdot 4 + 5 = 16 + 12 + 5 = 33 = 0$

Definition: $\alpha$ is a root of $P(x)$ if $P(\alpha) = 0$. 
Polynomial roots

Theorem:

Let $P(x) \in F[x]$ have degree 1.
Then $P(x)$ has exactly 1 root.

Proof:

Write $P(x) = cx + d$ (where $c \neq 0$).
Then $P(r) = 0 \iff cr + d = 0$

$\iff cr = -d$

$\iff r = -d/c.$
Polynomial roots

Theorem:

Let \( P(x) \in F[x] \) have degree 2.
Then \( P(x) \) has... how many roots??

E.g.: \( x^2 + 1 \)...

<table>
<thead>
<tr>
<th>Field</th>
<th># of roots</th>
</tr>
</thead>
<tbody>
<tr>
<td>( F_2[x] )</td>
<td>1</td>
</tr>
<tr>
<td>( F_3[x] )</td>
<td>0</td>
</tr>
<tr>
<td>( F_5[x] )</td>
<td>2</td>
</tr>
<tr>
<td>( \mathbb{R}[x] )</td>
<td>0</td>
</tr>
<tr>
<td>( \mathbb{C}[x] )</td>
<td>2</td>
</tr>
</tbody>
</table>
The single most important theorem about polynomials over fields:

A nonzero degree-

polynomial has

at most d roots.
**Theorem**: Over a field, for all \( d \geq 0 \), a nonzero degree-\( d \) polynomial \( P \) has at most \( d \) roots.

**Proof by induction on \( d \in \mathbb{N} \):**

**Base case**: If \( P(x) \) is degree-0 then \( P(x) = a \) for some \( a \neq 0 \). This has 0 roots.

**Induction**: Assume true for \( d \geq 0 \). Let \( P(x) \) have degree \( d+1 \).

If \( P(x) \) has 0 roots: we’re done! Else let \( b \) be a root.

Divide with remainder: \( P(x) = Q(x)(x-b) + R(x) \). \((\ast)\)

\( \deg(R) < \deg(x-b) = 1 \), so \( R(x) \) is a constant. Say \( R(x)=r \).

Plug \( x = b \) into \((\ast)\): \( 0 = P(b) = Q(b)(b-b)+r = 0+r = r \).

So \( P(x) = Q(x)(x-b) \). Now, \( \deg(Q) = d \). \( : \) \( Q \) has \( \leq d \) roots.

\( : \) \( P(x) \) has \( \leq d+1 \) roots, completing the induction.
A useful corollary

**Theorem**: Over a field $F$, for all $d \geq 0$, degree-$d$ polynomials have at most $d$ roots.

**Corollary**: Suppose a polynomial $R(x) \in F[x]$ is such that

(i) $R$ has degree $\leq d$ and 
(ii) $R$ has $> d$ roots 

Then $R$ must be the 0 polynomial

I’ve used the above corollary *several times* in my research.
Theorem:
Over a field, degree-$d$ polynomials have at most $d$ roots.

Reminder:
This is only true over a field.

E.g., consider $P(x) = 3x$ over $\mathbb{Z}_6$.

It has degree 1, but 3 roots: 0, 2, and 4.
Interpolation

Say you’re given a bunch of “data points” 

Can you find a (low-degree) polynomial which “fits the data”? 
Interpolation

Let pairs \((a_1, b_1), (a_2, b_2), \ldots, (a_{d+1}, b_{d+1})\) from a field \(F\) be given \((with all a_i’s distinct)\).

Theorem:

There is exactly one polynomial \(P(x)\) of degree at most \(d\) such that
\[ P(a_i) = b_i \text{ for all } i = 1 \ldots d+1. \]

E.g., through 2 points there is a unique linear polynomial.
Interpolation

There are two things to prove.

1. There is at least one polynomial of degree \( \leq d \) passing through all \( d+1 \) data points.

2. There is at most one polynomial of degree \( \leq d \) passing through all \( d+1 \) data points.

Let’s prove #2 first.
**Interpolation**

**Theorem:** Let pairs \((a_1,b_1), (a_2,b_2), \ldots, (a_{d+1},b_{d+1})\) from a field \(F\) be given (with all \(a_i\)'s distinct). Then there is **at most one** polynomial \(P(x)\) of degree at most \(d\) with \(P(a_i) = b_i\) for all \(i\).

**Proof:** Suppose \(P(x)\) and \(Q(x)\) both do the job. Let \(R(x) = P(x)−Q(x)\).

Since \(\text{deg}(P), \text{deg}(Q) \leq d\) we must have \(\text{deg}(R) \leq d\).

But \(R(a_i) = b_i−b_i = 0\) for all \(i = 1\ldots d+1\).

Thus \(R(x)\) has more roots than its degree.

\(\therefore\) \(R(x)\) must be the 0 polynomial, i.e., \(P(x) = Q(x)\).
Interpolation

Now let’s prove the other part, that there is at least one polynomial.

Theorem:
Let pairs \((a_1,b_1), (a_2,b_2), \ldots, (a_{d+1},b_{d+1})\) from a field \(F\) be given (with all \(a_i\)’s distinct). Then there exists a polynomial \(P(x)\) of degree at most \(d\) with \(P(a_i) = b_i\) for all \(i\).
Interpolation

The method for constructing the polynomial is called Lagrange Interpolation.

Discovered in 1779 by Edward Waring.

Rediscovered in 1795 by J.-L. Lagrange.
Lagrange Interpolation

Want $P(x)$
(with degree $\leq d$)
such that $P(a_i) = b_i \ \forall i$. 
Lagrange Interpolation

<table>
<thead>
<tr>
<th>$a_1$</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_2$</td>
<td>0</td>
</tr>
<tr>
<td>$a_3$</td>
<td>0</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>$a_d$</td>
<td>0</td>
</tr>
<tr>
<td>$a_{d+1}$</td>
<td>0</td>
</tr>
</tbody>
</table>

Can we do this special case?

**Promise:** once we solve this special case, the general case is very easy.
Lagrange Interpolation

\[ a_1 \quad 1 \]
\[ a_2 \quad 0 \]
\[ a_3 \quad 0 \]
\[ \ldots \quad \ldots \]
\[ a_d \quad 0 \]
\[ a_{d+1} \quad 0 \]
Lagrange Interpolation

\[
a_1 \quad 1 \\
a_2 \quad 0 \\
a_3 \quad 0 \\
\vdots \\
a_d \quad 0 \\
a_{d+1} \quad 0
\]

Idea #1: \( P(x) = (x-a_2)(x-a_3)\cdots(x-a_{d+1}) \)

Degree is \( d \). ✔

\[
P(a_2) = P(a_3) = \cdots = P(a_{d+1}) = 0. \quad \checkmark
\]

\[
P(a_1) = (a_1-a_2)(a_1-a_3)\cdots(a_1-a_{d+1}). \quad ??
\]

Just divide \( P(x) \) by this number.
Lagrange Interpolation

\[ \begin{align*}
  a_1 & : 1 \\
  a_2 & : 0 \\
  a_3 & : 0 \\
  \ldots & : \ldots \\
  a_d & : 0 \\
  a_{d+1} & : 0
\end{align*} \]

Idea #2:
Denominator is a nonzero field element
Numerator is a deg. \(d\) polynomial

Call this the selector polynomial for \(a_1\).

\[ S_1(x) = \frac{(x - a_2)(x - a_3)\ldots(x - a_{d+1})}{(a_1 - a_2)(a_1 - a_3)\ldots(a_1 - a_{d+1})} \]
Lagrange Interpolation

| a_1  | 0   |
| a_2  | 1   |
| a_3  | 0   |
| ...  | ... |
| a_d  | 0   |
| a_{d+1} | 0 |

Great! But what about this data?

\[
S_2(x) = \frac{(x - a_1)(x - a_3) \cdots (x - a_{d+1})}{(a_2 - a_1)(a_2 - a_3) \cdots (a_2 - a_{d+1})}
\]
Lagrange Interpolation

\[
\begin{array}{c|c}
\text{a}_1 & 0 \\
\text{a}_2 & 0 \\
\text{a}_3 & 0 \\
\vdots & \vdots \\
\text{a}_d & 0 \\
\text{a}_{d+1} & 1 \\
\end{array}
\]

Great! But what about **this** data?

\[
S_{d+1}(x) = \frac{(x - \text{a}_1)(x - \text{a}_2) \cdots (x - \text{a}_d)}{(\text{a}_{d+1} - \text{a}_1)(\text{a}_{d+1} - \text{a}_2) \cdots (\text{a}_{d+1} - \text{a}_d)}
\]
Lagrange Interpolation

\[ a_1 \quad b_1 \\
\quad a_2 \quad b_2 \\
\quad a_3 \quad b_3 \\
\quad \ldots \quad \ldots \\
\quad a_d \quad b_d \\
\quad a_{d+1} \quad b_{d+1} \]

Great! Finally, what about this data?

\[ P(x) = b_1 \cdot S_1(x) + b_2 \cdot S_2(x) + \cdots + b_{d+1} \cdot S_{d+1}(x) \]
Lagrange Interpolation – example

Over \( \mathbb{Z}_{11} \), find a polynomial \( P \) of degree \( \leq 2 \) such that \( P(5) = 1 \), \( P(6) = 2 \), \( P(7) = 9 \).

\[
S_5(x) = \frac{6}{(5 - 6)(5 - 7)}(x - 6)(x - 7)
\]

\[
S_6(x) = -\frac{1}{(5 - 6)(5 - 7)}(x - 5)(x - 7)
\]

\[
S_7(x) = \frac{6}{(5 - 6)(5 - 7)}(x - 5)(x - 6)
\]

\[
P(x) = 1 \cdot S_5(x) + 2 \cdot S_6(x) + 9 \cdot S_7(x)
\]

\[
P(x) = 6(x^2 - 13x + 42) - 2(x^2 - 12x + 35) + 54(x^2 - 11x + 30)
\]

\[
P(x) = 3x^2 + x + 9
\]
The Chinese Remainder Theorem had a very similar proof.

Not a coincidence: algebraically, integers & polynomials share many common properties.

Lagrange interpolation is the exact analog of Chinese Remainder Theorem for polynomials.
Chinese Remainder Theorem: Suppose $n_1, n_2, \ldots, n_k$ are pairwise coprime. Then, for all integers $a_1, a_2, \ldots, a_k$, there exists an integer $x$ solving the below system of simultaneous congruences

\[
x \equiv a_1 \pmod{n_1} \\
x \equiv a_2 \pmod{n_2} \\
\vdots \\
x \equiv a_k \pmod{n_k}.
\]

Further, all solutions $x$ are congruent modulo $N = \prod_{i=1}^{k} n_i$.

Let $m_i = N/n_i$

i’th “selector” number: $T_i = \left(m_i^{-1} \mod n_i\right) m_i$

\[
x = a_1 \ T_1 + a_2 \ T_2 + \ldots + a_k \ T_k
\]
Recall: Interpolation

Let pairs \((a_1, b_1), (a_2, b_2), \ldots, (a_{d+1}, b_{d+1})\) from a field \(F\) be given (with all \(a_i\)'s distinct).

**Theorem:**

There is a unique degree \(d\) polynomial \(P(x)\) satisfying \(P(a_i) = b_i\) for all \(i = 1 \ldots d+1\).
A linear algebra view

Let \( p(x) = p_0 + p_1x + p_2x^2 + \ldots + p_dx^d \)

Need to find the coefficient vector \((p_0, p_1, \ldots, p_d)\)

\[
p(a) = p_0 + p_1a + \ldots + p_da^d
= 1 \cdot p_0 + a \cdot p_1 + a^2 \cdot p_2 + \ldots + a^d \cdot p_d
\]

Thus we need to solve:

\[
\begin{pmatrix}
1 & a_1 & a_1^2 & \cdots & a_1^d \\
1 & a_2 & a_2^2 & \cdots & a_2^d \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & a_{d+1} & a_{d+1}^2 & \cdots & a_{d+1}^d \\
\end{pmatrix}
\begin{pmatrix}
p_0 \\
p_1 \\
\vdots \\
p_d \\
\end{pmatrix}
=
\begin{pmatrix}
b_1 \\
b_2 \\
\vdots \\
b_{d+1} \\
\end{pmatrix}
\]
Lagrange interpolation

The \((d+1) \times (d+1)\) Vandermonde matrix

\[
M = \begin{pmatrix}
1 & a_1 & a_1^2 & \cdots & a_1^d \\
1 & a_2 & a_2^2 & \cdots & a_2^d \\
1 & a_3 & a_3^2 & \cdots & a_3^d \\
& & \vdots & & \\
1 & a_{d+1} & a_{d+1}^2 & \cdots & a_{d+1}^d
\end{pmatrix}
\]

is invertible.

- The determinant of \(M\) is nonzero when \(a_i\)'s are distinct.

Thus can recover coefficient vector as \( \vec{p} = M^{-1} \vec{b} \)

The columns of \(M^{-1}\) are given by the coefficients of the various “selector” polynomials we constructed in Lagrange interpolation.
Representing Polynomials

Let $P(x) \in F[x]$ be a degree-$d$ polynomial.

Representing $P(x)$ using $d+1$ field elements:

1. List the $d+1$ coefficients.
2. Give $P$’s value at $d+1$ different elements.

Rep 1 to Rep 2: Evaluate at $d+1$ elements

Rep 2 to Rep 1: Lagrange Interpolation
Number Theory:
- Unique factorization
- Chinese Remainder theorem

Fields:
- Definitions
- Examples
- Finite fields of prime order

Polynomials:
- Degree-d polys have \( \leq d \) roots.
- Polynomial division with remainder
- Lagrange Interpolation