Communicating with Errors

We learned how to *encrypt* communication so that an eavesdropper cannot find out your personal information.

What if your enemy is not an eavesdropper, but *nature*?

Soon, we will learn how to send messages *reliably*, even when nature is *deleting* parts of your message.

Today: We finish modular arithmetic and learn about polynomials.

Composite Moduli

Look at a composite modulus, $\mathbb{Z}/35\mathbb{Z}$. Here, $35 = 5 \cdot 7$.

How is $\mathbb{Z}/35\mathbb{Z}$ related to $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$?

Take a number in $\mathbb{Z}/35\mathbb{Z}$, e.g., 24.

- In $\mathbb{Z}/5\mathbb{Z}$, we have $24 \equiv 4 \pmod 5$.
- In $\mathbb{Z}/7\mathbb{Z}$, we have $24 \equiv 3 \pmod 7$.

So, we have $24 = (4 \text{ in } \mathbb{Z}/5\mathbb{Z}, 3 \text{ in } \mathbb{Z}/7\mathbb{Z})$.

- From $(4,3)$, can we go back to 24?

Solving Modular Congruences

Does the system

$$\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

have a solution in $\mathbb{Z}/35\mathbb{Z}$?

Manual way of finding the solution: first, list all numbers which are equal to 3, modulo 7.

- 3, 10, 17, 24, 31.

The highlighted number also equals 4, modulo 5.

Does a solution always exist?

Chinese Remainder Theorem

Idea: Construct numbers Δ_1 and Δ_2 so that:

$$\Delta_1 \equiv 1 \pmod 5 \qquad \Delta_2 \equiv 0 \pmod 5$$
$$\Delta_1 \equiv 0 \pmod 7 \qquad \Delta_2 \equiv 1 \pmod 7$$

Then, we can check that $4 \cdot \Delta_1 + 3 \cdot \Delta_2$ satisfies

$$x \equiv 4 \pmod 5 \qquad \text{and} \qquad x \equiv 3 \pmod 7.$$

To construct Δ_1:

- Any multiple of 7 is 0 modulo 7.
- So consider $\Delta_1 = 7 \cdot (7^{-1} \bmod 5)$. This satisfies $\Delta_1 \equiv 1 \bmod 5$.
- Here, $7^{-1} \bmod 5 = 2^{-1} \bmod 5 = 3$. So, $\Delta_1 = 21$.
- Similarly, $\Delta_2 = 5 \cdot (5^{-1} \bmod 7) = 15$.
- So, $x = 4 \cdot 21 + 3 \cdot 15 = 129\ldots$ which equals 24, modulo 35.

This requires $\gcd(5, 7) = 1$.

Chinese Remainder Theorem

Chinese Remainder Theorem (CRT): If $y_1, \ldots, y_n$ are fixed numbers and the moduli $m_1, \ldots, m_n$ are pairwise coprime (i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j$), then the system

$$\begin{aligned} x &\equiv y_1 \pmod{m_1} \\ &\vdots \\ x &\equiv y_n \pmod{m_n} \end{aligned}$$

has a unique solution in $\mathbb{Z}/m_1 \cdots m_n\mathbb{Z}$.[1]

- Why is the solution unique? Consider the map

$$f : \mathbb{Z}/m_1 \cdots m_n\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$$

  given by $f(x) = (x \bmod m_1, \ldots, x \bmod m_n)$.
- The CRT says that the map is surjective. But the domain and range are the same size—f is a bijection.

[1] The construction is the same as before—see notes for details.

Isomorphism

For pairs $(a_1,b_1),(a_2,b_2) \in (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$, where $\gcd(m_1,m_2)=1$, define addition and multiplication:

$$(a_1,b_1)+(a_2,b_2) := (a_1+a_2 \bmod m_1,\ b_1+b_2 \bmod m_2),$$
$$(a_1,b_1)(a_2,b_2) := (a_1a_2 \bmod m_1,\ b_1b_2 \bmod m_2).$$

Consider the map f (the CRT map). Then, for $x,y \in \mathbb{Z}/m_1m_2\mathbb{Z}$,

$$\begin{aligned} f(x+y) &= (x+y \bmod m_1,\ x+y \bmod m_2) \\ &= (x \bmod m_1,\ x \bmod m_2) + (y \bmod m_1,\ y \bmod m_2) \\ &= f(x)+f(y). \end{aligned}$$

What does this say?

- Add $x+y$ in $\mathbb{Z}/m_1m_2\mathbb{Z}$, then convert to $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$. We get $f(x+y)$.
- Convert x and y to $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$, then add them as pairs. We get $f(x)+f(y)$.

Isomorphism

We showed: $f(x+y) = f(x) + f(y)$. Similarly, it holds that $f(xy) = f(x)f(y)$.

$$\begin{aligned} f(xy) &= (xy \bmod m_1,\ xy \bmod m_2) \\ &= (x \bmod m_1,\ x \bmod m_2)(y \bmod m_1,\ y \bmod m_2) = f(x)f(y). \end{aligned}$$

It does not really matter whether you do addition/multiplication in $\mathbb{Z}/m_1 m_2\mathbb{Z}$, or $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$. They are the same.

This is saying *more* than "bijection"—the bijection *preserves* addition and multiplication. Isomorphism. [2]

$$\mathbb{Z}/m_1 m_2\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}).$$

---

[2] To learn more about this, take Math 113.

Consequences of Isomorphism

CRT: If m_1 and m_2 are coprime, then
$\mathbb{Z}/m_1 m_2\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$. (isomorphism)

Fact: a has an inverse in $\mathbb{Z}/m_1 m_2\mathbb{Z}$ if and only if
$(a \bmod m_1,\ a \bmod m_2)$ has an inverse in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$.

What does it mean for (a, b) to have an inverse (x, y)?

$$(a, b)(x, y) = (1, 1).$$

In $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$, $(1, 1)$ is the multiplicative identity.

So, a has an inverse in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ if and only if it has an inverse in both $\mathbb{Z}/m_1\mathbb{Z}$ and $\mathbb{Z}/m_2\mathbb{Z}$.

This happens if and only if $\gcd(a, m_1) = \gcd(a, m_2) = 1$. But m_1 and m_2 are pairwise coprime. So, $\gcd(a, m_1 m_2) = 1$.

CRT, Euler's Totient Function

If $\gcd(m_1, m_2) = 1$, a has an inverse in $\mathbb{Z}/m_1 m_2\mathbb{Z}$ if and only if $(a \bmod m_1, a \bmod m_2)$ has an inverse in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$.

In particular, $|(\mathbb{Z}/m_1 m_2\mathbb{Z})^\times| = |(\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times|$.

The RHS is $|(\mathbb{Z}/m_1\mathbb{Z})^\times| \cdot |(\mathbb{Z}/m_2\mathbb{Z})^\times|$.

So, for coprime m_1 and m_2, $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.

So, φ is called **multiplicative.** [3]

[3] To learn more about the Euler totient function, multiplicative functions, and number theory, try Math 115.

Formula for Euler's Totient Function

For $n \geq 2$, write $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (prime factorization).

By multiplicativity, $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$.

So, what is $\varphi(p^\alpha)$ for p prime and a positive integer α?

There are p^α numbers from 1 to p^α. How many of them are *not* coprime with p^α?

$p, 2p, 3p, \ldots, p^\alpha$. There are $p^{\alpha-1}$ of them. So,
$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Thus, $\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$.

Using Euler's Theorem for Exponentiation

We can use Euler's Theorem to calculate $5^{1000000} \bmod 12$.

By Euler's Theorem, since $\gcd(5, 12) = 1$, then $5^{\varphi(12)} \equiv 1 \pmod{12}$.

So, $\varphi(12) = \varphi(2^2)\varphi(3) = 2 \cdot 2 = 4$.

- In fact, $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$.

So, write $5^{1000000} \equiv 5^{250000 \cdot 4} \equiv 1 \pmod{12}$.

In general, $a^k \equiv a^{k \bmod \varphi(m)} \pmod{m}$, if $\gcd(a, m) = 1$.

Polynomials

A **polynomial** is a function

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0.$$

The integer $d \in \mathbb{N}$ is called the **degree** of the polynomial.

- Exception: If $P(x) = 0$ for all x, the zero polynomial, then the degree is sometimes considered to be $-\infty$.

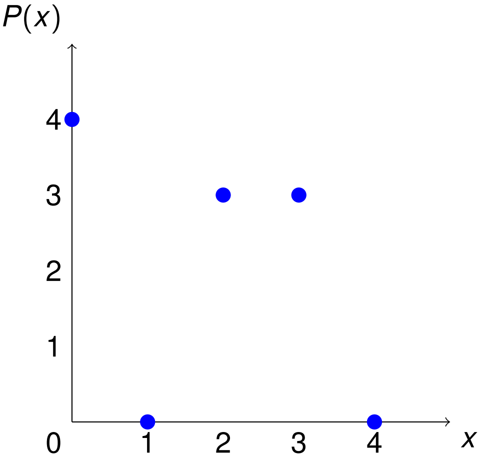
The numbers $a_0, a_1, \ldots, a_d$ are the **coefficients**. We say this is the coefficient representation.

Polynomials involve addition, multiplication.

- We can also consider polynomials over $\mathbb{Z}/m\mathbb{Z}$.

Polynomials in Modular Arithmetic

What does the polynomial $P(x) = x^2 + 4$ look like, modulo 5?



Not a continuous curve!

Polynomial Degree

Consider polynomials P and Q of degrees $d_1, d_2 > 0$.

What is the degree of $P + Q$?

- $\deg(P + Q)$ is at most $\max\{d_1, d_2\}$.
- Potentially $-\infty$, if $P = -Q$.

What is the degree of PQ?

- $d_1 + d_2$.

Fields

Without being too formal, a **field** is

- a set with two operations, $+$ (addition) and $\cdot$ (multiplication)
- such that addition and multiplication are associative and commutative;
- multiplication distributes over addition;
- every element has an additive inverse;
- every non-zero element has a multiplicative inverse.

What are some examples of fields?

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- $\mathbb{Z}/p\mathbb{Z}$ where p is prime.

What is not a field?

- $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ for m composite: missing multiplicative inverses.

Polynomial Long Division

Recall the Division Algorithm: Given $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, b-1\}$ with $a = qb + r$.

Polynomial Division: Given polynomials A and B where B is not constant, there exist unique polynomials Q and R with $A = QB + R$, and $\deg R < \deg B$.

Example: To divide $6x^4 + 4x^3 + 2x + 1$ by $3x + 2$:

- Match coefficients. Multiply $3x + 2$ by $2x^3$. Then $2x^3(3x+2) = 6x^4 + 4x^3$.
- The remaining terms are $2x + 1$. Match coefficients. Multiply $3x + 2$ by $2/3$. $(2/3)(3x+2) = 2x + 4/3$.
- So, $(2x^3 + 2/3)(3x+2) = 6x^4 + 4x^3 + 2x + 4/3$.
- So, $6x^4 + 4x^3 + 2x + 1 = (2x^3 + 2/3)(3x+2) - 1/3$.

The algorithm needs multiplicative inverses—work in a field.

Polynomial Roots

A **root** of a polynomial P is a value a such that $P(a) = 0$.

Theorem: The polynomial P has the root a if and only if $P(x) = (x - a)Q(x)$ for a polynomial Q.

Proof.

- ($\Longleftarrow$): Plug in $x = a$ to get $P(a) = 0$.
- ($\Longrightarrow$): By Division Algorithm, $P(x) = (x - a)Q(x) + R$, where $\deg R < 1$. So, R is a constant.
- Plug in $x = a$. $0 = P(a) = R$. $\square$

Degree d Has At Most d Roots

Theorem: If a non-zero polynomial P is degree d, it has at most d roots.

Proof.

- If a is a root of P, then factor $P(x) = (x - a)Q(x)$.
- Each root we factor out reduces the degree of the remaining polynomial by 1.
- Since P has degree d, we can only factor out at most d roots. $\square$

Polynomials vs. Functions

Consider polynomials P and Q over $\mathbb{Z}/p\mathbb{Z}$ for p prime.

Two definitions of equality:

- $P = Q$ if every coefficient is the same.
- $P = Q$ as *functions*: $P = Q$ if $P(x) = Q(x)$ for every $x \in \mathbb{Z}/p\mathbb{Z}$.

By the first definition, there are infinitely many distinct polynomials.

By the second definition, there are only finitely many polynomials. There are finitely many functions $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

- There are p possible outputs for the first input.
- Then p possible outputs for the second input.
- ... and p possible outputs for the pth input.
- There are p^p functions $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Polynomial Interpolation

Say we are given $d+1$ points $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$.

Can we find a polynomial that goes through these points?

A degree d polynomial has the representation
$P(x) = a_d x^d + \cdots + a_1 x + a_0$.
Try solving the system:

$$\begin{aligned} y_1 &= a_d x_1^d + \cdots + a_1 x_1 + a_0 \\ &\vdots \\ y_{d+1} &= a_d x_{d+1}^d + \cdots + a_1 x_{d+1} + a_0 \end{aligned}$$

There are $d+1$ equations, $d+1$ unknown coefficients. The system is linear.

- Try solving this system with linear algebra.

Lagrange Interpolation

Remember CRT? To solve

$$x \equiv y_1 \pmod{m_1}$$
$$x \equiv y_2 \pmod{m_2}$$

find Δ_1 and Δ_2 so that

$$\Delta_1 \equiv 1 \pmod{m_1} \qquad \Delta_2 \equiv 0 \pmod{m_1}$$
$$\Delta_1 \equiv 0 \pmod{m_2} \qquad \Delta_2 \equiv 1 \pmod{m_2}$$

and then take $x = y_1\Delta_1 + y_2\Delta_2$.

Same idea for polynomials. For $i = 1, \ldots, d+1$, we want:

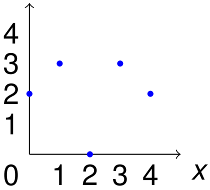
$$\Delta_i(x_j) = \begin{cases} 1, & j = i \\ 0, & j \neq i \end{cases}$$

and then $P(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)$.

Picture of Lagrange Interpolation

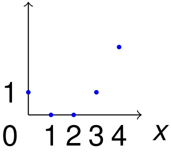
Consider points $(0,2)$, $(1,3)$, and $(2,0)$ in $\mathbb{Z}/5\mathbb{Z}$.

$$P(x) = 3x^2 + 3x + 2$$

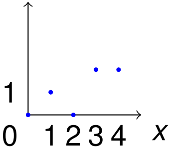


Here, $P(x) = 2 \cdot \Delta_1(x) + 3 \cdot \Delta_2(x)$.

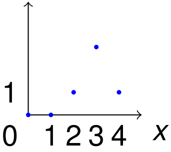
$\Delta_1(x) = 3x^2 + x + 1$



$\Delta_2(x) = 4x^2 + 2x$



$\Delta_3(x) = 3x^2 + 2x$



Constructing Δ Polynomials

For distinct points $x_1, \ldots, x_{d+1}$, construct:

$$\Delta_i(x_j) = \begin{cases} 1, & j = i \\ 0, & j \neq i \end{cases}$$

How? First, consider the polynomial

$$Q(x) = \prod_{j \neq i} (x - x_j).$$

This polynomial is zero at all x_j, $j \neq i$. Now set:

$$\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}.$$

This polynomial satisfies the required conditions. (Note: Division requires a field.) Also, $\deg \Delta_i = d$.

Polynomial Interpolation

Theorem: Given $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, where $x_1, \ldots, x_{d+1}$ are *distinct*, there is a *unique* polynomial P of degree at most d going through these points.

Proof.

- Existence: We constructed the polynomial using Lagrange interpolation!
- Each Δ_i has degree at most d, so $\deg P \leq d$.
- Uniqueness: Say that P_1 and P_2 both go through these points. Then, $P_1 - P_2$ has $d+1$ roots, $x_1, \ldots, x_{d+1}$.
- Since $P_1 - P_2$ has degree at most d, then $P_1 - P_2$ must be the zero polynomial, i.e., $P_1 = P_2$. $\square$

Slogan: $d+1$ points uniquely determine a degree $\leq d$ polynomial.

Summary

- CRT: $\mathbb{Z}/m_1 \cdots m_n\mathbb{Z}$ and $(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$ are isomorphic if $m_1, \ldots, m_n$ are pairwise coprime.
- If $\gcd(m_1, m_2) = 1$, then $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$ (φ is multiplicative).
- Thus, $\varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$ for a prime factorization.
- We work over fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ (AKA GF(p)) for p prime.
- A polynomial has a root a if and only if $P(x) = (x - a)Q(x)$ for some polynomial Q.
- A polynomial of degree d has at most d roots.
- Lagrange Interpolation: $d + 1$ distinct points uniquely determine a degree $\leq d$ polynomial.