Theorems and Definitions

12:28 PM

Definitions

Set:
A collection of distinct objects

Axiom:
A proposition which serves as a "starting point". Statements which are either self evident or defined for the purposes of further logical derivation.

Axioms cannot be proven as there are the base assumptions.

Commutative Ring:
A set R with operations "+" and "×" satisfying the properties A1-4, M-13, and D1

Field:
A commutative ring also satisfying M4.

Non-Commutative Ring:
A set R with operations "+" and "×" satisfying all of the properties of a commutative ring except for M1 and additionally satisfying D2

Contrapositive
The contrapositive of A ⇒ B is "not B" ⇒ "not A". They are equivalent.

Divisibility
In a commutative ring R, if a , b ∈ R we say a|b (a divides b) iff there is a c ∈ R such that b = ac

Prime Number
A prime (integer) is a positive integer p ≠ 1 such that the only divisors of p in **Z** are 1 and p

Integer Linear Combination
c is an integer linear combination of a, b ∈ ℤ if and only if there are s, t ∈ ℤ with
$c = sa + tb$

Greatest Common Divisor (GCD)
Let a, b ∈ ℤ be non-zero. Then gcd(a, b) is the largest d ∈ ℤ such that d|a and d|b.

Diophantine Equation
An equation with integer coefficients that one wants to solve over ℤ.

Congruence
Let a, b ∈ ℤ and n ∈ ℕ.
We say that a and b are congruent modulo n iff $n|(a-b)$
Write
$a \equiv b \ (mod\ n)$

Congruence/Residue Class
The "congruence class" or "residue class" of a ∈ ℤ modulo n is the set:
[a] = {b ∈ ℤ : $a \equiv b$ (mod n)}
For a fixed n

A Ring Z_n
The ring $\mathbb{Z}_n$ Is the set {[0], [1], ..., [n-1]} with the operations "+" and "·" defined by [a]+[b] = [c] iff $a + b \equiv c$ (mod n) and [a]·[b] = [c] iff $ab \equiv c$ (mod n). The zero element will be [0] and the one element is [1].

Permutation
A permutation of a set is a function from the set to itself which is:
1. Injective (one-to-one)
2. Surjective (onto)

Least Non-Negative Residue

Theorems and Principles

Well-Ordering Principle
If S ⊆ **N** and S is not empty, then S has a least element.

⊆ - Subset of

Induction Principle
Suppose that P(n) is some statement about the natural number n, suppose that P(1) holds and suppose that whenever P(k) is true for 1 ≤ k < n, the P(n) is true. Then P(n) holds for all n.

Unique Factorization
Every integer other than zero can be written in the form:
$\pm 1 \times p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times \cdots \times p_r^{a_r}$
This representation is unique up to reordering.

Primes
There are infinitely many primes.

Let p_n be the nth prime. Then $p_n < 2^{2^{n-1}}$.

Let p_n denote the nth prime. Then $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges.

The Division Algorithm
Let a ≥ 1 and b be integers. Then there exist integers q and 0 ≤ r < a such that
$b = aq + r$

Bezout's Identity (Extended Euclidian Algorithm)
If a and b are positive integers, then there exist x, y ∈ ℤ such that $ax + by = \gcd(a, b)$

Factoring Integers
If a and b are nonzero integers with $\gcd(a, b) = 1$ and a|bc, then a|c

Let p be a prime, and suppose that $p|a_1 a_2 \dots a_n$ $(a_i \in \mathbb{Z})$
The $p|a_i$ for some i

Chinese Remainder Theorem v.2
Let $M_1, M_2, \dots, M_k$ be rational number with $\gcd(M_i, M_j) = 1$
For all i ≠ j
Let $a_1, a_2, \dots, a_k \in \mathbb{Z}$. Then there is a solution x ∈ ℤ to
$x \equiv a_1 \ (mod\ M_1)$
$x \equiv a_2 \ (mod\ M_2)$
...
$x \equiv a_k (mod\ M_3)$
If x_0 is one solution, then x is another iff $x \equiv x_0 (mod\ M_1 M_2 \dots M_k)$

Fermat's Little Theorem
Let p be a prime and a ∈ ℤ with gcd(a, p) = 1
Then $a^{p-1} \equiv 1 (mod\ p)$

Fermat's Little Theorem, alternate form
If p∤a and $e_1 \equiv e_2 \ (mod\ p-1)$ then $a^{e_1} \equiv a^{e_2} \ (mod\ p)$

Euler's Totient Function
For m ≥ 1, $\varphi(m) = \#\ of\ values\ 0 \le k < m\ s.t. \gcd(k, m) = 1$
$= the\ number\ of\ units\ in\ the\ ring\ \mathbb{Z}_n$

Suppose gcd(n, m) = 1. Then $\varphi(nm) = \varphi(n)\varphi(m)$

If p is prime, e ≥ 1, then
$\varphi(p^e) = p^{e-1}(p-1)$

Euler's Theorem
Let n ≥ 1 and a are integers gcd(a, n) = 1. Then
$a^{\phi(n)} \equiv 1 \ (mod\ n)$

The least non negative residue of
$x \ (mod\ n)$ is a such that $[x] = [a]$ and
$0 \leq a \leq n$

Relation

A relation on a set is a set of pairs (a, b) which are "related".

Equivalence Relation

A relation $\approx$ on a set S is an equivalence relation if and only if:

1. $a \approx a$ for all a ∈ S
2. $a \approx b$ iff $b \approx a$ for all a, b ∈ S
   Symmetric
3. If $a \approx b$ and $b \approx c$ then $a \approx c$, for all a, b, c ∈ S
   Transitivity

Equivalence Classes

Given an equivalence relation $\approx$ on a set S, and a ∈ S define
$[a]_{\approx} = \{b \approx a, b \in S\}$

Rings and Fields

September-13-10 3:10 PM

Set:
A collection of distinct objects

Axiom:
A proposition which serves as a "starting point". Statements which are either self evident or defined for the purposes of further logical derivation.

Axioms cannot be proven as there are the base assumptions.

Commutative Ring:
A set R with operations "+" and "×" satisfying the properties A1-4, M-13, and D1

Field:
A commutative ring also satisfying M4.

Non-Commutative Ring:
A set R with operations "+" and "×" satisfying all of the properties of a commutative ring except for M1 and additionally satisfying D2

The Integers $\mathbb{Z}$ = {0, 1, 2, -1, -2, … }

Properties satisfied by Z - Commutative Ring

[si] The integers consist of the set **Z** and the operations "+" and "×"

[A1] Commutativity of Addition
For all a, b ∈ **Z**, $a + b = b + a$

[A2] Associativity of Addition
For all a, b, c ∈ **Z**, $(a + b) + c = a + (b + c)$

[A3] Additive Identity
There exists an element 0 ∈ **Z** such that $a + 0 = a$ for all a ∈ **Z**

[A4] Additive Inverse
For all a ∈ **Z,** there exists an element -a ∈ **Z** such that $a + (-a) = 0$

[M1] Commutativity of Multiplication
For all a, b ∈ **Z**, $a \times b = b \times a$

[M2] Associativity of Multiplication
For all a, b, c ∈ **Z**, $(a \times b) \times c = a \times (b \times c)$

[M3] Multiplicative Identity
There exists an element 1 ∈ **Z** such that $1 \times a = a$ for all a ∈ **Z**

[D1] Distributive Property
$(a + b) \times c = ac + bc$

$\mathbb{R}$ also satisfy the above properties with the usual "+" and "×" operations, as do $\mathbb{Q}$.
$\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ etc. are all commutative rings therefore properties proved for commutative rings will hold for all.

Fields

Let $\mathbf{F_2}$ be the set {0, 1}
Operators:

+	**0**	**1**
0	0	1
1	1	0

×	**0**	**1**
0	0	0
1	0	1

This is a commutative ring.

Sometimes we'll study rings with some additional properties:

[M4] Multiplicative Inverse
For all a ∈ **Z**, a $\neq 0$ there exists an element a^{-1} ∈ **Z** such that $a \times a^{-1} = 1$

Commutative rings with this property are called fields. **R**, **Q**, and $\mathbf{F_2}$ are all fields. **Z** is not a field.

Non-Commutative Ring

Does not satisfy M1

Let M be the set of 2x2 matrices with integer entries.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

With matrices, multiplication is not commutative.
Because M1 no longer applies, a new distributive property is needed:

[D2] Distributive Property
$a \times (b + c) = ab + ac$

Assignment 1

September-14-10 12:03 PM

PMATH 145 Assignment 1

Patrick Ingram

due September 29th by 12:30PM

Problem 1. The Fibonacci numbers F_n are defined by $F_0 = 0$, $F_1 = 1$, and

$$F_n = F_{n-1} + F_{n-2}$$

for all $n \geq 2$, so that $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, *etc.* (WARNING: The textbook defines the sequence differently, so that all terms are shifted by 1. Ignore that.)

(a) Prove that $F_n < 2^n$ for all $n \in \mathbb{N}$. (Induction might be helpful.)

(b) Prove that

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

for all $n \in \mathbb{N}$.

(c) Prove that

$$F_{2n} = F_{n+1}^2 - F_{n-1}^2$$

for all $n \in \mathbb{N}$.

(d) Let $\tau = (1 + \sqrt{5})/2$, the golden ratio. Prove that

$$F_n = \frac{\tau^n - (-1/\tau)^n}{\sqrt{5}}$$

for all $n \in \mathbb{N}$. (It might be useful to note that $\tau^2 - \tau - 1 = 0$.)

(e) Prove that

$$F_{n+m} = F_m F_{n+1} + F_{m-1}F_n$$

for all $n, m \in \mathbb{N}$.

Note: all of these properties hold for $n = 0$, too. I just asked you to prove them for $n \in \mathbb{N}$ for convenience.

Problem 2. Recall that $\sqrt{2}$ is irrational, and define

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \right\}.$$

(a) Show that if $a + b\sqrt{2} = c + d\sqrt{2}$, for some $a, b, c, d \in \mathbb{Q}$, then $a = c$ and $b = d$. This shows that the representation of an element of $\mathbb{Q}(\sqrt{2})$ in the form $a + b\sqrt{2}$ is unique.

(b) Let $x, y \in \mathbb{Q}(\sqrt{2})$. Show that 0, 1, $x + y$, xy, and $-x$ are in $\mathbb{Q}(\sqrt{2})$. This shows that $\mathbb{Q}(\sqrt{2})$ is a *subring* of $\mathbb{R}$. (The definition of a subring is that it's a subset of a ring which is closed under addition, multiplication, and taking additive inverses, and contains 0 and 1. A subring automatically satisfies the criteria for being a ring.)

(c) Show that $\mathbb{Q}(\sqrt{2})$ is a field. That is, show that if $x \neq 0$, then there is an element $x^{-1} \in \mathbb{Q}(\sqrt{2})$ such that $x \cdot x^{-1} = 1$.

Problem 3. Let

$$\mathbb{Z}[\sqrt{2}] = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Z} \right\},$$

which is clearly a subset of $\mathbb{Q}(\sqrt{2})$. For $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, we define the *conjugate* of x over $\mathbb{Z}$ to be $\overline{x} = a - b\sqrt{2}$, and define the *norm* by $N(x) = x \cdot \overline{x}$.

(a) Prove that $N(x) \in \mathbb{Z}$, for all $x \in \mathbb{Z}[\sqrt{2}]$.

(b) Prove that $N(xy) = N(x)N(y)$, for all $x, y \in \mathbb{Z}[\sqrt{2}]$.

(c) An element x of a ring is called a *unit* if and only if there is an element x^{-1} in the ring such that $x \cdot x^{-1} = 1$ (so, another way of defining a field is by saying that it's a commutative ring in which everything except 0 is a unit). Note that this definition depends on the ring: 2 is a unit in $\mathbb{Q}$, but isn't a unit in $\mathbb{Z}$.

Show that $17 + 12\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is a unit.

(d) Prove that $x \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $N(x) = \pm 1$.

(e) Prove that there are infinitely many units in $\mathbb{Z}[\sqrt{2}]$.

Problem 4. Recall that if R is a commutative ring, and $a, b \in R$, then the notation $a \mid b$ means that there exists a $c \in R$ such that $b = ac$.

(a) Let $a, b, c, d, e \in \mathbb{Z}$, and suppose that $a \mid b$ and $a \mid c$. Show that $a \mid (db + ce)$.

(b) Let R be a field. Prove that for $a, b \in R$, we have $a \mid b$ whenever $a \neq 0$, and that $0 \mid b$ if and only if $b = 0$.

Problem 5. Prove that for every $m \in \mathbb{N}$ there exists an $n \in \mathbb{N}$ such that none of the numbers

$$n, n + 1, n + 2, ..., n + m$$

is prime.

Induction

September-15-10 12:37 PM

Well-Ordering Principle

If S ⊆ **N** and S is not empty, then S has a least element.

⊆ - Subset of

Induction Principle

Suppose that P(n) is some statement about the natural number n, suppose that P(1) holds and suppose that whenever P(k) is true for $1 \leq k < n$, the P(n) is true. Then P(n) holds for all n.

Contrapositive

The contrapositive of A ⇒ B is "not B" ⇒ "not A". They are equivalent.

Example of Induction Principle - Arithmetic Series

$P(n): \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof:

$P(1)$ says $1 = \frac{1(1+1)}{2}$ which is true

Induction step:
Assume that P(k) holds for all $1 \leq k < n$
Since P(n-1) holds,

$$\sum_{i=1}^{n-1} i = \frac{(n-1)n}{2}$$

So

$$\sum_{i=1}^{n} i = \sum_{i=1}^{n-1} i + n = \frac{(n-1)n}{2} + n = \frac{n^2 - n + 2n}{2} = \frac{n(n+1)}{2}$$

By induction, P(n) holds for all $n \geq 1$

Induction ⇒ Well-Ordering Principle

Want to prove if S ⊆ **N** has no least element, then S = ∅ (empty set)
Let P(n) be "n ∉ S" where S has no least element
Base case: P(1) since if 1 ∈ S has a least element.

Induction case:
Assume P(k) for all $1 \leq k < n$ (n here is at least 2)
So k ∉ S for $1 \leq k < n$
Then n ∉ S because otherwise n would be the smallest element of S
So P(n) holds.

By induction, P(n) holds for all n so n ∉ S for all n ∈ **N**
∴ S = ∅ ■

Primes and Divisibility

September-15-10 1:04 PM

Divisibility

In a commutative ring R, if a , b ∈ R we say a|b (a divides b) iff there is a c ∈ R such that b = ac

Prime Number

A prime (integer) is a positive integer p ≠ 1 such that the only divisors of p in **Z** are 1 and p

Fundamental Theorem of Arithmetic

Every integer other than zero can be written in the form:
$\pm 1 \times p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times \cdots \times p_r^{a_r}$
This representation is unique up to reordering.

Theorem:

There are infinitely many primes

Theorem:

Let p_n be the nth prime. Then $p_n < 2^{2^{n-1}}$.

Diverging Sum

An infinite sum of positive real numbers:
$\sum_{n=1}^{\infty} a_n$
Diverges iff for all M there exists an N with
$\sum_{n=1}^{N} a_n \geq M$
In other words, $\sum_{n=1}^{\infty} a_n$ diverges iff
$\lim_{N \to \infty} \sum_{n=1}^{N} a_n = \infty$

Proof of Existence of Factorization (Fundamental Theorem of Arithmetic)

Let n ≥ 1
Let P(n) be the statement "there exists a way of writing $n = 1 \times p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times \cdots \times p_r^{a_r}$
P(1) is true, because 1 = 1
Suppose that P(k) holds for all 1 ≤ k < n (n ≥ 2)

If n is prime, the P(n) holds because $n = n^1$. If n is not prime, we can write n = ab, where 1 ≤ a, b, < n. We can write a and b as products of prime powers since P(a) and P(b) hold. So we can write n = ab as a product of prime powers.

By induction, every positive integer can be written as a product of powers of distinct primes.

Theorem: There are infinitely many primes

Proof:
Suppose that there are a finite number of primes, and list all of the primes $p_1, p_2, p_3, \ldots, p_n$. Then $p_1 \times p_2 \times p_3 \times \cdots \times p_n + 1$ is not divisible by any prime and yet is not on the list of primes. This is a contradiction, so there are infinitely many primes. ■

Frequency of Primes

Let π(x) = # of primes less than x.
π: ℝ -> ℕ ∪ {0}

Theorem:

Let p_n be the nth prime. Then $p_n \leq 2^{2^{n-1}}$.
Proof:
Base case n = 1 $p_1 = 2 \leq 2^{2^{1-1}}$
Induction. Suppose that $p_k \leq 2^{2^{k-1}}$ for all 1 ≤ k < n

Then $p_1 \times p_2 \times \cdots \times p_{n-1} + 1 \leq 2^{2^0} \times 2^{2^1} \times \cdots \times 2^{2^{n-2}} + 1$
$= 2^{2^0+2^1+\cdots+2^{n-2}} + 1$
$= 2^{2^{n-1}-1} + 1 = \frac{1}{2} \times 2^{2^{n-1}} + 1 \leq 2^{2^{n-1}}$
So $p_1 \times p_2 \times \cdots \times p_{n-1} + 1 \leq 2^{2^{n-1}}$
But $p_1 \times p_2 \times \cdots \times p_{n-1} + 1$ is divisible by some prime $q \geq p_{n-1}$
So $p_n \leq q \leq p_1 \times p_2 \times \cdots \times p_{n-1} \times p_n + 1 \leq 2^{2^{n-1}}$
So $p_n \leq 2^{2^{n-1}}$, and by induction we have the same for all n≥ 1

There is also a lower bound for the number of primes.
In particular, $\pi(x) \geq \log_2(\log_2(x))$

Why?
If π(x) = n, then $x \leq p_{n+1} \leq 2^{2^n}$
$\log_2(\log_2 x)) \leq n \leq \pi(x)$

Theorem:

Let p_n denote the nth prime. Then
$\sum_{n=1}^{\infty} \frac{1}{p_n}$
diverges.

Proof

Suppose that $\sum_{n=1}^{\infty} \frac{1}{p_n}$ converges where p_n is the nth prime.
If this is true, then there exists a k ≥ 1 such that
$\sum_{n=k+1}^{\infty} \frac{1}{p_n} < \frac{1}{2}$
Since the sum converges, then some subset at the end of the sum must be less than some arbitrary value.

Let $N = 4^{k+1}$
We'll count the elements of {1, 2, 3, ..., N}
First way: Clearly there are N elements in the set.

Let $X = \{1 \leq a \leq N : p_i | a \text{ for some } i \geq k+1\}$
Let $Y = \{1 \leq a \leq N : a \text{ is not in } X\}$
It should be clear that number of elements in X + number of elements in Y = N

Each element of X is divisible by some prime p_i for some i ≥ k+1
The number of integers from 1 to N divisible by p_i is at most $\frac{N}{p_i}$
Reason: if $p_i | x$ then $x = p_i \times m$ where $1 \leq m \leq \frac{N}{p_i}$

Therefore

$$\#X \leq \sum_{i=k+1}^{\infty} (\#\ of\ 1 \leq x \leq N\ divisible\ by\ p_i)$$
$$\leq \sum_{i=k+1}^{\infty} \frac{N}{p_i} = N \times \sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{N}{2}$$

Now we count the elemetns of Y. Every Element of Y can be written as $p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$ for some $e_i \geq 0$. It follows that every element of Y can be written as $p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k} \times b^2$, where $a_i = 0, 1$ for all i.

If $p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k} \times b^2 \leq N$, certainly $b \leq \sqrt{N}$. Since b is an integer, this leaves $\leq \sqrt{N}$ choices for b. Since each a_i is either 0 or 1, there are only 2^k choices for $a_1 \times a_2 \times \cdots \times a_k$
So the number of integers $1 \leq x \leq N$ which can be written in the form $\propto = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k} \times b^2$, for b ∈ N and $a_i = 0\ or\ 1$ is at most $2^k\sqrt{N}$
Therefore, $\#Y \leq 2^k\sqrt{N}$

$$2^k\sqrt{N} = 2^k\sqrt{4^{k+1}} = 2^k \times 2^{k+1} = 2^{\,2k+1}$$
$$= \frac{1}{2} \times 2^{2k+2} = \frac{1}{2} 4^{k+1} = \frac{N}{2}$$
$$\#Y \leq \frac{N}{2}$$

We assumed that $\sum_{n=1}^{\infty} \frac{1}{p_n}$ converges and showed that for some N:
$$N = \#X + \#Y < \frac{N}{2} + \frac{N}{2} = N$$
This is a contradiction. Therefore
$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$
diverges.

*Binomial Theorem

September-20-10 4:27 PM

The Binomial Theorem

Let x, y be variables, n ∈ ℕ. Then

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i$$

Binomial: a+b

Powers of binomials: $(a+b)^2 = a^2 + 2ab + b^2$

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

Binomial Theorem used to find $(a+b)^n,\ n \geq 1$

Notation/Definitions

Factorial function:

$0! = 1$

$n \geq 1, n! = n(n-1)(n-2)$

Binomial coefficients:

If n, r ∈ ℤ, 0≤ r ≤ n

$\binom{n}{r}$ Read "n choose r" is defined by:

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$$

Combinatorial meaning of $\binom{n}{r}$ is the number of ways of choosing r elements from a set with n elements.

$$n! = \binom{n}{r} \times r! \times (n-r)!$$

n! is the number of orderings for n elements

Properties of the Binomial Coefficient

1. $\binom{n}{r} = \frac{n \times (n-1) \times \cdots (n-r+1)}{r!}$
2. $\binom{n}{r}$ is an integer
3. $\binom{n}{0} = 1 = \binom{n}{n}$
4. $\binom{n}{r} = \binom{n}{n-r}$
5. If 1 ≤ r ≤ n, then $\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r+1}$

Proof 1

$S = \{e_1, e_2, e_3, \ldots, e_{n+1}\}$ Choose r elements from S

If e_{n+1} is one of them, then there are $\binom{n}{r-1}$ ways of choosing the others.

If e_{n+1} is not one of them, then there are $\binom{n}{r}$ ways of choosing the others

$\Rightarrow \binom{n+1}{r} = \binom{n}{r} + \binom{n}{r+1}$

Proof 2

$$\binom{n}{r} + \binom{n}{r-1} = \frac{n!}{r!\,(n-r)!} + \frac{n!}{(r-1!)(n-(r-1))!} = \frac{n!\,(n+1-r)! + n!\,r}{r!\,(n+1-r)!}$$

$$= \frac{(n+1)!}{r!\,(n+1-r)!} = \binom{n+1}{r}$$

The Binomial Theorem

Let x, y be variables, n ∈ ℕ. Then $(x+y)^n = \sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i$

Proof: Induction on n

n = 1

$$(x+y)^1 = \binom{1}{0}x + \binom{1}{1}y = x + y$$

Want to prove $(x+y)^{k+1} = \sum_{i=0}^{k+1}\binom{k+1}{i}x^{k+1-i}y^i$

$$(x+y)^{k+1} = (x+y)(x+y)^k = (x+y) \times \sum_{i=0}^{k}\binom{k}{i}x^{k-i}y^i$$

$$= \sum_{i=0}^{k}\binom{k}{i}x^{k+1-i}y^i + \sum_{i=0}^{k}\binom{k}{i}x^{k-i}y^{i+1}$$

Terms with the same powers will have coefficients that match in the form $\binom{k}{i} + \binom{k}{i-1}$

$$= \sum_{i=0}^{k+1}\binom{k+1}{i}x^{k+1-i}y^i$$

Division and Euclid's Algorithm

September-22-10 12:31 PM

The Division Algorithm

Let $a \geq 1$ and b be integers. Then there exist integers q and $0 \leq r < a$ such that
$b = aq + r$

Greatest Common Divisor (GCD)

Let $a, b \in \mathbb{Z}$ be non-zero. Then gcd(a, b) is the largest $d \in \mathbb{Z}$ such that d|a and d|b.

Remarks:

1. If d|a, and $a \neq 0$, then $d \leq |a|$
2. We can define gcd(a, 0) if $a \neq 0$ just by gcd(a, 0) = gcd(0, a) = |a|

Euclidian Algorithm for GCD

Basic idea: If b = aq + r, then gcd(b, a) = gcd(a, r)

Proof of Long Division

Let $a \geq 1$ and b be integers. Then there exist integers q and $0 \leq r < a$ such that
$b = aq + r$

Let S = {s : s = b-aq for some $q \in \mathbb{Z}$ and $s \geq 0$}

This set is non-empty, since $a \geq 1$ so we can choose q with $b \geq aq$
$S \subseteq \mathbb{N}$ so if $S \neq \emptyset$, S has a least element, call it $r \in S$.
$r = b - aq$ for some $q \in \mathbb{Z}$.
Also, $r \geq 0$
Suppose $r \geq a$
Then $r - a \geq 0$, and b = aq +r = a(q+1) +(r-a)
So r-a ∈ S

But r-a < r. This is a contradiction. So r < a ■

How to Calculate GCD?

1. List all divisors of a, all divisors of b, and choose the largest common element in each list.
2. Factor a & b as a product of powers of primes, because it is easy to describe divisibility in terms of theses factorizations. (eg. $p^e | p^f$ iff $e \leq f$)

Euclidian Algorithm for GCD

Basic idea: If b = aq + r, then gcd(b, a) = gcd(a, r)

Proof

We'll suppose that $a, b \geq 1$
If b = aq + r and d|a and d|b then d| b - aq = r
Conversely, if d|a and d|r, then d| aq + r = b

Therefore, {common divisors of a & b} = {common divisors of a & r}
gcd(a, b) = gcd(a, r)

If we start with $b > a \geq 1$, then b > a & a > r

Bezout's Identity

September-24-10 1:06 PM

Integer Linear Combination

c is an integer linear combination of a, b ∈ ℤ if and only if there are s, t ∈ ℤ with
$c = sa + tb$

Factoring Integers

Lemma:

If a and b are nonzero integers with $\gcd(a, b) = 1$ and a|bc, then a|c

Lemma:

Let p be a prime, and suppose that $p|a_1a_2 \dots a_n$ $(a_i \in \mathbb{Z})$
The $p|a_i$ for some I

Bezout's Identity (Extended Euclidian Algorithm)

If a and b are positive integers, then there exist integers s & t so that as + bt = gcd(a, b)

Bezout's Identity (Extended Euclidian Algorithm)

If a and b are positive integers, then there exist integers s & t so that as + bt = gcd(a, b)

How? Use the Euclidian algorithm.
In computing $\gcd(a_1, a_2)$ $a_1 > a_2 \geq 0$
$a_1 = q_1a_2 + a_3$
$a_2 = q_2a_3 + a_4$
$a_{n-2} = q_{n-2}a_{n-1} + a_n$ <- you can write $\gcd(a_1, a_2)$ as an ILC of a_{n-2} and a_{n-1}
$a_{n-1} = q_{n-1}a_n + 0$

The previous line allows you to write a_{n-1} in terms of a_{n-3} and a_{n-2} so you can write $\gcd(a_1, a_2)$ as an ILC of a_{n-3} and a_{n-2}

Ex.
$\gcd(5172, 1002) = ?$
$5172 = 5 \times 1002 + 162$
$1002 = 6 \times 162 + 30$
$162 = 5 \times 30 + 12$
$30 = 2 \times 12 + 6$
$12 = 2 \times 6$

Backwards to compute ILC
$6 = 1 \times 30 + (-2) \times 12$
$= 1 \times 30 + (-2)(162 - 5 \times 30)$
$= 11 \times 30 + (-2) \times 162$
$= 11 \times (1002 - 6 \times 162) + (-2) \times 162$
$= 11 \times 1002 + (-68) \times 162$
$= 11 \times 1002 + (-68)\big(5172 + (-5 \times 1002)\big)$
$= (-68) \times 5172 + (351) \times 1002$

Factoring Integers

Lemma:

If a and b are nonzero integers with $\gcd(a, b) = 1$ and a|bc, then a|c

Proof:
Chose integers s and t such that as + bt = 1, and d such that ad = bc
$c = c \times 1$
$= c\ (as + bt)$
$= cas + cbt$
$= cas + adt$
= a(cs + dt)
So a|c. ■

Lemma:

Let p be a prime, and suppose that $p|a_1a_2 \dots a_n$ $(a_i \in \mathbb{Z})$
The $p|a_i$ for some i

Proof
By induction on n.
Base case: n = 2
Suppose that $p|a_1a_2$
If $p|a_i$, we're done, so suppose $p \nmid a_1$
Then $\gcd(p, a_1) = 1$
By the previous lemma, $p|a_2$

Induction Step:
Assume the statement is true for $1 \leq k < n$ (i.e. that $p|a_1a_2 \dots a_n \Rightarrow p|some\ a_i$)
If $p|a_1a_2 \dots a_n$ then $p|a_1a_2 \dots (a_{n-1}a_n)$ so either $p|a_i$ for some $1 \leq i \leq n\text{-}2$, or else $p|a_{n-1}a_n$. In the last case, $p|a_{n-1}$ or $p|a_n$.
By induction, the lemma holds ■

We've shown that every $n \geq 2$ can be written as
$n = p_1p_2 \dots p_r$ for some primes $p_1 \dots p_r$ (maybe some repeats)

We will now prove that this representation is unique.

Proof of Unique Factorization of Integers

Base case:
For n = 2, this is clear. Since 2 is the only prime ≤ 2, and $2 \times 2 \geq 2$.
$n = 1$ is also unique since 1 is the product of no primes.

Induction:
Suppose that the prime factorization of k is unique for $1 \leq k < n$, $(n \geq 3)$

Write
$n = p_1 \dots p_r = q_1 \dots q_s$
In particular, $p_1|q_1 \dots q_s$
By the previous lemma, $p_1|q_i$ for some I
So $p_1 = q_i$ since q_i is prime.
Assume changing the order if necessary, that $q_i = q_1$

Now,
$p_2 p_3 \dots p_r = q_2 \dots q_s$, but this number is 1≤ num ≤ n, so it has a unique prime factorization.

Therefore $p_2, p_3, \dots p_r$ are the same as $q_2, q_3, \dots q_s$, up to order. ■

Application

Let n ≥ 1, n ∈ ℕ and suppose that $\sqrt[k]{n} \in \mathbb{Q}$. Then $n = a^k$ for some a ∈ ℤ

Proof
If $\sqrt[k]{n} = \frac{a}{b}$, a, b ∈ ℤ, gcd$(a, b) = 1$
Then $n \times b^k = a^k$, a, b, n ∈ ℤ
Suppose p|b. Then $p|a^k$, so $p|a$. But gcd(a, b) = 1 so this is impossible. So b = 1 (or -1)
Therefore, $n = \pm a^k$
■

Diophantine & Bezout

September-27-10 12:31 PM

Diophantine Equation

An equation with integer coefficients that one wants to solve over $\mathbb{Z}$.
e.g. $2x + 3y = 7$
$x^5 + y^5 = z^5$

$ax + by = c$ can be solved in $\mathbb{Z}$ if and only if $\gcd(a, b) \mid c$

Bezout's Identity

$ax + by = gcd(a, b)$

For a, b, c $\in \mathbb{Z}$ (non-zero)
$ax + by = c$ can be solved in $\mathbb{Z}$ if and only if $\gcd(a, b) \mid c$

If $c = m \times \gcd(a, b)$, and $ax + by = \gcd(a, b)$
Then $a(mx) + b(my) = m \times \gcd(a, b)$
On the other hand, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, so if $ax + by = c$, then $\gcd(a, b) \mid c$

Observation

$ax + by = c$ has a solution iff $\gcd(a, b) \mid c$, and then if x_0, y_0 is one solution, all other solutions are of the form:

$$x = x_0 + k \times \frac{\text{b}}{\gcd(\text{a}, \text{b})}$$

$$y = y_0 - k \times \frac{a}{\gcd(a, b)}$$

k $\in \mathbb{Z}$

$$ax + by = ax_0 + k \times \frac{ab}{\gcd(a, b)} + by_0 - k \times \frac{ab}{\gcd(a, b)}$$

$$= ax_0 + by_0 = c$$

Congruences (modulus)

September-27-10 12:42 PM

Congruence

Let a, b ∈ ℤ and n ∈ ℕ.
We say that a and b are congruent modulo n iff
$n|(a-b)$
Write
$a \equiv b\ (mod\ n)$

Proposition

If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and n ∈ ℕ, with $a_1 \equiv a_2$ (mod n) and $b_1 \equiv b_2$ (mod n) then:

1. $a_1 + b_1 \equiv a_2 + b_2$ (mod n)
2. $a_1 b_1 \equiv a_2 b_2$ (mod n)

Proof of (1)
If $a_1 \equiv b_2$ (mod n) and $b_1 \equiv b_2$ (mod n), then $a_1 - a_2 = cn$, say, and $b_1 - b_2 = dn$, say.
$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$
$= cn + dn = n(c + d)$

Congruence/Residue Class

The "congruence class" or "residue class" of a ∈ ℤ modulo n is the set:
[a] = {b ∈ ℤ : $a \equiv b$ (mod n)}
For a fixed n

A Ring Z_n

The ring $\mathbb{Z}_n$Is the set {[0], [1], ..., [n-1]} with the operations "+" and "·" defined by [a]+[b] = [c] iff $a + b \equiv c$ (mod n)
and [a]·[b] = [c] iff $ab \equiv c$ (mod n). The zero element will be [0] and the one element is [1].

Congruence

We say the ring $\mathbb{Z}_2$ (aka F_2) is defined by

+	**0**	**1**
0	0	1
1	1	0

×	**0**	**1**
0	0	0
1	0	1

Arithmetic in $\mathbb{Z}_2$ is arithmetic up to multiples of 2
So $a_1 + b_1 \equiv a_2 + b_2$ (mod 2)

Example:
$a \equiv b$ (mod 2) iff both are even or both are odd.
$x \equiv 7$ (mod 10) iff the 'ones" digit of x is 7 for x > 0
$a \equiv 0$ (mod n) iff $n|a$

Fix n ∈ ℕ
The "congruence class" of a ∈ ℤ modulo n is the set:
[a] = {b ∈ ℤ : $a \equiv b$ (mod n)}

There are n base congruence classes: [0], [1], [2], ... [n-1]

[1] = [n+1] since
$n \mid (b-1)$ iff $n \mid (b-n-1)$
To check that the operation [a] + [b] is well defined, what do we need to check?

Need to check that if $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then $a_1 + b_1 \equiv a_2 + b_2$ (mod n)
$[a_1] = [a_2]$ iff $a_1 \equiv a_2$ (mod n), so the above follows from this fact.

If $[a_1] = [a_2]$ and $[b_1] = [b_2]$ then $[a_1 + b_1] = [a_2 + b_2]$
In other works,
$[a] + [b] = [a + b]$
$[a] \cdot [b] = [ab]$

Example (mod 5)
[2] + [2] = [2 + 2] = [4]
[3] + [3] = [3 + 3] = [6] = [1]
[2] + [3] = [5] = [0]
[2][3] = [6] = [1]

*Groups

September-27-10 4:34 PM

Group

A group G is a set with a binary operation * (G is closed under this) with the following properties:

1. Associativity
   $a * (b * c) = (a * b) * c$
2. Identity
   There exists an e ∈ G such that for all a ∈ G,
   $a * e = e * a = a$
3. For all a ∈ G there is an a^{-1} ∈ G such that
   $a * a^{-1} = e$

Commutative/"Abelian"

A group (G, *, e) is commutative (or Abelian) if for all a, b ∈ G
$a * b = b * a$

Permutation

A permutation of a set is a function from the set to itself which is:

1. Injective (one-to-one)
2. Surjective (onto)

In other words, a permutation of {1, 2, …, N} is a function
f: {1, 2, …, N} -> {1, 2, …, N}
which is invertible.

Injective

$x = y \Leftrightarrow f(x) = f(y)$

Surjective

For every y, there is an x with f(x) = y

Injective and Surjective imply each other on a finite set

Examples
$(G, *, e) = (\mathbb{Z}, +, 0)$
$(g, *, e) = (\mathbb{R}^*, \times, 1)$
$\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}$

If R is a ring, (R, +, 0) is a group.

Another example:
$S_N = \{permutations\ of\ \{1, 2, 3, \dots, N\}\}$

The ring $\mathbb{Z}_N$

September-29-10 12:32 PM

[a] ∈ $\mathbb{Z}_N$ is a unit (has a multiplicative invers) iff gcd(a, N) = 1

Least Non-Negative Residue

The least non negative residue of $x\ (mod\ n)$ is a such that $[x] = [a]$ and $0 \leq a \leq n$

The ring $\mathbb{Z}_N$, N ≥ 1 ∈ ℤ
[a] = {b ∈ ℤ : b ≡ a (mod n)}

$\mathbb{Z}_N$ is the set of congruence classes [0], [1], … [n-1] with the operations [a] + [b] = [a + b] and [a][b] = [ab]

To know that $\mathbb{Z}_N$ is a commutative right, we need to know that:
1. [a] + [b] = [b] + [a]
2. [a] + ([b] + [c]) = ([a] + [b]) + [c]
3. … and many others

All of these qualities follow from the integers
ex. [a] + [b] = [a+b] = [b+a] = [b] + [a]
ex. [a] + ([b] + [c]) = [a] + [b+c] = [a + (b+c)] = ([a] + [b]) + [c]
Etc.

So $\mathbb{Z}_N$, with this "+" and "·" really is a commutative ring.
"0" = [0]
"1" = [1]

[a] = [b] ⇔ a ≡ b (mod N)

Addition and multiplication for $\mathbb{Z}_3$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

*	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Can we divide in $\mathbb{Z}_N$? Is $\mathbb{Z}_N$ a field? Maybe this depends on N

Multiplication for $\mathbb{Z}_4$

*	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

When can we solve
[a][x] = [1] in $\mathbb{Z}_N$? (for [x])

Claim: Iff gcd(a, N) = 1
⇒ When can we solve ax ≡ 1 (mod N)

We can solve ax ≡ 1 (mod N) iff there is an integer m with
$ax = 1 + mN$ if there exists x, y ∈ ℤ with
$ax + Ny = 1$, which can be solved iff gcd(x, N)=1

Proposition:
[a] ∈ $\mathbb{Z}_N$ is a unit (has a multiplicative invers) iff gcd(a, N) = 1

Ex. Find the multiplicative inverse of [26] in the ring $\mathbb{Z}_{137}$
Also: solve
26x ≡ 1 (mod 137)

Need to solve $26x + 137y = 1$
$137 = 5 \times 26 + 7$
$26 = 3 \times 7 + 5$
$7 = 1 \times 5 + 2$
$5 = 2 \times 2 + 1$
$2 = 2 \times 1 + 0$

$1 = 1 \times 5 + (-2) \times 2$
$= 1 \times 5 + (-2)(1 \times 7 + (-1) \times 5)$
$= (-2) \times 7 + 3 \times 5$
…
$= 58 \times 26 + (-11) \times 137$

$26 \times 58 \equiv 1$ (mod 137)
Therefore, [58] is the multiplicative inverse of [26] in the right $\mathbb{Z}_{137}$.
[26] [58] = [1]

It follows that $\mathbb{Z}_N$ is a field iff N is prime (or maybe N = 1)

Proof:
If N is prime, gcd(a, N) = 1 unless N|a

⇒ [a] is a unit unless [a] = [0]
If there is some $1 \leq a \leq N-1$ such that [a] is not a unit, then $\gcd(a, N) \neq 1$, but $1 < \gcd(a, N) \leq a < N$
gcd(a, N) divides N so N is not prime *proved same direction as above*

If N is not prime, then N is note a field:
If N is not prime, write $N = ab$, $1 < a, b < N$
In $\mathbb{Z}_N$, [a][b] = [0]
If [a] has a multiplicative inverse, [a][x] = [1], then
[x][a][b] = [x][0] ⇒ [b] = [0]
This means N|b, which is impossible so [a] has no multiplicative inverse.

Example:
Solve $123x \equiv 6 \pmod{321}$
Trying to solve $123x + 321y = 6$
$\Rightarrow 41x + 107y = 2$
Can solve iff gcd(41, 107)|2
41*47 - 18*107 = 1
41*94 +(-36)*107 = 2
123 * 94 + (-36)*321 = 6
⇒ [123][94] = 6

Equivalence

October-01-10 12:30 PM

Relation

A relation on a set is a set of pairs (a, b) which are "related".

Equivalence Relation

A relation $\approx$ on a set S is an equivalence relation if and only if:

1. $a \approx a$ for all a ∈ S
2. $a \approx b$ iff $b \approx a$ for all a, b ∈ S
   Symmetric
3. If $a \approx b$ and $b \approx c$ then $a \approx c$, for all a, b, c ∈ S
   Transitivity

Equivalence Classes

Given an equivalence relation $\approx$ on a set S, and a ∈ S define
$[a]_{\approx} = \{b \approx a : b \in S\}$

Chinese Remainder Theorem v.1

If $\gcd(M, N) = 1$ and a, b ∈ $\mathbb{Z}$ then we can solve
$x \equiv a \pmod N$
$x \equiv b \pmod M$
$x \in \mathbb{Z}$

Examples of Equivalence Relations

On any set S, the relations x = y is an equivalence relation.

For any N ≥ 1, a ≡ b (mod N) is an equivalence relation
Check:

1. $a \equiv a \pmod N \Leftrightarrow N|(a-a) = 0$, which is true
2. $a \equiv b \pmod N$ iff $b \equiv a \pmod N \Leftrightarrow$ N|(b-a) iff N|(a-b), which is true
3. If $a \equiv b \pmod N$ and $b \equiv c \pmod N$ then N|(b-a) and N|(c-b) so N|(c-a)
   $\Rightarrow a \equiv c \pmod N$

For real numbers x, y write $x \approx y$ if x, y have the same sign (+, -, 0)

Equivalence Classes

$a \approx b$ if and only if $[a]_{\approx} = [b]_{\approx}$

If $[a]_{\approx} = [b]_{\approx}$, then $b \in [a]_{\approx}$ (because $b \in [b]_{\approx}$ by (1)) $\Rightarrow a \approx b$

If $a \approx b$, then $b \in [a]_{\approx}$
If $c \in [b]_{\approx}$, a ≈ b, b ≈ c, so a ≈ c, so $c \in [a]_{\approx}$
So $[b]_{\approx} \subseteq [a]_{\approx}$. Also, $[a]_{\approx} \subseteq [b]_{\approx}$.
Therefore $[a]_{\approx} = [b]_{\approx}$ ■

For the equivalence relation $x \approx y$ if x, y have the same sign, on $\mathbb{R}$
-<----------0---------->
$[-1]_{\approx}$ $[0]_{\approx} = \{0\}$ $[1]_{\approx}$

Question:

Given a ∈ $\mathbb{Z}$ and M, N, ∈ $\mathbb{N}$ if we know the congruence class of a modulo N, do we know anything about the congruence class of a modulo M?
i.e. When can $x \equiv a \pmod N$ and $x \equiv b \pmod M$ be solved?
$x \equiv 1 \pmod 4$
$x \equiv 3 \pmod 4$ is clearly unsolvable

What about
$x \equiv 1 \pmod 4$
$x \equiv 2 \pmod 5$
$x = 17$ is a solution
$17 + 20k$ is also a solution for any k ∈ $\mathbb{Z}$

Chinese Remainder Theorem v.1

If $\gcd(M, N) = 1$ and a, b ∈ $\mathbb{Z}$ then we can solve
$x \equiv a \pmod N$
$x \equiv b \pmod M$
$x \in \mathbb{Z}$

Given one solution x_0, the full set of solutions is just the congruence class of x_0 modulo MN.

Chinese Remainder Theorem

October-04-10 12:30 PM

Chinese Remainder Theorem v.1

If gcd$(N, M) = 1$ and a, b ∈ ℤ, then there is a solution x ∈ ℤ to
$x \equiv a$ (mod N)
$x \equiv b$ (mod M)
If x_0 is one solution, then x is a solution iff $x \equiv x_0$ (mod MN)

Need gcd$(N, M) \mid b - a$

Chinese Remainder Theorem v.2

Let $M_1, M_2, \dots, M_k$ be rational number with gcd$(M_i, M_j) = 1$
For all i ≠ j
Let $a_1, a_2, \dots, a_k \in \mathbb{Z}$. Then there is a solution x ∈ ℤ to
$x \equiv a_1 \ (mod\ M_1)$
$x \equiv a_2 \ (mod\ M_2)$
…
$x \equiv a_k (mod\ M_3)$
If x_0 is one solution, then x is another iff $x \equiv x_0 (mod\ M_1 M_2 \dots M_k)$

Proof of Chinese Remainder Theorem

Want to solve
$x = a + Ny$
$x = b + Mz$
x, y, z ∈ ℤ
Want
$a + Ny = b + Mz$
$Ny + (-z)M = (b - a)$
Can solve iff gcd$(N, M) \mid b - a$
(Prove uniqueness as homework)

Example: Solve

$x \equiv 7$ (mod 17)
$x \equiv 9$ (mod 23)
Want to solve
17y +23w = 2
$23 = 1 \times 17 + 6$
$17 = 2 \times +5$
$6 = 1 \times 5 + 1$

$(-4) \times 17 + 3 \times 23 = 1$
$(-8) \times 17 + 6 \times 23 = 2$
$y = -8$
$z = -w = -6$
$x = a + Ny = 7 + 17 \times -8 = -129$

Solution $x \equiv -129$ (mod 391)
$\equiv 262$ (mod 291)

Proof to Chinese Remainder Theorem v.2 by induction on k

(Repeated application of v.1 on groups of two)

Question:

How many solutions are there to $x^2 \equiv 1 \ (mod\ N)$?
If N = p ≥ 3 is prime?
$x^2 \equiv 1 \ (mod\ p)$ iff $x^2 - 1 \equiv 0$ (mod p)
$\Rightarrow (x + 1)(x - 1) \equiv 0 \ (mod\ p)$
Iff $p \mid (x + 1)(x - 1)$
Iff $p \mid (x + 1)$ or $p \mid (x - 1)$
$x \equiv \pm 1 \ (mod\ p)$

Now, consider $N = p^e$ p≥ 3, prime, e ≥ 1
x ∈ ℤ satisfies
$x^2 \equiv 1$ (mod p), iff $p^e \mid (x + 1)(x - 1)$
By unique factorization, write
$x + 1 = p^a \times (something\ not\ divisble\ by\ p)$
$x - 1 = p^b \times (something\ not\ divisible\ by\ p)$
a, b ≥ e
If a ≠ 0 and b ≠ 0, then p|(x+1) and p|(x-1), so
p|(x+1)-(x-1) = 2
Impossible because p > 2, so min(a, b) = 0
So b ≥ e or a ≥ e so $p^e \mid (x - 1)$ or $p^e \mid (x + 1)$
And so $x \equiv \pm 1 \ (mod\ p^e)$

So For p odd (prime), e ≥ 1, $x^2 \equiv 1 \ (mod\ p^e)$ iff $x = \pm 1 \ (mod\ p^e)$

For e ≥ 1, how many solutions to
$x^2 \equiv 1 \ (mod\ 2^e)$
$e = 1 \Rightarrow x \equiv 1 \ (mod\ 2)$
$e = 2 \Rightarrow x \equiv \pm 1 \ (mod\ 4)$
$e \geq 3$:
Suppose $x^2 \equiv 1 \ (mod\ 2^e)$
$x + 1 = 2^a \times (something\ odd)$
$x - 1 = 2^b \times (something\ odd)$
a, b ≥ 0
$a + b \geq e$

$2^{\min(a,b)} \mid (x + 1)$
$2^{\min(a,b)} \mid (x - 1)$
So $2^{\min(a,b)} \mid (x + 1) + (x - 1) = 2$
So $\min(a, b) \leq 1$

Case 1: $a = 0$ *or* $b = 0$
$x \equiv 1\ (mod\ 2^e)$ *or* $x \equiv -1 (mod\ 2^e)$

Case 2: a = 1, then b ≥ e-1
So $2^{e-1} | (x - 1)$
$x = 1 + 2^{e-1} \times k$
If k is even, then $x \equiv 1 (mod\ 2)$
If k is odd, say k = 2m + 1
Then
$x = 1 + 2^{e-1} \times (1 + 2m)$
$= 1 + e^{e-1} + 2^e m$
$\equiv 1 + 2^{e-1} (mod\ 2^e)$

Case 3: b = 1 and a ≥ e-1
Then $x \equiv -1\ (mod\ 2^e)$
Or $x \equiv -1 + 2^{e-1} (mod\ 2^e)$

The number of solutions to $x^2 \equiv 1\ (mod\ 2^e)$ is
1 if e = 1
2 if e = 2
4 if e ≥ 3

*Groups and Functions

October-04-10 4:32 PM

Group

A group is a set G with an operation * and an element e such that

1. $a * (b * c) = (a * b) * c$
2. $a * e = e * a = a$
3. For all a there is an $a^{-1} \in G$ with $a * a^{-1} = e$

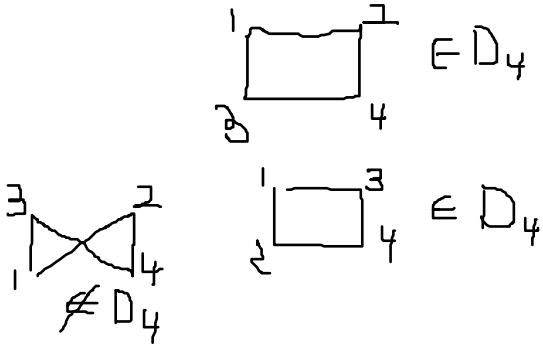
(When a set has an operation, it is closed under that operation)

Commutative

G is commutative iff $a * b = b * a$ for all a, b ∈ G

Subgroup

Let G be a group. A subgroup of G is a subset H ⊆ G containing e and closed under * and inverse.



Let S_N be the set of permutations of $\{1, 2, \dots, N\}$
Functions f:{1, ..., N} -> {1, ..., N} which are invertible
This is a group under "∘"
Given f and f, g ∈ S_N define f ∘g

If f and g are invertible, then f∘g and $(f \circ g)^{-1} = f^{-1} \circ g^{-1}$

1. f∘(g∘h) = (f∘g)∘h
   f(g∘h(x)) = f(g(h(x)))
   f∘g(h(x)) = f(g(h(x)))
2. Identity element e(x) = x
   f∘e(x) = f(e(x)) = f(x)
3. Inverses
   $f \circ f^{-1}(x) = x$
   $f(f^{-1}(x)) = e$

Denote functions by pseudo matrices
$\begin{pmatrix} 1 & 2 & 3 & \dots & N \\ f(1) & f(2) & f(3) & \dots & f(N) \end{pmatrix} \in S_N$

Examples:

In S_3
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

In S_4
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$

In S_3
$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
$b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
$ab = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
$ba = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
So S_3 is not commutative

S_2, however, is commutative
$S_2 = \left\{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\}$

In fact, S_N is not commutative for N ≥ 3

Example of Subgroup

If G = ℤ (with + as the operation) then for any n ∈ ℕ, H_n = {a ∈ ℤ : n|a} is a subgroup of ℤ

Show it is a group:

1. n|0 so 0 ∈ H_n
2. If a, b ∈ H_n then n|a and n|b so n|(a+b) ⇒ (a+b) ∈ H_n
3. n|(-a), so -a ∈ H_n

Exercise: Every subgroup of ℤ is of the form H_n for some n ∈ ℕ or {0} (= H_0)

Another example

Mark the corners of a square with 1, 2, 3, 4
Let D_4 be the subset of S_4 consisting of permutations which preserve the square.
Then $D_4 \subseteq S_4$ is a subgroup

Show that D_4 is a subgroup of S_4 and find how many elements there are in D_4

$x^2 \equiv 1\ (mod\ N)$

October-06-10 12:30 PM

Lemma

If p is prime, e ≥ 1, then $x^2 \equiv 1\ (mod\ p^e)$ has exactly 2 solutions $(mod\ p^e)$, unless
$p = 2\ and\ e = 1 \Rightarrow$ 1 solution
$p = 2\ and\ e \geq 3 \Rightarrow$ 4 solutions

How many solutions are there to $x^2 \equiv 1\ (mod\ N)$?

Theorem

Let $N = 2^e p_1^{d_1} p_2^{d_2} \dots p_k^{(d_k)}, d_k \geq 1$
With p distinct odd primes. Then the number of solutions to $x^2 \equiv 1\ (mod\ N)$ is exactly:

- 2^k if $e = 0, 1$
- 2^{k+1} if e = 2
- 2^{k+2} if e ≥ 3

Proof:
Suppose that N is odd so that e = 0
Then $x^2 \equiv 1\ (mod\ N)$ iff

$x^2 \equiv 1\ (mod\ p_1^{d_1})$
$x^2 \equiv 1\ (mod\ p_2^{d_2})$
…
$x^2 \equiv 1\ (mod\ p_k^{d_k})$

If $m_i = p_i^{d_i}$, then $\gcd(m_i, m_j) = 1$ for i, j ≤ k so by CRT
$y \equiv 1\ (mod\ m_1)$
$y \equiv 1\ (mod\ m_2)$
…
$y \equiv 1\ (mod\ m_k)$
$\Rightarrow y \equiv 1\ (mod\ m_1 m_2 m_3 \dots m_k)$

$x^2 \equiv 1\ (mod\ p_1^{d_1}) \Leftrightarrow x \equiv \pm 1\ (mod\ p_1^{d_1})$
$x^2 \equiv 1\ (mod\ p_1^{d_1}) \Leftrightarrow x \equiv \pm 1\ (mod\ p_2^{d_2})$
…
$x^2 \equiv 1\ (mod\ p_1^{d_1}) \Leftrightarrow x \equiv \pm 1\ (mod\ p_k^{d_k})$

Each choice of + or - in each congruence defines a unique congruence class modulo N
There are 2^k choices of + or - for each congruence so there are 2^k congruence classes mod N corresponding to:

$x^2 \equiv 1\ (mod\ p_1^{d_1})$
$x^2 \equiv 1\ (mod\ p_2^{d_2})$
…
$x^2 \equiv 1\ (mod\ p_k^{d_k})$

So there are 2^k solutions to the congruence $x^2 \equiv 1\ (mod\ N)$ if N is odd

Aside

Example:
$x^2 \equiv 1\ (mod\ 15)$
Same as solving $x^2 \equiv 1 (mod\ 3)\ and\ x^2 \equiv 1\ (mod\ 5)$
Same as solving the four systems of congruencies

$x \equiv 1 (mod\ 3)$	$x \equiv 1 (mod\ 3)$	$x \equiv 2 (mod\ 3)$	$x \equiv 2 (mod\ 3)$
$x \equiv 1 (mod\ 5)$	$x \equiv 4 (mod\ 5)$	$x \equiv 1 (mod\ 5)$	$x \equiv 4 (mod\ 5)$
$\boldsymbol{x \equiv 1 (mod\ 15)}$	$\boldsymbol{x \equiv 4 (mod\ 15)}$	$\boldsymbol{x \equiv 11 (mod\ 15)}$	$\boldsymbol{x \equiv 14 (mod\ 15)}$

Proof Cont.

If N is even, write $N = 2^e \times N'$ for N' odd
We have

$$x^2 \equiv 1\ (mod\ N) \Leftrightarrow \begin{cases} x^2 \equiv 1\ (mod\ 2^e) \\ x^2 \equiv 1\ (mod\ N') \end{cases}$$

There are 2^k distinct values $0 \leq a_1, a_2, a_3, \dots a_k < N'$ such that $x^2 \equiv 1\ (mod\ N')$

$x^2 \equiv 1\ (mod\ 2^e) \Leftrightarrow x \equiv 1\ (mod\ 2^e)$ for e = 1
$x^2 \equiv 1\ (mod\ 2^e) \Leftrightarrow x \equiv \pm 1\ (mod\ 2^e)$ for e = 2
$x^2 \equiv 1\ (mod\ 2^e)$ iff $x \equiv \pm 1\ or \pm 1 + 2^{e-1} (mod\ 2^e)$ for e ≥ 3
By CRT, there are $2^k, 2 \times 2^k, 4 \times 2^k$ congruence classes mod $2^e N$ corresponding to:

$x \equiv a_i (mod\ N')$ for some i and
$x \equiv \pm 1, (\pm 1 + 2^{e-1}, if\ e \geq 3) (mod\ 2^e)$

Therefore, there are exactly $2^k, 2^{k+1}, or\ 2^{k+2}$ congruence classes mod N whose square is 1, depending on if $e = 0, 1$ e $= 2$, or e $= 3$

Fermat's Little Theorem

October-06-10 1:07 PM

Midterm, everything up to and including this lecture

Fermat's Little Theorem

Let p be a prime and a ∈ ℤ with gcd(a, p) = 1
Then $a^{p-1} \equiv 1(mod\ p)$

FLT, alternate form

If p∤a and $e_1 \equiv e_2\ (mod\ p-1)$ then $a^{e_1} \equiv a^{e_2}\ (mod\ p)$

In ℤ, the values $a, a^2, a^3, a^4, \ldots$ are all different (if a ≠ 0, ± 1)

In $\mathbb{Z}_N$, this is not true. If [a] ∈ $\mathbb{Z}_N$ $[a], [a]^2, [a]^3, \ldots, [a]^m$ cannot all be different because there are finitely many congruence classes.

When do you get the first repetition?

What happens with addition?
There is some smallest m≥1 such that [ma] = 0 (eg, if N is prime and [a] ≠ 0 then m = N)
$m = N/GCD(a, N)$ Repeats at (m+1)

Is there a smallest k positive such that $[a]^k = [1]$ in $\mathbb{Z}_N$? If so, what is it?

Fermat's Little Theorem

Let p be a prime and a ∈ ℤ with gcd(a, p) = 1
Then $a^{p-1} \equiv 1(mod\ p)$

Ex. If a is 2 and p = 7, then $2^6 \equiv 1\ (mod\ 7)$

Proof of Fermat's Litter Theorem

Define a function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$
By $f([x]) = [ax] = [a][x]$

Claim: f is a one-to-one (ie. $f([x_1]) = f([x_2])\ iff\ [x_1] = [x_2]$) and onto (ie. Fore every $[y] \in \mathbb{Z}_p$ there is an $[x] \in \mathbb{Z}_p$ with $f([x]) = [y]$)

Proof that f is onto and one-to-one
If $[y] \in \mathbb{Z}_p$, then $f([a]^{-1}[y]) = [y]$
So everything is in the image of f ⇒ onto.
$\mathbb{Z}_p$ is finite so f also has to be one-to-one

Therefore f just permutes the residue classes.

Since $f([0]) = [0]$,
$$[1] \times [2] \times \cdots \times [p-1] = f([1]) \times f([2]) \times \cdots \times f([p-1])$$
$$= [a \times 1][a \times 2] \ldots [a \times (p-1)]$$
$$= [a][1][a][2] \ldots [a][p-1]$$
$$= [a]^{p-1}[1][2] \ldots [p-1]$$
In other words,
$[(p-1)!] - [a^{p-1}][(p-1)!]$
$[(p-1)!] \neq 0$, since p∤1, p∤2, … p∤(p-1)
So $[(p-1)!]$ has a multiplicative inverse
Multiplying both sides by this inverse gives:
$[1] = [a^{p-1}]$ or, equivalently $a^{p-1} \equiv 1\ (mod\ p)$

Fermat's Little Theorem:

If p∤a, $a^{p-1} \equiv 1\ (mod\ p)$
If p∤a and $e_1 \equiv e_2\ (mod\ p-1)$ then $a^{e_1} \equiv a^{e_2}\ (mod\ p)$
Because if $e_1 = e_2 + k(p-1)$
So $a^{e_1} = a^{e_2+k(p-1)} = a^{e_2} \times (a^{p-1})^k \equiv a^{e_2} \times 1^k\ (mod\ k)$
$$\equiv a^{e_2}(mod\ k)$$

Example

Find some 0 ≤ x < 11 (least non-negative residue) such that
$7^{291373} \equiv x\ (mod\ 11)$

By FLT, we only need to know what the exponent is mod 11-1 = 10
So $7^{291373} \equiv 7^3(mod\ 11)$
$$\equiv 49 \times 7\ (mod\ 11)$$
$$\equiv 5 \times 7\ (mod\ 11)$$
$$\equiv 2\ (\text{mod}\ 11)$$

Euler's Theorem

October-08-10 1:00 PM

Euler's Totient Function

For m ≥ 1, $\varphi(m) = \#\ of\ values\ 0 \le k < m\ s.t.\ \gcd(k,m) = 1$
$= the\ number\ of\ units\ in\ the\ ring\ \mathbb{Z}_n$

Euler's Theorem

Let n ≥ 1 and a are integers gcd(a, n) = 1. Then
$a^{\phi(n)} \equiv 1\ (mod\ n)$

Theorem

Suppose gcd(n, m) = 1. Then $\varphi(nm) = \varphi(n)\varphi(m)$

If p is prime, e ≥ 1, then
$\varphi(p^e) = p^{e-1}(p-1)$

Euler's Totient Function

For m ≥ 1, $\varphi(m) = \#\ of\ values\ 0 \le k < m\ such\ that\ \gcd(k,m) = 1$
$= the\ number\ of\ units\ in\ the\ ring\ \mathbb{Z}_n$

Euler's Theorem

Let n ≥ 1 and a are integers gcd(a, n) = 1. Then
$a^{\varphi(n)} \equiv 1\ (mod\ n)$

Example:
What is the last (one's) digit of 7^{291373}?
We want the least non-negative residue of this mod 10

Need to know the least non-negative residue of the 291373 mod (φ(10)) and we've check that gcd(7, 10) = 1

0	1	2	3	4	5	6	7	8	9
No	Yes	No	Yes	No	No	No	Yes	No	Yes

So $\varphi(10) = 1$
$291373 \equiv 1\ (mod\ 4)$

By Euler's Theorem:
$7^{291373} \equiv 7^1\ (mod\ 10)$

Example

Find the least non-negative residue of
$2^{17^{19}}\ (mod\ 13)$
Need to find the least non-negative residue of $17^{19}(mod\ 12)$
Need to fine the least non-negative residue of 19 $(mod\ \varphi(12))$
$\varphi(12) = 4$
$19 \equiv 3\ (mod\ \varphi(12))$
$\Rightarrow 17^{19} \equiv 17^3 \equiv 5^3 \equiv 5\ (mod\ 12)$
$\Rightarrow 2^{17^{19}} \equiv 2^5 \equiv 32 \equiv 6\ (mod\ 13)$

Proof

Let U be the set of integers 0 ≤ u ≤ n-1 with gcd(u, n) = 1
By definition, $\varphi(n) = \#U$
Given a ∈ ℤ with gcd(a, n) = 1 define $f([x]) = [ax]$ for all [x] in $\mathbb{Z}_n$
If u ∈ U, then f([u]) is also a unit.

$U = \{0 \le u \le n-1\ such\ that\ [u] \in \mathbb{Z}_n\ is\ a\ unit\}$
If u ∈ U then [u] is a unit but so is [au] because $[au] = [a]^{-1}[u]^{-1}$
[u] by definition has an inverse, gcd(a, n) = 1 so [a] has an inverse

Also, we have that f is one-to-one because $f([u_1]) = f([u_2]) \Rightarrow [au_1] = [au_2]$
$\Rightarrow [a]^{-1}[a][u_1] = [a]^{-1}[a][u_2] \Rightarrow [u_1] = [u_2]$
So f sends each [u] with u ∈ U to some unique [v] = [au] with v ∈ U
Therefore f is a permutation of the residue classes [u] for u ∈ U

If $U = \{u_1, u_2, \dots, u_{\varphi(n)}\}$ then
$[u_1][u_2] \dots [u_{\varphi(n)}] = [au_1][au_2] \dots [au_{\varphi(n)}]$
$\Rightarrow ([u_1][u_2] \dots [u_{\varphi(n)}]) = [a]^{\varphi(n)}\ ([u_1][u_2] \dots [u_{\varphi(n)}])$
This gives $[1] = [a]^{\varphi(n)} = [a^{\varphi(n)}]$
$\therefore a^{\varphi(n)} = 1\ (mod\ n)$ ■

Computing ϕ(n)

To compute $\varphi(n)$ so far, we had to count (explicitly) things with gcd 1

Theorem

Suppose gcd(n, m) = 1. Then $\varphi(nm) = \varphi(n)\varphi(m)$
(Aside: φ is a multiplicative function)

Proof

Given that gcd(n, m) = 1, then for each 0 ≤ a < n and 0 ≤ b < m, there is a unique 0 ≤ c < nm such that
$x \equiv a\ (mod\ n)$
$x \equiv b\ (mod\ m)$
$x \equiv c\ (mod\ mn)$

Suppose that gcd(a, n) = gcd(b, m) = 1
And suppose that for the c constructed by the CRT, gcd(c, mn) ≠ 1
Then for some prime p, p|c and p|mn. Then p|m or p|n. suppose p|m.
But c ≡ b (mod m), say b = c + km, k ∈ ℤ but then p|c and p|m means p|b
But gcd(b, m) =1, contradiction. So the supposition that g(c, mn) ≠ 1 is false

So gcd(a, n) = gcd(b, m) = 1 ⇒ gcd(c, mn) =1

Suppose that gcd(c, mn) = 1
If p|a and p|n (if gcd(a, n) ≠ 1), then
$c \equiv a \ (mod\ n), say\ c = a + kn$ so p|c.
So p|c and p|mn, a contradiction so gcd(a, n) =1
Similarly, gcd(b, m) = 1 b y the same argument.
So gcd(c, mn) = 1 ⇒ gcd(a, n) = gcd(b, m) = 1

So gcd(a, n) = gcd(b, m) = 1 ⇔ gcd(c, mn) = 1

So every pair a, b with 0 ≤ a < n and 0 ≤ b < m defines a unique 0 ≤ c ≤ mn such that
$\left\{\begin{matrix} x \equiv a\ (mod\ n) \\ x \equiv b (mod\ m) \end{matrix}\right\} \Leftrightarrow x \equiv c\ (mod\ mn)$
And gcd(c, mn) = 1 iff gcd(a, n) = gcd(b, m) = 1
So the number of 0 ≤ c < mn with gcd(c, mn) = 1
Is equal to the number of pairs (a, b) with
0 ≤ a < n, gcd(a, n) = 1
0 ≤ b < m, gcd(b, m) = 1
$\varphi(mn) = \varphi(n)\varphi(m)$

This shows that if
$n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$, then
$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \dots \varphi(p_s^{e_s})$
(if the p_i are distinct)

$\varphi(p^e) =$
$of\ 0 \le k < p^e with \gcd(k, p^e) = 1$
$= p^e - \#\ of\ 0 \le s < p^e$ with $\gcd(s, p^e) \neq 1$
$= p^e - p^{e-1}$
Because $\gcd(s, p^e) \neq 1$iff p|s, which happens iff s = pr with $0 \le r < \frac{p^e}{p} = p^{e-1}$

Lemma
If p is prime, e ≥ 1, then
$\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

Example
$\varphi(1000) = ?$
$\varphi(1000) = \varphi(2^3 \times 5^3) = \varphi(2^3)\varphi(5^3) = 2^2(2-1)5^2(5-1) = 400$

Encryption

October-15-10 12:34 PM

Encoding

Translating data into numbers
(In general, one type of data into another type of data)

Ex. Text: Unicode, ASCII

Encrypting

Translating data into some form which is hard for other people to read.

Basic Problem:

Send a message from person A (Alice) to person B (Bob), in such a way that the message cannot be read by anyone else if intercepted.

One-time Pad

Shift each character by some amount given by the pad, and that is the encrypted message.
Unbreakable.
But how do Alice and Bob share the same pad? They need some common secret to start with.

Is there any easy way for Alice and Bob to generate a common secret over open communication?
Mathematically, no (barring quantum mechanics). But practically, yes.

Diffie-Hellman Key Exchange

Used to generate a common secret "key" or secret number.

Using successive squaring, Alice and Bob can generate a key very quickly. Eve takes a long time to figure out the key.

Algorithm

Alice and Bob choose a large prime p, and some $0 < g < p$, $g \in \mathbb{Z}$
Public: p and g

Choose g so that $g^k \not\equiv 1 \ (mod\ p)$ for $1 < k <$ p-1
In secret, Alice chooses an integer a and Bob an integer b.
Alice computes the least non-negative residue of $g^a (mod\ p)$ and sends this to Bob. Bob sends the least non-negative residue of $g^b (mod\ p)$
Public: $g^a (mod\ p)$, $g^b (mod\ p)$

Now, Alice computes $\left(g^b\right)^a = g^{ab}$
Bob computes $(g^a)^b = g^{ab}$
The least non-negative reside of g^{ab} (mod p) is the secret.

If Eve intercepts g, p, $g^a (mod\ p)$, *and* $g^b (mod\ p)$, then she needs to solve:

Discrete Log Problem

Given p, g (mod p), and $g^a (mod\ p)$, find a (mod p-1)

To solve this, compute g^k (mod p) for $0 \leq k \leq$ p -1

Examples

Suppose p is some large prime. Find a such that
$2^a = 97\ (mod\ 101)$

We hope (think) that the computations Alice and Bob need to do are a lot faster than the one Eve needs to do

Successive Squaring

Very fast way to compute $g^a (mod\ n)$

1. Write a as a sum of powers of 2 (in binary)
   $a = b_0 + 2b_1 + 4b_2 + \cdots + 2^k b_k$
2. Compute
   $g^2\ (mod\ p)$
   $(g^2)^2 = g^{2^2} (mod\ p)$
   ...
   $g^{2^k} (mod\ p)$
3. $g^a = g^{b_0 + 2b_1 + 4b_2 + \cdots + 2^k b_k} = g^{b_0} \times (g^2)^{b_1} \times \cdots \times \left(g^k\right)^{b_k}\ (mod\ p)$

Example

Compute $5^{10275}\ (mod\ 22447)$
$10275 = 2^{13} + 2^{11} + 2^5 + 2^1 + 2 + 0$
$5^{2^1} \equiv 25\ (mod\ 22447)$
$5^{2^2} \equiv 625\ (mod\ 22447)$
$5^{2^3} \equiv 9026\ (mod\ 22447)$
...
$5^{2^5} \equiv 12253\ (mod\ 22447)$
$5^{2^{11}} \equiv 18470\ (mod\ 22447)$
$5^{2^{13}} \equiv 10583\ (mod\ 22447)$

$5^{10275} \equiv 10583 \times 18470 \times 12253 \times 25 \times 5$
$\equiv 10009\ (mod\ 22447)$

Suppose you have a function (on a computer): multiply_mod_p(x, y) which takes a fixed amount of

time (depending on p)

Calculating $g^a (mod\ p)$ by repeated multiplication takes approximately a uses of this function.
$O(2^n)$ where n is the length of a in binary

For successive squaring, we need to square k times, where k is largest power of two less than (or equal to) a.
$2^k \leq a \Rightarrow k \leq \log_2 a$
To construct $g^a\ (mod\ p)$ from this we have to do at most k more multiplications.
# of calls of multiply_mod_p $\leq 2 \log_2 a$
O(n) where n is the length of a in binary

So Alice and Bob can generate the keys exponentially faster than Eve can break the key

Example
Assume that 1 multiplication takes $\approx 10^{-3} s$

a	Alice & Bob	Eve
1000	0.053s	1s
10^6	0.079s	17 min
10^8	0.106s	24 hours
10^{20}	0.2657s	3.17 billion years

Public Key Cryptography

October-20-10 12:32 PM

Diffie-Hellman Key Exchange

Reasonable for communication between two equal parties, Alice and Bob. But it requires both to do work so it is less reasonable for things like e-commerce. If there a central hub receiving lots of encrypted information, they have to spend time setting up a key with each partner.

Alice should be able to post a "public key" which people can use to send her encrypted messages. Cannot use the concept of a one time pad to be able to send/receive messages

RSA (Rivest-Shamir-Adelman)

Creating the Key

- Alice chooses two large primes p and q and computes m = pq, $\varphi(m) = (p-1)(q-1)$
- She then chooses $1 \leq e \leq \varphi(m)$ with $\gcd(e, \varphi(m)) = 1$
  Hopefully not e = 1 or e = $\varphi(m) - 1$
- Then compute d such that $ed \equiv 1 \ (mod\ \varphi(m))$
  (Using Bezout's and Euclidean Algorithm)

Public Key: m and e
Private Key: $\varphi(m)$ and d (forget p, q)

Encrypting the Message

If Bob wants to send a message a,
Bob's message needs to satisfy:

- $1 \leq a < m$
- $\gcd(a, m) = 1$, this is very likely since the only possibilities are 1, p, q

Bob computes $a^e (mod\ m)$ - can by done very quickly by successive squaring and sends that

Public: $a^e (mod\ m)$

Decrypting the Message

Alice gets $a^e (mod\ m)$
She computes $(a^e)^d \equiv a^{ed} \equiv a \ (mod\ m)$ by Euler's Theorem since $ed \equiv 1 \ (mod\ \varphi(m))$

Cracking

How can Eve, using m, e, and $a^e (mod\ m)$, find a (mod m)
Even needs to figure out d, so needs to solve $ex \equiv 1 \ (mod\ \varphi(m))$
She needs to know $\varphi(m)$. If you can factor m you can easily compute $\varphi(m)$

How do you factor m?
It is the product of two primes, so you just have to find a factor.

In fact, if m = pq, it turns out that computing $\varphi(m)$ is just as hard as factoring m.
Suppose we know m and $\varphi(m)$.
Then $pq = m \ and \ (p-1)(q-1) = \varphi(m)$
$(p-1)\left(\frac{m}{p} - 1\right) = \varphi(m)$
$(p-1)(m-p) = \varphi(m)p$
$(pm - p^2 - m + p) = \varphi(m)$
$p^2 + (\varphi(m) - m - 1)p + m = 0$
Can solve for p using the quadratic formula, so factoring m must be at least as fast as finding $\varphi(m)$

We suspect that it is hard (not polynomial time) to factor integers.

Chance that Bob's Message is relatively prime to m

$\frac{m}{p}$ possible a which are divisible by p and $\frac{m}{q}$ which are divisible by q so
$m - \frac{m}{p} - \frac{m}{q} = m(1 - \frac{1}{p} - \frac{1}{q})$ different messages are OK. The proportion of messages which will work is $\geq 1 - \frac{1}{p} - \frac{1}{q}$

Example of RSA

Alice chooses p = 31, q = 37 so m = 1147. $\varphi(m) = 30 \times 36 = 1080$
Public Key: m = 1147, e = 419
$d = 299$ because $299 \times 419 \equiv 1 \ (mod\ 1080)$

Bob want to send "917". $\gcd(1147, 917) = 1$
Bob computes $917^{419} \equiv 763 \ (mod\ 1147)$
Public Cyphertext: $763 \ (mod\ 1147)$

Alice gets this and computes
$763^{299} \equiv 917 \ (mod\ 1147)$

Creating the key and encrypting/decrypting use

1. Successive squaring
2. Euclidean Algorithm

Running Times

Successive squaring is fast (polynomial time). The time it takes is roughly proportional to the number of digits of the numbers involved (linear time)

The Euclidean algorithm is also polynomial time.

Breaking the key requires factoring, which is slow.

Factoring Numbers

October-22-10 12:55 PM

How do you factor numbers?

Pollard p-1 "Algorithm"

Not guaranteed to work but it is fast if it does work.

Idea:

Want to factor $m = pq$ (or anything else)

Pick $ka < m$. If gcd(a, m) $\neq 1$, we're done.

If $(p-1)|k$, then $a^k \equiv 1\ (mod\ p)$
So $p|(a^k - 1)$
If we compute $b \equiv a^k - 1\ (mod\ m)$
$p|\ \gcd(a^k - 1, m) = \gcd(b, m)$
Hopefully gcd(b, m) is not m, if it isn't then we have another multiple of p

In general, it's possible that $a^k \equiv 1\ (mod\ p)$ for some k smaller than p-1
We chose a "likely candidate" k,
compute $b \equiv a^k - 1\ (mod\ m)$ and $\gcd(a^k - 1, m) = \gcd(b, m)$

This is a divisor of m. If it is 1 or m, this tells us nothing. But maybe it isn't.

This works best if k has a lot of small prime factors. k is usually chosen so:
$k = lcm(2, 3, 4, 5, \dots, ?)$

Example

$m = 143$
$a = 2$
$k = lcm(2,3,4) = 12$
Calculate $b \equiv 2^{12} - 1\ (mod\ 143)$
$2^{12} \equiv 92\ (mod\ 143)\ so$
$b \equiv 91\ (mod\ 143)$
$\gcd(2^{12} - 1, 143) = \gcd(91, 143) = 13$

So $143 = 13 \times 11$

Example

$m = 391$
$a = 2$
$k = lcm(2, 3, 4) = 12$
$2^{12} - 1 \equiv 185\ (mod\ 391)$
$\gcd(2^{12} - 1, 185) = \gcd(185, 391) = 1$

Try again:
$k = lcm(2, 3, 4, 5, 6, 7) = 420$
$2^{420} - 1 \equiv 49\ (mod\ 391)$
$\gcd(49, 391) = 1$

And again:
$k = lcm(1, 2, 3, 4, 5, 6, 7, 8) = 840$
Don't need to recalculate everything. k = $2 \times k_{prev}$ in this case
$2^{840} = (2^{420})^2$
$2^{840} - 1 \equiv 153\ (mod\ 391)$
$\gcd(153, 391) = 17$
$m = 23 \times 17$

Multiplicative Functions

October-25-10 12:33 PM

Multiplicative Function

$f: \mathbb{N} \to \mathbb{R}$ is multiplicative if and only if
$\gcd(m,n) = 1 \Rightarrow f(mn) = f(m)f(n)$

Theorem

If g is a multiplicative function, then

$$f(n) = \sum_{d|n} g(d)$$

Is multiplicative.

Sigma

$$\sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}$$

Perfect Numbers

A number is perfect if it is the sum of all it's positive divisors other than itself.

Back to Euler φ function
Recall, if gcd(m, n) = 1 then $\varphi(m,n) = \varphi(m)\varphi(n)$

Obvious, Trivial Examples of Multiplicative Functions

$f(n) = 1 \; \forall$ n
$f(n) = n \; \forall n$

Less Trivial Examples

$f(n) = 2^{\#\ of\ distinct\ prime\ factors\ of\ n}$
$f(p^e) = 2$
$f(p_1^{e_1} \dots p_s^{e_s}) = 2^s$

Theorem

If g is a multiplicative function, then

$$f(n) = \sum_{d|n} g(d)$$

Is multiplicative.

Proof of Theorem

Lemma

Let $\gcd(m,n) = 1$, and d|mn. Then d can be written in one and only one way as d=ab with a|m and b|n.

Proof of Lemma

Let $a = gcd(d, \text{m})$ and $b = gcd(d,n)$. Then gcd(a, b) = 1 and a|d and b|d so ab|d.
On the other hand,
$d = \gcd(d, mn) \mid \gcd(d,n)\gcd(d,m) = ab$
So d|ab, thus d = ab leave uniqueness as an exercise.

Proof of Theorem

If $\gcd(m,n) = 1$ then

$$f(mn) = \sum_{d|mn} g(d) = \sum_{a|m}\sum_{b|n} g(ab) = \left(\sum_{a|m} g(a)\right)\left(\sum_{b|n} g(b)\right) = f(m)f(n)$$

Example

Let d(n) be # of divisors of n
$d(1) = 1$
$d(p^e) = e + 1$
So if $n = p_1^{e_1} \dots p_s^{e_s}$ then $d(n) = (e_1 + 1)(e_2 + 1) \dots (e_s + 1)$

Example:
$d(1000) = d(2^3 \times 5^3) = (3 + 1)(3 + 1) = 16$

Set

$$\sigma(n) = \sum_{d|n} d$$

So σ is multiplicative.
$\sigma(6) = 1 + 2 + 3 + 6 = 12$
$\sigma(4) = 1 + 2 + 4 = 7$
$\sigma(5) = 1 + 5 = 6$

If $n = p_1^{e_1} \dots p_s^{e_s}$, what is $\sigma(n)$?
Well,

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}$$

$$\sigma(n) = \left(\frac{p_1^{e_1+1} - 1}{p_1 - 1}\right) \dots \left(\frac{p_s^{e_s+1} - 1}{p_S - 1}\right)$$

Example

Let $n = 1521 = 3^2 \times 13^2$

$$\sigma(1521) = \left(\frac{3^3 - 1}{2}\right)\left(\frac{13^3 - 1}{12}\right) = 2379$$

Perfect Numbers

A number is perfect if it is the sum of all it's positive divisors other than itself.

$$\sigma(n) = \sum_{d|n} d = 2n$$

$\sigma(6) = 1 + 2 + 3 = 6$ so 6 is perfect
$\sigma(28) = \sigma(4 \times 7) = \sigma(4)\sigma(7) = 7 \times 8 = 56 = 2 \times 28$

*Complex Numbers

October-25-10 4:40 PM

The set of complex number is $\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$
Where i is a symbol have the property $i^2 = -1$

We define addition and multiplication on $\mathbb{C}$
$z = x + iy, w = u + iv \in \mathbb{C}$
$z + w = (x + u) + i(y + v)$
$z \times w = (x + iy)(u + iv) = (xu - yv) + i(xv + uy)$

Theorem

$\mathbb{C}$ is a field
If $z = x + iy \neq 0$, z has a multiplicative inverse

$$z^{-1} = \frac{1}{x + iy} = \frac{x - iy}{(x + iy)(x - iy)} = \frac{x}{x^2 + y^2} - \frac{iy}{x^2 + y^2}$$

Check Everything Else

Definition

If $z = x + iy \in \mathbb{C}$
$x + iy$ is the standard form of z
(x, y) are the Cartesian coordinates
$x = Re(z)$ is the real part of z
$y = Im(z)$ is the imaginary part of z

Complex Numbers

Geometric representation of $\mathbb{C}$
The function $f : \mathbb{C} \to \mathbb{R}$ is a bijection $x + iy \to (x, y)$
Check $(\mathbb{C}, +)$ corresponds to parallelogram law of addition of vectors

Exercise

Write the standard form of $(1 + i)^{-2}$

$$(1 + i)^{-2} = \frac{1}{(1 + i)^2} = \frac{1}{1 - 1 + 2i} = \frac{1}{2i} \times \frac{-i}{-i} = -\frac{i}{2} = 0 - \frac{1}{2}i$$

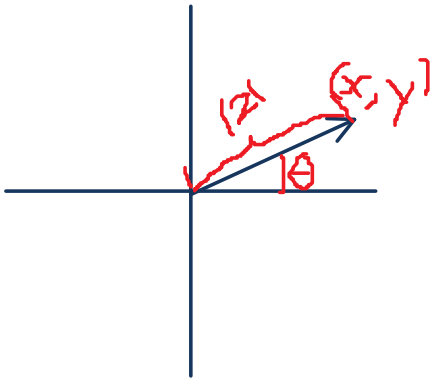
If $z = x + iy \in \mathbb{C}$

The complex conjugate of z *is* $\bar{z} = x - y$
The modulus (or absolute value) of z is $|z| = \sqrt{x^2 + y^2}$

Theorem (Properties of $\bar{z}$)

If $z = x + iy, w = u + iw \in \mathbb{C}$

1. $\overline{z + w} = \bar{z} + \bar{w}$
2. $\overline{zw} = \bar{z} \times \bar{w}$
3. $\bar{\bar{z}} = z$
4. $z\bar{z} = |z|^2$
5. $z + \bar{z} = 2x$
6. $z - \bar{z} = 2yi$
7. $z \neq 0, z^{-1} = \frac{\bar{z}}{|z|}$



Properties of |z|

1. $|z| = 0 \Leftrightarrow z = 0$
2. $|\bar{z}| = |z|$
3. |zw|=|z| |w|
4. $|z| \geq x, |z| \geq y$
5. Triangle inequality $|z + w| \leq |z| + |w|$
6. $|z - w|$ is the distance between z and w in $\mathbb{R}^2$

Polar Coordinates

$r = |z|$
Coordinate: (r, θ)

*Complex Numbers cont.

November-01-10 4:31 PM

Polar Coordinates

Let $z = x + iy \in \mathbb{C}$
Let $r = |z|, \theta = angle\ in\ radians\ away\ from\ the\ real\ axis$
$\theta = \tan^{-1}\frac{y}{x}$

(r, θ) - the polar coordinates for z
$r \in \mathbb{R}, r \geq 0$
$\theta \in \mathbb{R}, \theta$ is not unique
$0 = (0, \theta)$

Other notation:
$z = r(\cos\theta + i\sin\theta) = r\ cis\ \theta$

Converting from polar to standard form

From polar to standard form
$z = r\ cis\ \theta \Rightarrow z = r\cos\theta + i\,r\sin\theta$

From standard to polar form
$z = x + iy$
$r = \sqrt{x^2 + y^2} = |z|$
$\tan\theta = \frac{y}{x}, and\ same\ quadrant\ as\ (x, y)$

Examples

1. Write $z = 5\ cis\left(\frac{\pi}{4}\right)$ in standard form
$$z = 5\cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{5\sqrt{2}}{2} + i\frac{5\sqrt{2}}{2}$$
2. Write $z = -\sqrt{3} - i$ in polar form
$r = 2$
$\tan\theta = \frac{1}{\sqrt{3}}, \tan\frac{\pi}{6} = \frac{1}{\sqrt{3}}\ but\ wrong\ quadrant$
$\theta = \pi + \frac{\pi}{6}$
$z = 2\ cis\left(\frac{7\pi}{6}\right)$

Theorem

Let $z_1 = r_1\ cis\ (\theta_1), z_2 = r_2\ cis\ (\theta_2)$ be complex numbers
Then $z_1 z_2 = r_1 r_2\ cis\ (\theta_1 + \theta_2)$

$z_1 z_2 = (r_1\cos\theta_1 + ir_1\sin\theta_1)(r_2\cos\theta_2 + ir_2\sin\theta_2)$
$= r_1 r_2\cos\theta_1\cos\theta_2 - r_1 r_2\sin\theta_1\sin\theta_2 + 2(r_1 r_2\cos\theta_1\sin\theta_2 + r_1 r_2\sin\theta_1\cos\theta_2$
$= r_1 r_2\cos(\theta_1 + \theta_2) + 2r_1 r_2\sin(\theta_1 + \theta_2) = r_1 r_2\ cis\ (\theta_1 + \theta_2)$

Corollary (De Moivre's Theorem)

$(r\ cis\ \theta)^n = r^n\ cis\ (\theta n)\ n \in \mathbb{N}, r \in \mathbb{R} \geq 0, \theta \in \mathbb{R}$
Write $\left(1 - \sqrt{3}i\right)^6$ in standard form.
Convert to polar form $\left(1 - \sqrt{3}i\right)^6 = 2\ cis\left(-\frac{\pi}{3}\right)$
$\left[2\ cis\left(-\frac{\pi}{3}\right)\right]^6 = 2^6\ cis\left(-\frac{6\pi}{3}\right) = 2^6$

Theorem (Roots of Complex Numbers)

Let $z = r\ cis\ \theta, n \in \mathbb{N}$
Then the nth complex root of z $(w \in \mathbb{C} : w^n = z)$
are $r^{\frac{1}{n}}\ cis\ ($

Perfect Numbers

October-27-10 12:33 PM

Theorem

Let n be an even number. Then n is perfect if and only if $n = 2^{p-1}(2^p - 1)$ for some prime p such that $2^p - 1$ is also prime.

Mersenne Prime

A prime of the from $2^n - 1$ is called a Mersenne Prime
⇒ n is prime

Theorem

For any n,

$$\sum_{d|n} \varphi(d) = n$$

Is 2^e perfect?
$\sigma(2^e) = \frac{2^{e+1}-1}{2-1} = 2^{e+1} - 1 \neq 2^{e+1}$
What about other numbers?

Write n = $2^e m$ where m is odd
$\sigma(n) = \sigma(2^e)\sigma(m) = (2^{e+1} - 1)\sigma(m)$
If n is perfect the σ(n) = 2n = $2^{e+1}m$

So $(2^{e+1} - 1)\sigma(m) = 2^{e+1}m$
and thus
$2^{e+1}|\sigma(m)$ and $2^{e+1} - 1|m$

So there is a k such that $m = (2^{e+1} - 1)k$
So $\sigma(m) = 2^{e+1}k$
So $k|\sigma(m)$

m and k are both divisors of m and m+k = $(2^{e+1}-1)k + k = 2^{e+1}k = \sigma(m)$
So m has only two divisors, so m is prime.

So m has only two divisors and thus m is prime, which implies k =1. Since $m = 2^{e+1} - 1$ is prime, e+1 is prime.

Set p = e+1 (since primes should be called p)
Then e = p-1 so $n = 2^{p-1}(2^p - 1)$

Theorem

Let n be an even number. Then n is perfect if and only if $n = 2^{p-1}(2^p - 1)$ for some prime p such that $2^p - 1$ is also prime.

To see the other way
$\sigma\left(2^{p-1}(2^p - 1)\right) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)(2^p) = 2 \times 2^{p-1}(2^p - 1)$
$(2^p - 1)$ is prime so $\sigma(2^p - 1) = \frac{(2^p-1)^2-1}{(2^p-1)-1} = \frac{((2^p-1)+1)((2^p-1)-1)}{(2^p-1)-1} = 2^p$
(2^{p-1}) is not prime so $\sigma(2^{p-1}) = \frac{2^p-1}{1} = 2^p - 1$

Are there any odd perfect numbers?
Probably not, but we can't show how.

Mersenne Number

A number of the from $2^n - 1$ is called a Mersenne number.

Mersenne Prime

A prime of the from $2^n - 1$ is called a Mersenne Prime
⇒ n is prime

However, if p is prime then $2^p - 1$ is not necessarily prime

Conjecture

There are infinitely many Mersenne Primes

*** In homework, this alone makes no sense ***
For example, if e is odd, p is prime (n is odd)
$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = even$
but 4 does not divide 2n,
at most one exponent of p_i or $n = p_1^{e_1} \ldots p_s^{e_s}$ can be odd.
*** end of nonsense ***

Identify an multiplicative function, want to know when $f(n) = g(n)$
You need only show that $f(p^k) = g(p^k)$ for all prime powers p^k

Theorem

For any n,

$$\sum_{d|n} \varphi(d) = n$$

Proof

Since φ is multiplicative, so is

$$g(n) = \sum_{d|n} \varphi(d)$$

$$g(p^k) = \sum_{d|p^k} \varphi(d) = \varphi(1) + \varphi(p) + \cdots + \varphi(p^k) = 1 + p - 1 + \cdots (p^{k-1} - p^{k-2}) + (p^k - p^{k-1})$$

$= p^k$
■

Question:

If we have

$$f(n) = \sum_{(d|n)} g(d)$$

Can you tell what g is? Yes

Ex.

$$\sum_{(d|n)} \varphi(d) = n$$

Gives us a formula for φ

Mobius Inversion

October-29-10 12:35 PM

Characteristic / Identify Function

$$I(n) = \begin{cases} 1 \; if \; n = 1 \\ 0 \; if \; n > 1 \end{cases}$$

Mobius Function

$$\mu(n) = \begin{cases} 0 \; if \; p^2 | n \\ (-1)^s, n = p_1 \times p_2 \times \cdots \times p_s \end{cases}$$

if n is the product of s distinct primes

Lemma

μ is multiplicative

Theorem

$$I(n) = \sum_{(d|n)} \mu(d)$$

Mobius Inversion

If g is a multiplicative function and

$$f(n) = \sum_{(d|n)} g(d), then$$

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

don't need to know below this line

Prime Number Theorem

$$\lim_{x \to \infty} \left(\frac{\pi(x)}{\left(\frac{x}{\log x}\right)} \right) = 1$$

Riemann Hypothesis

For any $\varepsilon > 0$

$$\lim_{N \to 0} \left(\frac{(\sum_{n=1}^{N} \mu(n))}{N^{\frac{1}{2}+\varepsilon}} \right) = 0$$

g(n) is NOT the function denoting the number of divisors of n, it is a placeholder function

If

$$f(n) = \sum_{(d|n)} g(d)$$

Then can we get a nice expression for g(n)?

The simplest multiplicative function is

$$I(n) = \begin{cases} 1 \; if \; n = 1 \\ 0 \; if \; n > 1 \end{cases}$$

Find a g such that

$$I(n) = \sum_{(d|n)} g(d)$$

If p is a prime, then $I(p) = 0$

So we need $g(p) = -1$ since

$$\sum_{(d|p)} g(d) = g(1) + g(p) = 1 + p(p) = 0 = I(p)$$

So $g(p) = -1 \; and \; g(1) = 1$

$$\sum_{(d|p^2)} g(d) = g(1) + g(p) + g(p^2) = 1 - 1 + 0 = 0$$

So $g(p^2) = 0$

So g is given on prime powers by

$$g(p^e) = \begin{cases} 1 \; if \; e = 0 \\ -1 \; if \; e = 1 \\ 0 \; if \; e > 1 \end{cases}$$

Mobius Function

This is called the Mobius function, and is denoted by μ

$$\mu(n) = \begin{cases} 0 \; if \; p^2 | n \\ (-1)^s, n = p_1 \times p_2 \times \cdots \times p_s \end{cases}$$

Lemma

μ is multiplicative

Proof

Let $m, n \in \mathbb{N}$ and gcd(m, n) = 1.

If $p^2 | mn$ then $p^2 | m$ or $p^2 | n$

So that $\mu(mn) = 0 = \mu(n)\mu(m)$

Now suppose that m and n are square free and write $m = p_1 \dots p_s$ and $n = q_1 \dots q_r$

Since $\gcd(m, n) = 1, p_i \neq q_j$ for any $i \in \{1, 2, \dots, s\} \; and \; j \in \{1, 2, \dots, r\}$

$\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(n)\mu(m)$

Theorem

$$I(n) = \sum_{(d|n)} \mu(d)$$

Proof

$n = 1$ is obvious. $I(n) = \mu(1) = 1$

If $n = p^k \; and \; k \geq 1, then \; I(p^k) = 0 \; and \; \sum_{(d|p^k)} \mu(d) = 1 - 1 + 0 + 0 + \cdots + 0 = 0$

Mobius Inversion

If g is a multiplicative function and

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

Proof

Assume

$$f(n) = \sum_{(d|n)} g(d)$$

Then

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

$$= \sum_{(e|n)} g(e)\, I\left(\frac{n}{e}\right) = g(n)$$

■

Example

We have

$$n = \sum_{(d|n)} \varphi(d)\,, so$$

$$\varphi(n) = \sum_{(d|n)} \mu(d) \times \frac{n}{d}$$

If $n = pq$

$$\varphi(n) = \sum_{(d|pq)} \mu(d) \frac{pq}{d} = pq - q - p + 1 = (p-1)(q-1)$$

Example

$$f(n) = \sum_{(d|n)} 1 \; so$$

$$1 = \sum_{(d|n)} \mu(d) f\left(\frac{n}{d}\right)$$

Why is μ interesting?

Prime Number Theorem

Not proving here PMATH 740 level

$$\lim_{x \to \infty} \left(\frac{\pi(x)}{\left(\frac{x}{\log x}\right)} \right) = 1$$

This is equivalent to

$$\lim_{N \to \infty} \left(\frac{\sum_{n=1}^{N} \mu(n)}{N} \right) = 0$$

Riemann Hypothesis

For any $\varepsilon > 0$

$$\lim_{N \to 0} \left(\frac{\left(\sum_{n=1}^{N} \mu(n)\right)}{N^{\frac{1}{2}+\varepsilon}} \right) = 0$$

(Worth $1000000 if solved)

Polynomials and Divisibility

November-01-10 12:30 PM

Definition of a Polynomial

If R is a commutative ring, then let R[x] be the set of polynomials with coefficients in R.

$$f(x) = \sum_{i=0}^{d} a_i x^i \, , a_i \in R$$

R[x] as a Ring

Adding and multiplying polynomials:

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$$

$$\left(\sum a_i x^i\right)\left(\sum b_i x^i\right) = \sum \left(\sum_{j+k=i} a_j b_k\right) x^i$$

Note

If F is a field, and $f(x), g(x) \in F[x]$
Then $\deg(fg) = \deg(f) + \deg(g)$

Constant Units

Let F be a field, and $f(x) \in F[x]$ be a unit. Then f(x) is constant.

Division on Polynomials

Let F be a field, and f(x), g(x) ∈ F[x] (non-zero). Then there are polynomials q(x) and r(x) such that $g(x) = q(x)f(x) + r(x)$ and $\deg(r) < \deg(f)$. Furthermore, q(x) and r(x) are unique.

Useful Fact:

$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

Other Useful Fact:

$f(x) = q(x)(x - c) + f(c)$

Corollary to the Division Algorithm

If F is a field, $f(x) \in F[x]$, and $c \in F$, then $f(c)=0$ iff $(x - c) | f(x)$

Definition of a Polynomial

If R is a commutative ring, then let R[x] be the set of polynomials with coefficients in R.

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x^1 + a_0 = \sum_{i=0}^{d} a_i x^i \, , a_i \in R$$

Consider them not as functions but as objects

Note also polynomials always have positive degrees since $i \geq 0$

R[x] as a Ring

Adding and multiplying polynomials:

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$$

$$\left(\sum a_i x^i\right)\left(\sum b_i x^i\right) = \sum \left(\sum_{j+k=i} a_j b_k\right) x^i$$

Can check that R[x] is also a commutative right, with 0 and 1 being the constant polynomials 0 and 1

The degree of a polynomial
$\sum_{n=0}^{m} a_i x^i$
Is the largest d such that $a_d \neq 0$. The zero polynomial has degree $-\infty$

Note

If F is a field, and $f(x), g(x) \in F[x]$
Then $\deg(fg) = \deg(f) + \deg(g)$

Example of a ring where this doesn't work:
$R = \mathbb{Z}_6$
$f(x) = 3x^2 + 1$ <- Degree 2
$g(x) = 2x^5 + x$ <- Degee 5
$f(x)g(x) = 6x^7 + 3x^3 + 2x^5 + x = 2x^5 + 3x^2 + x$ <- Degree 5

Why does it work in a field?
$(a_d x^d + \cdots)(b_e x^e + \cdots) = a_d b_e x^{d+e} + \cdots$
If the coefficients are in a field, F and $a_d \neq 0, b_e \neq 0$, then $a_d b_e \neq 0$

Claim

Let F be a field, and $f(x) \in F[x]$ be a unit. Then f(x) is constant.

Proof
If $g(x) \in F[x]$ with fg = 1, then
$\deg(f) + \deg(g) = \deg(fg) = 0$
$f \neq 0 \; and \; g \neq 0, so \deg(f), \deg(g) \geq 0$
So $\deg(f) = \deg(g) = 0$

Algebra with Polynomials

If F is a field, then algebra in F[x] is a lot like algebra in $\mathbb{Z}$
We really need F to be a field, or things are **not** like $\mathbb{Z}$

Example

In $\mathbb{Z}$, if $a^2 = 1$, then a $\pm$ 1. If F is a field then this is true in F[x]
Case when not a field: If f(x) ∈ $\mathbb{Z}_4[x]$ then $(2f(x) + 1)^2 = 4\big(f(x)\big)^2 + 4f(x) + 1 = 1$

Lemma: Division on Polynomials

Let F be a field, and f(x), g(x) ∈ F[x] (non-zero). Then there are polynomials q(x) and r(x) such that $g(x) = q(x)f(x) + r(x)$ and $\deg(r) < \deg(f)$. Furthermore, q(x) and r(x) are unique.

Proof

We can assume that $\deg(g) \geq \deg(f)$, otherwise q = 0 , r = g works.

Proceed by induction on the degree of g.
Base Case:
If deg(g) = 0, then either deg(g) < deg(f) (done!) or else f(x) and g(x) are both constant.
If $f(x) = a_0, g(x) = b_0 \; then$
$g(x) = \frac{b_0}{a_0} f(x) + 0$

Induction Step:
Assume that for any $g_2(x) \in F[x]$ with $\deg(g_2) < \deg(g)$ we can write
$g_2(x) = q_2(x)f(x) + r_2(x), \deg(r_2) < \deg(f)$
Write $g(x) = a_d x^d + [other \; lower \; degree \; terms]$
and $f(x) = b_e x^e + [lower \; order \; terms], b_e \neq 0$
deg(g)≥ deg(f) so d ≥ e

$let\ g_2(x) = g(x) - \frac{a_d}{b_e} f(x) x^{d-e}$

Write out the first term
$g_2(x) = \left(a_d x^d + \cdots\right) - \frac{a_d}{b_e} x^{d-e}(b_e x^e + \cdots)$
$g_2(x) = \left(a_d x^d + \cdots\right) - \left(a_d x^d + \cdots\right) = something\ of\ degree\ less\ than\ d = \deg(g)$
So $\deg(g_2) < \deg(g)$

By the induction hypothesis, we can write
$g_2(x) = q_2(x)f(x) + r(x) with\ q_2, r \in F[x] and\ \deg(r) < \deg(f)$
Since $g(x) = g_2(x) + \frac{a_d}{b_e} x^{d-e} f(x)$, we get

$$g(x) = \frac{a_d}{b_e} x^{d-e} f(x) + q(x)f(x) + r(x) = \left(\frac{a_d}{b_e} x^{d-e} + q_2(x)\right) f(x) + r(x) with\ \deg(r) < \deg(f)$$

So take $q(x) = \frac{a_d}{b_e} x^{d-e} + q_2(x)$
By induction, this is true for all polynomials. ■

Proof of Uniqueness

Suppose that
$g(x) = q_1(x)f(x) + r_1(x)\ and\ g(x) = q_2(x)f(s) + r_2(s)$
Then $0 = q_1 f + r_1 - q_2 f - r_2$ so $r_1 - r_2 = f(q_2 - q_1)$
Since F is a field, $\deg(r_1 - r_2) = \deg(f) + \deg(q_2 - q_1)$
If $q_1 - q_2 \neq 0, then$
$\deg(r_1 - r_2) \geq \deg(f)$
but $\deg(r_1), \deg(r_2) < \deg(f), so\ \deg(r_1 - r_2) < \deg(f)$

Useful Fact:

$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

That is a contradiction, so $q_1 = q_2, so\ r_1 = r_2$
Therefore, $q(x) and\ r(x)$ are unique.

This proof also shows how to do the division algorithm using long division.

Example:

Long divide $x^2 - 1$ into $x^3 - 2x^2 + 1$ and fine the quotient q(x) and remainder r(x)

$$\begin{array}{r} x - 2 \\ x^2 + 1 \,\big|\, x^3 - 2x^2 + 1 \\ \underline{x^3 + x} \\ -2x^2 - x + 1 \\ \underline{-2x^2 - 2} \\ -x + 3 \end{array}$$

So $q(x) = x - 2\ and\ r(x) = -x + 3 \Rightarrow (x^3 - 2x^2 + 1) = (x - 2)(x^2 + 1) + (-x + 3)$

Corollary to the Division Algorithm

If F is a field, $f(x) \in F[x]$, and $c \in F$, then $f(c)$=0 iff $(x - c) | f(x)$

Proof

By the division algorithm, we can write $f(x) = q(x)(x - c) + r(x)$ where
$deg(r(x)) < deg(x - c) = 1, so\ r \in F$ is a constant.

So $f(c) = q(c)(c - c) + r = q(c) \times 0 + r = r$
$f(x) = q(x)(x - c) + f(c)$

If $f(c) = 0, then\ f(x) = q(x)(x - c), so\ (x - c) | f(x)$
Conversely, if $f(x) = (x - c)h(x)\ for\ some\ h(x) \in F[x], so\ f(c) = (c - c)h(c) = 0$

GCD of Polynomials

November-03-10 1:10 PM

Division on a commutative ring

For any commutative ring R, we say that a divides b (for a, b ∈ R) if and only if b = ac for some c ∈ R, a|b.

Division on a polynomial field

If F is a field and $f(x), g(x) \in F[x]$, then $f(x)|g(x)$ means $c_1 f(x)|c_2 g(x)$ for any $c_1, c_2 \in F$

GCD for Polynomials

Let F be a field, $f(x), g(x) \in F[x]$
There is a polynomials $d(x)$ so that

1. d|f and d|g
2. if $e(x) \in F[x]$ with e|f and e|g then e|d
3. There exist $s(x), t(x) \in F[x]$ with
$$d = fs + gt$$

Call the GCD of f and g the polynomial d which satisfies all of these properties and is monic.

Monic

$f(x) \in F[x]$ is monic if
$f(x) = x^d + smaller\ terms$

Example of division on polynomials

$(x-1)|(x^3-1)\ \ in\ \mathbb{Q}[x]$ but also $(2x-2)|(x^3-1)$
$$(x^3-1) = (2x-2)\left(\frac{1}{2}x^2 + \frac{1}{2}x + \frac{1}{2}\right)$$

Theorem (Euclidean Algorithm for Polynomials)

Let F be a field, $f(x), g(x) \in F[x]\ and\ non-zero$
There is a polynomials $d(x)$ so that

1. d|f and d|g
2. if $e(x) \in F[x]$ with e|f and e|g then e|d
3. There exist $s(x), t(x) \in F[x]$ with
$$d = fs + gt$$

d is not unique
If d has those properties then so does cd for any $c \in F, c \neq 0$
If d_2 is another polynomial with all of the same properties, then $d(x) = cd_2(x)$ for some non-zero $c \in F\ (since\ d|d_2\ and\ d_2|d)$

Observation

If F is a field and $f, g \in F[x]$ then $f|g\ and\ g|f$ iff $f = cg$ for some c ∈ F, c ≠ 0

Proof
If $f = cg$ then g|f, and $g = c^{-1}f$, so f|g
If $g|f\ and\ f|g$, deg(f)=deg(g). So $g = hf$ for some $h \in F[a]$, deg(h)=0, so $h = c \in F$

Proof of the Theorem (Euclidean Algorithm for Polynomials)

We can suppose that $\deg(f) \geq \deg(g)$
Using the division algorithm, write
$f = q_1 g + r_1, \deg(r_1) < \deg(g)$
$g = q_2 r_1 + r_2, \deg(r_2) < \deg(r_1)$
…
Eventually, $r_j = 0$
$r_{j-2} = q_j r_{j-1} + 0$
Then the GCD is r_{j-1} (made monic) (proof of 1.)

$d = r_{j-1}|r_{j-2}$
$d \mid q_{j-1}r_{j-2} + r_{j-1} = r_{j-3}$
… etc. Eventually see $g|d\ and\ g|f$

$d = 1 \times r_{j-3} + (-q_{j-1}) \times r_{j-2}$
but $r_{j-4} = q_{j-2}r_{j-3} + r_{j-2}, so$
$d = (1) \times r_{j-3} + (-q_{j-1})(r_{j-4} - q_{j-2}r_{j-3}) = (?)r_{j-3} + (?)r_{j-4} = (?)f + (?)g.$
(proof of 3.)

Now, if e|f and e|g, then $e|sf + tg = d$ (proof of 2.)
■

Example

Find the GCD of
$f(x) = x^4 - 2x^3 + x^2 - 2x$
$g(x) = x^4 + 3x^3 + 2x^2 + 3x + 1$

Step 1: write $f = q_1 g + r_1, q_1 = 1, r_1 = -5x^3 - x^2 - 5x - 1$
Now write $g = q_2 r_1 + r_2$

$$\begin{array}{r|l} & -\frac{1}{5}x - \frac{14}{25} \\ \hline -5x^3 - x^2 - 5x - 1 & x^4 + 3x^3 + 2x^2 + 3x + 1 \\ & \underline{-x^4 + \frac{1}{5}x^3 + x^2 + \frac{1}{5}x} \\ & \frac{14}{5}x^3 + x^2 + \frac{14}{5}x + 1 \\ & \underline{-\frac{14}{5}x^3 + \frac{14}{25}x^2 + \frac{14}{5}x + \frac{14}{25}} \\ & \frac{11}{25}x^2 + \frac{11}{25} \end{array}$$

So $q_2 = -\frac{1}{5}x - \frac{14}{25}, r_2 = \frac{11}{25}x^2 + \frac{11}{25}$
Now want to write
$r_1 = q_3 r_2 + r_3$

$$\begin{array}{r|l} & -\frac{125}{11}x - \frac{25}{11} \\ \hline \frac{11}{25}x^2 + \frac{11}{25} & -5x^3 - x^2 - 5x - 1 \\ & \underline{-5x^3 + 0 - 5x + 0} \\ & -x^2 - 1 \\ & \underline{-x^2 - 1} \\ & 0 \end{array}$$

$$d = \frac{11}{25}x^2 + \frac{11}{25}\ so\ \gcd(f(x), g(x)) = x^2 + 1$$

Find s and t so that $sf + tg = x^2 + 1$
$$x^2 + 1 = \left(\frac{5}{11}x + \frac{14}{11}\right)f(x) + \left(-\frac{5}{11}x + 1\right)g(x)$$

GCD for polynomials over F ⇔ GCD for integers

Factorization of Polynomials

November-05-10 1:10 PM

Irreducible Polynomial

A polynomial $f(x) \in F[x]$ is irreducible iff whenever $f(x) = g(x)h(x), g, h \in F[x]$, then g or h is constant. (In other words, degree of its divisors can only be 0 or the degree of itself)

Unique Factorization for Polynomials

Any non-zero polynomial $f(x) \in F[x]$ can be written as $f = ap_1^{e_1}p_2^{e_2} \times \cdots \times p_k^{e_k}$ where a ∈ F
$p_i \in F[x]$ are distinct, monic and irreducible, and $e_1 \geq 1$. This representation is unique (up to order)

Lemma

If $p, q, r \in F[x]$ and $\gcd(p, q) = 1$ and $p|qr$, then $p|r$.

Corollary

If p is irreducible, and $p|q_1q_2 \dots q_r$, then $p|q_i$ for some i

Unique factorization for polynomials

Theorem

Any non-zero polynomial $f(x) \in F[x]$ can be written as $f = ap_1^{e_1}p_2^{e_2} \times \cdots \times p_k^{e_k}$ where a ∈ F
$p_i \in F[x]$ are distinct, monic and irreducible, and $e_1 \geq 1$. This representation is unique (up to order)

Lemma

If $p, q, r \in F[x]$ and $\gcd(p, q) = 1$ and $p|qr$, then $p|r$.

Proof

Choose $s, t \in F[x]$ so that $sp + tq = 1$
$r = r \times 1 = r(sp + tq) = prs + rqt$
$p|p \text{ and } p|qr$ so $p|r$
■

Corollary

If p is irreducible, and $p|q_1q_2 \dots q_r$, then $p|q_i$ for some i

Proof (For r = 2)

Suppose that p is irreducible and $p|q_1q_2$
$\gcd(p, q_1)$ is a divisor of p(x)
So $\gcd(p, q_1) = 1 \text{ or } cp$ for some c ∈ F
If $\gcd(p, q_1) = cp$, then $cp|q_1 \text{ so } p|q_1$
If $\gcd(p, q_1) = 1$ then the previous lemma gives $p|q_2$
■

For r > 2

Induct over r, either divides p_r or divides $p_1p_2 \dots p_{r-1}$, in which case p divides one of those

Proof of Factorization

$If\ f(x) = ax^d + \cdots$, then $\frac{1}{a}f(x)$ is monic.

So we'll assume that f(x) is monic (because we can just multiply by a at the end)
Want to show that f(x) can be written as the product of irreducible monic polynomials.
By induction on the degree of f.

Base Case: deg(f) = 1
Then $f(x) = x + b$ for some $b \in F$
f(x) is irreducible, so can write f as a product of itself.

Induction: Suppose that the statement is true for polynomials of degree < degree(f)
If f is irreducible then we're done. If not, then $f(x) = g(x)h(x)$ with deg(g), deg(h) < deg(f) say,
$g(x) = bx^e + \cdots$
$h(x) = cx^w + \cdots$
$f(x) = (bx^e + \cdots)(cx^w + \cdots) = bcx^{e+w}, so\ bc = 1$
$f(x) = g(x)h(x) = \big(cg(x)\big)\big(c^{-1}h(x)\big) = (x^e + \cdots)(x^w + \cdots)$
So f can be factored into two monic polynomials. By the induction hypothesis, both $cg(x)$ and $c^{-1}h(x)$ can be written as a product of monic, irreducible polynomials.
So f(x) can be written as the product of monic, irreducible polynomials.

By induction, any monic polynomial can be written as a product of monic irreducible polynomials.
If $f(x) \in F[x]$ is non-zero (possibly not monic) then $f(x) = ap_1^{e_1}p_2^{e_2} \dots p_r^{e_r}$ as in the theorem.
■

Proof of Uniqueness

Suppose that
$ap_1^{e_1}p_2^{e_2} \dots p_r^{e_r} = bq_1^{w_1}q_2^{w_2} \dots q_s^{w_s}$
with a, b ∈ F non-zero, p_i, q_i monic and irreducible, and $e_i, w_i, \geq 1$
Multiplying out, a is the coefficient of the highest power of x in $ap_1^{e_1}p_2^{e_2} \dots p_r^{e_r}$ and b is the coefficient of the highest power of x in $bq_1^{w_1}q_2^{w_2} \dots q_s^{w_s}$ so a = b.

Now we want to show that $p_1^{e_1}p_2^{e_2} \dots p_r^{e_r} = q_1^{w_1}q_2^{w_2} \dots q_s^{w_s} \Rightarrow p_i \text{ are the } q_j (in\ some\ order)$
Induction on the number of factors. Total number of factors on the left is n= $e_1 + e_2 + \cdots + e_r$

Base Case: n = 1
$LHS = p = q_1^{w_1}q_2^{w_2} \dots q_s^{w_s}$
RHS should not be the product of two or more monic irreducible polynomials, since p is irreducible.
So RHS = q, and p = q
So we're done if n = 1

Induction: Suppose that this is true for products of fewer than n monic, irreducible polynomials.
If $p_1^{e_1}p_2^{e_2} \dots p_r^{e_r} = q_1^{w_1}q_2^{w_2} \dots q_s^{w_s}$, then with $n = e_1 + e_2 + \cdots e_r$, then p_1 is monic, irreducible, and $p_1|q_1^{w_1}q_2^{w_2} \dots q_s^{w_s}$.
By the corollary, $p_1|q_j$ for some j. But q_j is also irreducible and monic, so $p_1 = q_j$
So $p_1^{e_1-1}p_2^{e_2} \dots p_r^{e_r} = q_1^{w_1} \dots q_j^{w_j-1} \dots q_s^{w_s}$
By the induction hypothesis, the polynomials on the LHS are the same as the polynomials on the RHS, up to order.

By induction, the representation is unique. ■

*Elliptic Curves

November-08-10 4:31 PM

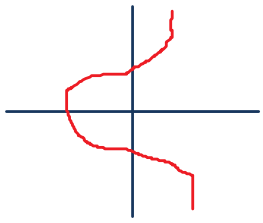
Elliptic Curve: Simple Explanation

Solutions to an equation of the from $y^2 = x^3 + ax + b$, where a and b are given (in some field).

Want $27b^2 + 4a^3 \neq 0$, ensures the equation has three distinct roots (in the complex plane)

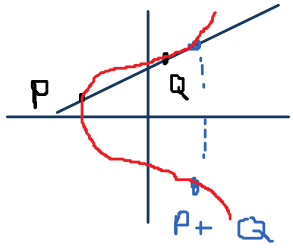
Example

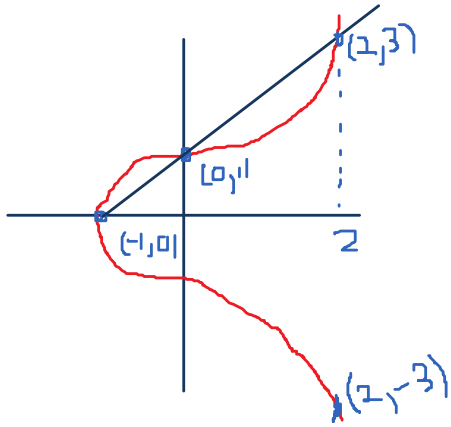
$y^2 = x^3 + 1, F = \mathbb{R}$



Elliptic Curves are Groups

Addition of Points





Example: Let $C: y^2 = x^3 + 1$

The equation of the line is
$y = x + 1$
$(x + 1)^2 = x^3 + 1$
$x^2 + 2x + 1 = x^3 + 1$
$x^3 - x^2 - 2x = 0 = x(x + 1)(x - 2)$
$x = -1, 0, 2$
$y^2 = 2^3 + 1 \Rightarrow y = 3$

So $(-1, 0) + (0, 1) = (2, -3)$

What about when P = Q?
The line should be the tangent line

What about when the line is vertical?
Need to add a "point" O, which is on all vertical lines. The reflection of O is O

(0, 1) + (0, -1) = O

Fact

This operation makes the points on the curve (along with O) into a group, with O as the identity.

For all points P and Q, $P + Q = Q + P$ (abelian group)

1. P+O = P for all O on C
2. For every P on the curve, there is a -P such that P+(-P) = 0
   So -(x, y) = (x, -y)
3. P+(Q+R)=(P+Q)+R

If P and Q have $\mathbb{Q}$ coordinates, then the line joining P and Q has rational coefficient. Therefore the third point must have rational coefficients.

If P and Q have coefficients in any field F, so does P+Q

Example

On $y^2 = x^3 + 1$
Calculate $2(2, -3)$
$2y\frac{dy}{dx} = 3x^2 \Rightarrow \frac{dy}{dx} = \frac{3x^2}{2y}$
At $(2, -3)$, the slope of the tangent line is $\frac{12}{-6} = -2$
Tangent line: $y = -2x + 1$
$x^3 + 1 = (-2x + 1)^2$
$x^3 + 1 = 4x^2 - 4x + 1$
$x^3 - 4x^2 + 4x = 0 \Rightarrow x(x - 2)^2$
So the third point of intersection is $(0, 1)$
So $2(2, -3) = (0, -1)$
Interpret tangents as double intersections
Inflection points are interpreted as triple intersections.
(0, 1) is an inflection point
2(0, 1) = (0, -1) = -(0, 1)
3(0, 1) = -(0, 1) + (0, 1) = O

Irreducible Polynomials in $\mathbb{Z}[x]$

November-10-10 12:31 PM

Primitive

A polynomials $f(x) \in \mathbb{Z}[x]$ is primitive if the gcd of the coefficients is 1. i.e. if there is no prime dividing all of the coefficients.

Lemma (Gauss' Lemma)

If f, g ∈ $\mathbb{Z}$[x] are primitive, then so is fg.

Theorem (Gauss)

If $f(x) \in \mathbb{Z}[x]$ and f(x) is reducible in $\mathbb{Q}[x]$, then $f(x)$ is reducible in $\mathbb{Z}[x]$

Corollary

Let

$$f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$$

and suppose that $f\left(\frac{b}{c}\right) = 0, \quad b, c \in \mathbb{Z}, \gcd(b, c) = 1$

Then $c|a_d$ and $b|a_0$

When can $f(x) \in \mathbb{Z}[x]$ be factored (in $\mathbb{Z}$[x])

Proof of Lemma

Let p be a prime, and

$$f(x) = \sum_{i=0}^{d} a_i x^i \quad (a_i \in \mathbb{Z})$$

$$g(x) = \sum_{i=0}^{e} b_i x^i \quad (b_i \in \mathbb{Z})$$

By hypothesis, there is at least one i with $p \nmid b_i$. Let i_0 be the smallest i such that $p \nmid b_i$
Similarly, let j_0 be the least j such that $p \nmid a_j$

Now,

$$fg = \left(\sum_{j=0}^{d} a_j x^j\right)\left(\sum_{i=0}^{e} b_i x^i\right) = \sum_{k=0}^{d+e}\left(\sum_{i+j=k} a_j b_i\right) x^k$$

The coefficient of $x^{i_0+j_0}$ is:

$$\sum_{i+j=i_0+j_0=k_0} a_j b_i = (a_0 b_{k_0} + a_1 b_{k_0-1} + \cdots + a_{k_0-1} b_1 + a_{k_0} b_0$$

$$= \left(a_0 b_{k_0} + a_1 b_{k_0-1} + \cdots\right) + a_{j_0} b_{i_0} + \left(a_{j_0+1} b_{i_0-1} + \cdots + a_{k_0} b_0\right)$$

The first term is divisible by p since a_j is divisible by p for every $j < j_0$
The last term is divisible by p since b_i is divisible by p for every $i < i_0$
$a_{j_0} b_{i_0}$ is not divisible by p

So the coefficient of $x^{i_0+j_0}$ in f(x)g(x) is not divisible by p.
Since p was any prime, fg is primitive. ■

Proof of Theorem

Let $f(x) \in \mathbb{Z}[x]$ and suppose that $f = gh$ for $g, h \in \mathbb{Q}[x]$
deg(g), deg(h) < deg(f)

Choose M, N ∈ $\mathbb{Z}$ such that Mg(x), Nh(x) ∈ $\mathbb{Z}$[x]
Also, if m is the gcd of the coefficients of Mg(x), then
$Mg(x) = mg_1(x)$ for $g_1(x) \in \mathbb{Z}[x]$. g_1 is primitive
Similarly,
$Nh(x) = nh_1(x)$ where $h_1(x) \in \mathbb{Z}[x], n = \gcd\, of\ coeffcients\ of\ h$, h_1 is primitive.

Now, $g_1 h_1 \in \mathbb{Z}[x]$ is primitive, and $mn(g_1 h_1) = \left(mg_1(x)\right)\left(nh_1(x)\right) = Mg(x)Nh(x) = MNf(x)$

If d is the gcd of the coefficients of f, then mn=MNd
Since gcd of coefficients of $mn(g_1 h_1)$ is m× n× 1=mn and gcd of coefficients of $MNf(x)$ is MNd and so
$MNd\ g_1(x)h_1(x) = MNf(x)$
$\left(dg_1(x)\right)\left(h_1(x)\right) = f(x)$
$dg_1(x), h_1(x) \in \mathbb{Z}[x]$
(degrees have not changed) ■

Proof of Corollary

Suppose that $f\left(\frac{b}{c}\right) = 0$. Then in $\mathbb{Q}[x]$, $\left(x - \frac{b}{c}\right)|f(x)$
So there is some integer N such that $N\left(x - \frac{b}{c}\right) \in \mathbb{Z}[x]$ is primitive and $N\left(x - \frac{b}{c}\right)|f(x)$ in $\mathbb{Z}$[x]
$(cx - b) = c\left(x - \frac{b}{c}\right)$ is primitive so
$(cx - b)|f(x)$ in $\mathbb{Z}$[x]
This means
$(cx - b)(g_e x^e + \cdots + g_0) = \left(a_d x^d + \cdots + a_0\right)$
$cg_e x^{e+1} + \cdots - bg_0 = a_d x^d + \cdots + a_0$
So $a_0 = -bg_0 \Rightarrow b|a_0$
$a_d = cg_e \Rightarrow c|a_e$
■

Example

Show that $f(x) = 3x^5 + 2x - 2$ has no rational roots.

Solution

If $f\left(\frac{b}{c}\right) = 0, \frac{b}{c} \in \mathbb{Q}[x]$ in lowest terms. Then the corollary says that
$b|2\ and\ c|3$
$b = \pm 1, \pm 2 \quad c = \pm 1, \pm 3$
$\frac{b}{c} = \pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}$
None of these is a root. ■

Eisenstein's Criterion

November-10-10 1:16 PM

Theorem (Eisenstein's Criterion)

Let $f(x) \in \mathbb{Z}[x]$,

$$f(x) = \sum_{i=0}^{d} a_i x^i, \qquad a_i \in \mathbb{Z}, a_d \neq 0$$

If there is a prime p such that

1. $p \nmid a_d$
2. $p | a_i$ for $0 \leq i < d$
3. $p^2 \nmid a_0$

then f(x) is irreducible.

Example

$f(x) = 2x^{10} - 10x^3 + 5$
is irreducible, since
$5 \nmid 2, 5|10, 5|, 5^2 \nmid 5$

Proof of Eisenstein's Criterion

Suppose f(x) is reducible, and write

$$f(x) = g(x)h(x) = \left(\sum_{i=0}^{m} b_i x^i\right)\left(\sum_{j=0}^{n} c_j x^j\right)$$

$\deg(g), \deg(h) < \deg(f), \quad b_i, c_j \in \mathbb{Z}$ by Gauss' Lemma
$a_d = b_m c_n$ (assuming m=deg(g), n = deg(h))
So $p \nmid b_m, and\ p \nmid c_n$
Also, $a_0 = b_0 c_0$.
So $p|b_o c_o\ but\ p^2!|b_0 c_0$
Thus, exactly one of b_0, c_0 is divisible by p

We'll suppose that $p|b_0, b \nmid c_0$
Let i_0 be the least value of i such that $p \nmid b_i$
Look at a_{i_0} $(i_0 \leq m < d)$
Since $i_0 < d, p|a_{i_0}$

$$a_{i_0} = \sum_{j+k=i_0} b_k c_j = b_{i_0} c_0 + b_{i_0-1} c_1 + \cdots + b_0 c_{i_0}$$

$b_{i_0-1} c_1 + \cdots + b_0 c_{i_0}$ is divisible by p since $p|b_i$ for $i < i_0$
but $p|a_{i_0}$ so $p|b_{i_0} c_0$
However, $p \nmid b_{i_0}$ and $p \nmid c_0$
This is a contradiction. So $f(x)$ does not factor in $\mathbb{Q}$[x]

Algebraic Numbers

November-12-10 12:48 PM

Algebraic Numbers

A number $a \in \mathbb{C}$ is algebraic if there is some polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(a) = 0$

Transcendental

If $a \in \mathbb{C}$ is not algebraic, then it is transcendental.

Theorem

If $a \in \mathbb{C}$ is algebraic, then there is a unique monic polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(a) = 0$ and $f(x)|g(x)$ for any non-zero $g(x) \in \mathbb{Q}[x]$ such that $g(a) = 0$

Minimal Polynomial

The polynomial in the theorem is the minimal polynomial for a.

Corollary

If $a \in \mathbb{C}$ is the root of a polynomial $f(x) \in \mathbb{Q}[x]$, which is non-zero and irreducible, then a is irrational - unless deg(f) = 1

Example

Despite being rational, $\sqrt{2}$ can be described in terms of rational numbers
$\sqrt{2}$ is the positive solution to $x^2 - 2 = 0$

If $f(x) \in \mathbb{Q}[x]$, the roots of $f(x)$ (in $\mathbb{C}$ or $\mathbb{R}$) are somehow described in terms of $\mathbb{Q}$

Proof of Theorem

We know that a is the root of some non-zero polynomial. Let $f(x)$ be a polynomial of lowest degree in $\mathbb{Q}[x]$ which is monic, and $f(a) = 0$. Suppose that $g(a) = 0$ for $g(x) \in \mathbb{Q}[x]$
Write:
$g(x) = q(x)f(x) + r(x), \qquad q, r \in \mathbb{Q}[x]\ and\ \deg(r) < \deg(f)$
Then
$0 = g(a) = q(a)f(a) + r(a) \Rightarrow 0 = r(a), since\ f(a) = 0$
If r(x) is not the zero polynomial, then dividing by the leading coefficient gives a polynomial $r_2(x) \in \mathbb{Q}[x]$ which is monic, and $r_2(a) = 0$, and $\deg(r_2) < \deg(f)$
But f is a polynomial of the smallest degree with these properties, so this is a contradiction.
So $r(x) = 0$ and $g(x) = q(x)f(x)$, in other words $f(x)|g(x)$

If $f_1(x)$ and $f_2(x)$ both have this property.
$f_2(a) = 0$, so $f_1(x)|f_2(x)$
$f_1(a) = 0$, so $f_2(x)|f_1(x)$
This means that $f_1(x) = cf_2(x)$ for c ∈ $\mathbb{Q}$
But both f_1 and f_2 are monic, so $c = 1$, so $f_1 = f_2$
And so $f(x)$ is unique.
■

Proof of Corollary

If a is rational, then $(x - a)|f(x)$ (given that $f(a) = 0$)
So f(x) is not irreducible, a contradiction. ■

Example

$f(x) = x^n - 2 \in \mathbb{Q}[x]$ is irreducible, by the Eisenstein criterion
So if $n > 1$, then $\sqrt[n]{2} \notin \mathbb{Q}$

Example

$\sqrt{2} + \sqrt{3}$ is algebraic but what is the (minimal) polynomial $f(x) \in \mathbb{Q}[x]$ s.t. $f\left(\sqrt{2} + \sqrt{3}\right) = 0$

$w = \sqrt{2} + \sqrt{3}$
Find a polynomials $f(x) \in \mathbb{Q}[x]$ with $f(w) = 0$

Solution
Want some $a_d w^d + a_{d-a} w^{d-1} + \cdots + a_0 = 0$

$w = \sqrt{2} + \sqrt{3}$
$w^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$
$w^3 = 11\sqrt{2} + 9\sqrt{3}$
$w^4 = 49 + 20\sqrt{6}$
$w^4 - 10w^2 = \left(49 + 20\sqrt{6}\right) - 10\left(5 + 2\sqrt{6}\right) = -1$

So $f(x) = x^4 - 10x^2 + 1$ ■

Done, but is f(x) the minimal polynomial?
If not, f(x) factors in $\mathbb{Z}[x]$. If f(x) factors, then either it has a root in $\mathbb{Q}$, or else it factors as (quadratic)(quadratic)

By Gauss Lemma Corollary, the only possible roots of f(x) in $\mathbb{Q}$ are x = ± 1, these are not roots so f(x) has no roots in $\mathbb{Q}$.
So if it is reducible, it factors as
$f(x) = x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$
$= x^4 + (a + c)x^3 + (d + b + ac)x^2 + (ad + bc)x + db$

$a + c = 0, \Rightarrow a = -c$
$ad + bc = 0$
$d + b + ac = -10$
$db = 1$

$-cd + bc = 0 \Rightarrow d = b$
$d^2 = 1 \Rightarrow d = b = \pm 1$
$1 + 1 - c^2 = -10 \Rightarrow c^2 = 12 \Rightarrow c = \sqrt{12} = 2\sqrt{3}, which\ is\ irrational$
$-1 - 1 - c^2 = -10 \Rightarrow c^2 = 8 \Rightarrow c = 2\sqrt{2}, which\ is\ irrational$
So there are no solutions for factors in $\mathbb{Q}$[x]

Transcendental Numbers

November-15-10 12:30 PM

Transcendental Number

$a \in \mathbb{C}$ is transcendental iff it is not algebraic.

Theorem (Liouville)

Suppose that $a \in \mathbb{R}$ is a root of the irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Then there is a $\delta > 0$ such that $\left|a - \frac{p}{q}\right| > \frac{\delta}{q^d}$ for any rational number $\frac{p}{q} \in \mathbb{Q}$ in lowest terms, d= deg(f) > 1

Examples (Without proof)

e, π, ...

How do you show that a specific number is transcendental?

Theorem (Liouville)

Suppose that $a \in \mathbb{R}$ is a root of the irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Then there is a $\delta > 0$ such that $\left|a - \frac{p}{q}\right| > \frac{\delta}{q^d}, or = 0$ for any rational number $\frac{p}{q} \in \mathbb{Q}$ in lowest terms, d= deg(f)

For any real number a, you can find rationals $\frac{p}{q}$ with $\left|a - \frac{p}{q}\right|$ as small as you want.
Ex: just cut off the decimal expansion of a at some point.

If I want $\left|a - \frac{p}{q}\right| < \varepsilon$, a algebraic and irrational
$\frac{\delta}{q^d} < \ ... < \varepsilon$
So $\sqrt[d]{\delta\varepsilon^{-1}} < q$

Proof

We have $f(x) \in \mathbb{Q}[x]$ of degree d > 1, irreducible, $f(a) = 0$
Without loss of generality, $f(x) \in \mathbb{Z}[x]$

So $f(x) = a_d x^d + \ ... a_1 x + a_0$
Want a lower bound on $|x - a|$ for $x \in \mathbb{Q}$
If x is not in $[a-1, a+1]$ then $|x - a| > 1$

On the other hand, if x is in $[a-1, a+1]$, then for some c in $[a-1, a+1]$, by the mean value theorem we have:
$f(x) - f(a) = f'(c)(x - a)$
$f(a) = 0$, so
$|f(x)| = |f'(c)| \times |x - a|$
By the extreme value theorem $|f'(c)| \leq M$ for c on this interval, for some M.
$|x - a| \geq \frac{1}{M}|f(x)|$
Now we want a lower bound on $|f(x)|$ for $x \in \mathbb{Q}$. Write $x = \frac{p}{q}, \ \ p, q, \in \mathbb{Z}$

$$f\left(\frac{p}{q}\right) = a^d \frac{p^d}{q^d} + a_{d-1}\frac{p^{d-1}}{q^{d-1}} + \cdots + a_0$$

$$q^d f\left(\frac{p}{q}\right) = a_d p^d + a_{d-1} q p^{d-1} + \cdots + a_1 p q^{d-1} + a_0 q^d$$

So $q^d f\left(\frac{p}{q}\right) \in \mathbb{Z}$

$q^d f\left(\frac{p}{q}\right) \neq 0 \ \ so \ \ \left|q^d f\left(\frac{p}{q}\right)\right| \geq 1$

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}$$

So

$$\left|\frac{p}{q} - a\right| \geq \frac{1}{M} \times \frac{1}{q^d}$$

So if $\frac{p}{q}$ is not in $[a-1, a+1]$, $\left|a - \frac{p}{q}\right| > 1 \geq \frac{1}{q^d}$ and if a is in $[a-1, a+1]$ then $\left|a - \frac{p}{q}\right| \geq \frac{M^{-1}}{q^d}$
So

$$\left|a - \frac{p}{q}\right| \geq \frac{\min\{1, M^{-1}\}}{q^d} > \frac{\frac{1}{2}\min\{1, M^{-1}\}}{q^d} = \frac{\delta}{q^d}$$

■

Example of Liouville's Theorem
For p/q ∈ ℚ, $\left|\sqrt{2} - \frac{p}{q}\right| > \frac{\delta}{q^2}$ for some δ > 0

Constructing transcendentals, construct $a \in \mathbb{R}$ with very good approximations in ℚ

*Elliptic Curves Cont.

November-15-10 4:38 PM

Example Curve

Considering $y^2 = x^3 + 1$

Obvious points on this curve:
$O, (-1, 0), (0, 1), (0, -1), (2, 3), (2, -3)$

Addition of Points

	O	**(2, -3)**	**(0, -1)**	**(-1, 0)**	**(0, 1)**	**(2, 3)**
O	O	(2, -3)	(0, -1)	(-1, 0)	(0, 1)	(2, 3)
(2, -3)	(2, -3)	(0, -1)	(-1, 0)	(0, 1)	(2, 3)	O
(0, -1)	(0, -1)	(-1, 0)	(0, 1)	(2, 3)	O	(2, -3)
(-1, 0)	(-1, 0)	(0, 1)	(2, 3)	O	(2, -3)	(0, -1)
(0, 1)	(0, 1)	(2, 3)	O	(2, -3)	(0, -1)	(-1, 0)
(2, 3)	(2, 3)	O	(2, -3)	(0, -1)	(-1, 0)	(0, 1)

If labeled P_0, P_1, P_2, P_4, P_5 in order along the table
then
$P_a + P_b = P_{a+b\ (mod\ 6)}$

Are there more points with coordinates in $\mathbb{Q}$?
Hard question

Could consider elliptic curves over any field, Eg $\mathbb{Z}_p$ $(4a_4 + 27b^2 \neq 0\ in\ \mathbb{Z}_p)$

Eg. $y^2 = x^3 + 1$ over $\mathbb{Z}_5$
Solutions: O, (0, 1), (0, -1), (2, 3), (2, -3), (4, 0)
These are the "same" six points, and add in the same way.

$y^2 = x^3 + 1\ in\ \mathbb{Z}_7$
Solutions: O, (0, 1), (0, -1), (1, 3), (1, -3), (2, 3), (2, -3), (3, 0), (4, 3), (4, -3), (5, 0), (-1, 0)
12 points on $y^2 = x^3 + 1\ in\ \mathbb{Z}_7$
If we take any points that work over integers, than you have the same closed group of 6 points. But look at other points.

Try to add $(5, 0) + (5, 0)$
"slope of the tangent line"
$= \frac{3x^2}{2y}$
which is a vertical line so
$(5, 0) + (5, 0) = O$

$(1, 3) + (1, 3)$
slope of tangent line:
$\frac{3}{2 * 3} = \frac{1}{2} = 4$
So the equation of the tangent line: $y - 3 = 4(x - 1)$
$y = 4x - 1$
$y^2 = x^3 + 1$
$x^3 + 1 = (4x - 1)^2 = 16x^2 - 8x + 1 = 2x^2 - x + 1$
$x^3 - 2x^2 + x = 0 = x(x - 1)^2 = 0$
So $x = 0, y = -1$

So $(1, 3) + (1, 3) = (0, 1)$

Use in Cryptography

What can elliptic curves over finite fields be used for?

With an elliptic curve C over a finite field, can use the Diffie-Hellman key exchange.
Alice and Bob want to agree on a common secret.

1. Alice and Bob select a prime p, and elliptic curve C over $\mathbb{Z}_p$, and a point Q on C.
2. Alice choses a, and makes aQ public.
3. Bob choses b, and makes bQ public (a, b ≥ 2 are integers)
4. Common secret: abQ

For a 3rd person to get the key, they need to solve the. ECDLP (Elliptic Curve Discrete Log Problem):
Given an elliptic curve C over $\mathbb{Z}_p$ a point Q, and the point aQ, find a.

Elliptic curves over $\mathbb{Z}_p$ have approximately p points on them, so for p large, this is hard.

Transcendentals With Liouville

November-17-10 12:38 PM

Want to use Liouville's Theorem to show that certain numbers are transcendental
Need to construct a number with very good rational approximations

Ex
Let
$a = \sum_{m=1}^{\infty} 10^{-m!}$
Then a is transcendental

$a = \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} + \frac{1}{10^{120}} + \frac{1}{10^{720}} + \cdots$
$a = 0.11000100000000000000000010000 \ldots 00000010000$

Point: the partial sums are rational numbers that are extremely close to a

Let
$\frac{p_n}{q_n} = \sum_{m=1}^{n} 10^{-m!} \in \mathbb{Q}$
$q_n = 10^{n!}$
$p_n = \sum_{m=1}^{n} 10^{n!-m!}$

$\frac{p_1}{q_1} = \sum_{m=1}^{1} 10^{-m!} = \frac{1}{10}$
$\frac{p_2}{q_2} = \sum_{m=1}^{2} 10^{-m!} = \frac{1}{10} + \frac{1}{100} = \frac{11}{100}$
$\frac{p_3}{q_3} = \sum_{m=1}^{3} 10^{-m!} = \frac{1}{10} + \frac{1}{100} + \frac{1}{1000000} = \frac{11001}{1000000}$

$\left|a - \frac{p_n}{q_n}\right| = \left|\sum_{m=1}^{\infty} 10^{-m!} - \sum_{m=1}^{n} 10^{-m!}\right| = \sum_{m=n+1}^{\infty} 10^{-m!} = 10^{-(n+1)!} + 10^{-(n+2)!} + \cdots < 2 \times 10^{-(n+1)!}$
So
$\left|a - \frac{p_n}{q_n}\right| < 2 \times 10^{-(n+1)!}$
$q_n = 10^{n!}$
$\left|a - \frac{p_n}{q_n}\right| < 2\left(10^{n!}\right)^{-(n+1)} = 2q_n^{-(n+1)}$

Now, suppose that a is algebraic. So
$f(a) = 0$ for some irreducible $f(x) \in \mathbb{Q}[x]$ of degree d ≥ 2
a is not rational since the decimal expansion never halts or repeats

By Liouville's Theorem, there is a $\delta > 0$ such that
$\left|a - \frac{p}{q}\right| > \frac{\delta}{q^d}$
for all $\frac{p}{q} \in \mathbb{Q}$
So…
$\frac{\delta}{q_n^d} < \left|a - \frac{p_n}{q_n}\right| < \frac{2}{q_n^{n+1}}$
So
$\delta q_n^{n+1} < 2q_n^d$
As soon as n ≥ d, we get $10^{n!} = q_n \leq q_n^{n+1-d} < \frac{2}{\delta}\ for\ all\ n \geq d$
But $\frac{2}{\delta}$ is constant, while $10^{n!}$ is unbounded, so this is impossible.
Therefore, a is transcendental. ■

Can use this to show that
$\sum_{m=1}^{\infty} b^{-m!}$
is transcendental for any integer b≥ 2
Or
$\sum_{m=1}^{\infty} 2^{-2^m}$
Lots of transcendental numbers.

$e\ and\ \pi$ are transcendental

Arithmetic Modulo a Polynomial

November-17-10 1:09 PM

Modular Arithmetic for Integers

If a, b, m ∈ ℤ, m≥ 1 then
$a \equiv b \ (mod\ m) \Leftrightarrow m|(a-b)$

Modular Arithmetic for Polynomials

If F is a field, and g, h, f ∈ F[x], f ≠ 0, then

$g \equiv h \ (mod\ f)$ iff $f|(g-h)$

Theorem

If $a_1 \equiv a_2 \ (mod\ f)$ and $b_1 \equiv b_2 (mod\ f)$
$a_1, a_2, b_1, b_2, f \in F[x], f \neq 0$
Then

$a_1 + b_1 \equiv a_2 + b_2 \ (mod\ f)$
$a_1 b_1 \equiv a_2 b_2 \ (mod\ f)$

Congruence Classes for Polynomials

Define the congruence class of g mod f to be
$[g] = \{h \in F[x] such\ that\ h \equiv g \ (mod\ f)\}$

$[g] + [h] = [g + h]$
$[g][h] = [gh]$

Theorem

The set of congruence classes (mod f) under the operations is a commutative ring. 0 = [0], 1 = [1]

Observation

Working modulo f, deg(f) ≥ 1, every congruence class has a representative g with deg(g) < deg(f)

Notation

If F is a field, and f(x) ∈ F[x] has degree ≥ 1 then,
F[x]/(f) is the ring of congruence classes (mod f)

Examples

$x^3 + x + 1 \equiv x \ (mod\ x^3 + 1)$
$x^3 \equiv x \ (mod\ x^2 - 1)$
since $x^3 - x = x(x^2 - 1)$

With congruence classes:
Mod $x^3 - 1$
$[x^3] = [x]$
$[x^2 + 1] = [2]$

Congruence Class Properties

- $g \equiv g \ (mod\ f) for\ all\ g$
- g ≡ h (mod f) ⇔ $h \equiv g (mod\ f)$ for all g, h
- $g \equiv h \ (mod\ f) and\ h \equiv j \ (mod\ f) \Rightarrow g \equiv j \ (mod\ f)$

$[g] = [h] \Leftrightarrow g \equiv h \ (mod\ f)$

Operations on the Congruence Classes

Define:

$[g] + [h] = [g + h]$

Fact:
If $a_1 \equiv a_2 \ (mod\ f)$ and $b_1 \equiv b_2 \ (mod\ f)$ then $a_1 + b_1 \equiv a_2 + b_2 \ (mod\ f)$
So the definition for addition of congruence classes is well defined. No matter what representatives are chosen for [g] and [h], [g+h] will always be the same.

Define:

[g][h] = [gh]

Fact:
If $a_1 \equiv a_2 (mod\ f) and\ b_1 \equiv b_2 (mod\ f)\ then\ a_1 b_1 \equiv a_2 b_2 (mod\ f)$ so multiplication is well-defined.

So all of the properties of the congruence classes follow from the properties of the polynomials, so the congruence class under + and × is a commutative ring.

Example

F = ℚ,
$f(x) \in \mathbb{Q}[x] is\ x^2 + 1$
$[x-1][x+1] = [(x-1)(x+1)] = [x^2 - 1] = [-2]$

Observation

Working modulo f, deg(g) ≥ 1, every congruence class has a representative g with deg(g) < deg(f)

Proof

If $f(x) \in F[x]$, deg(f) ≥ 1 and $h(x) \in F[x]$, we can write $h(x) = f(x)q(x) + r(x), \deg(r) < \deg(f)$
$h \equiv r \ (mod\ f), [h] = [r]$

Example

$F = \mathbb{Z}_3, f(x) = x^2 + 1$
F[x]/(f) = $\mathbb{Z}_3/(x^2 + 1)$

Every congruence class has a representative of degree less than 2.
Polynomials in $\mathbb{Z}_3[x]$ with degree < 2:
$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$

The only congruence classes are $[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2]$

So $\mathbb{Z}_3[x]/(x^2 + 1) = \{[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2]\}$
Is this a field? Does every non-zero element have a multiplicative inverse?

$[1][1] = [1]$
$[2][2] = [4] = [1]$
$[x][2x] = [2x^2] = [-x^2] = [-x^2 + x^2 + 1] = [1]$
$[x+1][x+2] = [x^2 + 3x + 2] = [1]$
$[2x+1][2x+2] = [2][2][x+1][x+2] = [1][1] = [1]$

$\mathbb{Z}_3[x]/(x^2 + 1)$ is a field with 9 elements.
This is the first example of a finite field where the number of elements is not prime.

Finite Fields

November-19-10 1:07 PM

Theorem
If F is a field, and $f(x) \in F[x]$ and $\deg(f) \geq 1$ then $F[x]/(f)$ is a field if and only if $f(x)$ is irreducible.

Theorem
Let F be a field, and $f(x) \in F[x]$ an irreducible polynomial of degree ≥ 1. Then $F[x]/(f)$
1. Is a field
2. Contains a copy of F
3. Contains a root of f(x)

Proposition
Let p be a prime and $f(x) \in \mathbb{Z}_p$ an irreducible polynomial of degree d ≥ 1
Then $\mathbb{Z}_p[x]/(f)$ is a field with p^d elements.

Theorem
Fermat's Little Theorem for Finite Fields
If F is a field with n ($< \infty$) elements, and $a \in F$ is non-zero then $a^{n-1} = 1$

Corollary
If F is a finite field with n elements, then $(x^n - x)$ factors as:

$$\prod_{a \in F} (x - a)$$

What are the finite fields?

Ones we know: $\mathbb{Z}_p, \mathbb{Z}_3[x]/(x^2+1)$

Proof of Theorem
Suppose f(x) is not irreducible, then $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$,
$deg(g), deg(h) < deg(f)$
$[g], [h] \neq 0$ since $f \nmid g, h$
But $[g][h] = [gh] = [f] = 0$
If [g] had a multiplicative inverse, then $[g]^{-1}[g][h] = [0] \Rightarrow [h] = [0]$, a contradiction.
Therefore $F[x]/(f)$ is not a field.

Suppose $f(x)$ is irreducible, then for any $[g] \neq 0$, so $f \nmid g$. The only divisors of f are 1 and f so: $\gcd(f, g) = 1$
So we can choose polynomials $s, t \in F[x]$ with $sf + tg = 1$
By Bezout's Identity for Polynomials
$[1] = [sf + tg] = [tg] = [t][g]$
So $[g]^{-1} = [t]$ Since $[g] \neq 0$ was any element of $F[x]/(f)$, this is a field
■

Example
$x^2 + 1$ is irreducible in $\mathbb{Q}$[x], so $\mathbb{Q}[x]/(x^2+1)$ is a field
Can think of $\mathbb{Q}$ as being in this field since for every rational q $\in \mathbb{Q}$, $q \in \mathbb{Q}[x]/(x^2+1)$

If $[q_1] = [q_2], q_1, q_2 \in \mathbb{Q}$ then $(x^2+1) | (q_2 - q_1)$
$q_1 = q_2$ as rational numbers
So the function $q \to [q]$ is injective (one-to-one)

This field also contains a square root of -1
$[x]^2 = [x^2] = [-1]$
so $[x]$ is $\sqrt{-1}$

This field is "the same" as $\mathbb{Q}[i]$

Finite Fields
Proof of 2nd Theorem
1. Already done
2. We can define a function $g(a) = [a]$ from F to $F[x]/(f)$
   By definition, $g(a+b) = g(a) + g(b)$ and $g(ab) = g(a)g(b)$
   and g is one-to-one because if
   $g(a) = g(b), then\ [a] = [b]$ so $f(x) | (b - a)$. This is impossible unless b=a
   So g(a) take every F to a unique $F[x]/(f)$
3. $f([x]) = [f(x)] = 0, so\ [x]$ is a root of f(x) ■

Proof of Proposition
Every congruence class contains a unique polynomial $r(x)$ with $\deg(r) \leq d - 1$
If $r_1(x), r_2(x)$ have degree ≤ d-1 then if $[r_1] = [r_2]$, we have $f | (r_2 - r_1)$ then $\deg(f) > \deg(r_2 - r_1)$
So this is only possible if $r_2 = r_1$
The congruence classes are in one-to-one correspondence with the polynomials of degree ≤ d-1
The number of polynomials in $\mathbb{Z}_p[x]$ with degree ≤ d-1 is the number of sequences
$a_0, a_1, a_2, \ldots a_{d-1} \in \mathbb{Z}_p$
So there are p^d choices. ■

Proof of Fermat's Little Theorem for Finite Fields
Define $f : F \to F$ by $f(x) = ax$
$f(0) = 0$
f is one-to-one because if $f(x) = f(y)$, then
$ax = ay \Rightarrow a(x-y) = 0 \Rightarrow a^{-1}a(x-y) = a^{-1}0 \Rightarrow x - y = 0 \Rightarrow x = y$
f is onto, since for any $x \in F$, $f'(a^{-1}x) = x$
So

$$\prod_{\substack{x \in F \\ x \neq 0}} x = \prod_{\substack{x \in F \\ x \neq 0}} f(x) = \prod_{\substack{x \in F \\ x \neq 0}} ax = a^{n-1} \prod_{\substack{x \in F \\ x \neq 0}} x$$

$$\prod_{\substack{x \in F \\ x \neq 0}} x \neq 0$$

So $1 = a^{n-1}$ ■

Proof of Corollary
For each $a \in F$, either a = 0 so $a^n - a = 0^n - 0 = 0$
Or $a \neq 0, and$
$a^n - a = a(a^{n-1} - 1) = a \times 0 = 0$
So

$$\prod_{a \in F} (x - a) \mid x^n - x$$

But both have the same degree n so

$C\prod_{a\in F}(x-a)=(x^n-x)for\ some\ c\in F$

So c = 1 and

$x^n-x=\prod_{a\in F}(x-a)$

■

* Gaussian Integers $\mathbb{Z}[\sqrt{-1}]$

November-22-10 4:30 PM

$d > 0, \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{C}$
$S \subset R, R \text{ is a ring}$
S is a subring if

- closed under addition
- closed under additive inverses
- $0, 1, \in S$

$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}, a, b \in \mathbb{Z}\}$
$(a + b\sqrt{d}) + (e + f\sqrt{d}) = (a + e) + (b + f)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$
$(a + b\sqrt{d})(e + f\sqrt{d}) = (ae + bfd) + (af + be)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$
$(a + b\sqrt{d}) + (-a - b\sqrt{d}) = 0, (-a - b\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$
$(0 + 0\sqrt{d}), (1 + 0\sqrt{d}) \in \mathbb{Z}[d]$

The Gaussian integers are $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] = \{a + bi, a, b, \in \mathbb{Z}\}$
N is the norm function
$N : \mathbb{Z}[i] \to \mathbb{Z}^+$
$a + bi \to a^2 + b^2$

Units of $\mathbb{Z}[i]$

$\mathcal{U}(\mathbb{Z}[i]) = \{u \in \mathbb{Z}[i] | i \exists v \in \mathbb{Z}[i] \text{ such that } uv = 1\}$
$1 = N(uv) = N(u)N(v) \Rightarrow N(u) = 1$
$u = a + bi$
$a^2 + b^2 = 1$
$\Rightarrow a = \pm 1, b = 0$
$\Rightarrow a = 0, b = \pm 1$
So
$\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$

Lemma

$a, b \in \mathbb{Z}[i], a \neq 0$
Then there are elements $q, r \in \mathbb{Z}[i]$ such that $b = aq + r, 0 \leq N(r) < N(a)$
$\frac{b}{a} = \frac{b_1 + ib_2}{a_1 + ia_2} \times \frac{a_1 - ia_2}{a_1 - ia_2}$
So $\frac{b}{a} \in \mathbb{Q}[i]$
$\frac{b}{a} = u + iv, u, v \in \mathbb{Q}$
Pick $n, m \in \mathbb{Z}, |u - n| \leq \frac{1}{2}, |v - m| \leq \frac{1}{n}$
Let $q = n + im \in \mathbb{Z}[i]$

Verify $0 \leq N(x) < N(a)$
$N(x) = N(b - aq) = N\big(b - a(n - im)\big)$
$b = a(u + iv)$
$N(x) = N\big(a(u + iv - n - mi)\big) = N(a)\big((u - n)^2 + (v - m)^2\big) \leq \frac{N(a)}{2} < N(a)$

Theorem (Euclidean Algorithm)

$a, b \in \mathbb{Z}[i], a \neq 0 \neq b$
$\Rightarrow \exists\, d \in \mathbb{Z}[i], d|a, d|b$
$\exists s, t \text{ such that } d = as + bt = \gcd(a, b)$

$a = bq_1 + r_1, \quad 0 \leq N(r_1) < N(b)$
$b = r_1q_2 + r_2$
$r_1 = r_2q_3 + r_3, \{N(r_j)\}$ strictly decreasing $\subseteq \mathbb{Z} \geq 0$
$\Rightarrow \exists k \text{ such that } r_{k-1} = r_kq_{k+1} + 0 \Rightarrow d = r_k$
$r_j = asj + btj, sj, tj \in \mathbb{Z}[i]$
$d = as + bt$
$d|r_{k-1}, d|r_{k-2} \Rightarrow d|r_{k-3} \Rightarrow d|a, d|b$
$x|a, x|b \Rightarrow x|as + bt = d$

Exercise
Find $\gcd(-21 + 27i, -77 + 49i)$

Lemma

p prime in $\mathbb{Z}[\sqrt{-1}], p|ab \Rightarrow p|a \text{ or } p|b$

Theorem: Unique Factorization

$a \in \mathbb{Z}[i], a \neq 0$

$a = up, p_k = vq_1 \dots q_l, uv \in \mathcal{U}, p_1 \dots p_l$ are prime
$\Rightarrow k = l, \exists a\ permutation\ \pi\ such\ that\ p_i\ is\ associated\ to\ (backwards\ F)\pi(i)$
for $1 \leq i \leq k$

Are 2, 3 and 5 primes in $\mathbb{Z}[i]$?
$2 = (1+i)(1-i)$
$5 = (1+2i)(1-2i)$
3 is prime
$N(xy) = N(3) = 9$
$N(x) = 3$
$a^2 + b^2 = 3, impossible$

Characteristic of Finite Fields

November-24-10 12:32 PM

Characteristic

The characteristic of a field is the smallest m > 0 such that
1+1+…+1=0
m times
or 0 if there is no such m.

Lemma

Let F be a field of characteristic m ≠ 0. Then m is prime.
(If you think F = {0} is a field, then characteristic 1 is also possible, but for us F = {0} is not a field.)

Theorem

Let F be a finite field of characteristic p.

1. p ≠ 0 is prime
2. $\#F = p^d$ for some d ≥ 1

The Characteristic of a (finite) field.

Every field F contains a multiplicative identity "1".
1, 1+1, 1+1+1, …
If F is finite, eventually this sequence repeats. So for some m ≠ n
1+1+1+…+1=1+1+…+1
m times n times
1+1+…+1=0
m-n times

Example

$\mathbb{Q}$ has characteristic 0
$\mathbb{Z}_p$ has characteristic p
because $1 + 1 + 1 + \cdots + 1 \equiv m \ (mod\ p)$
m times
m = p is the smallest integer m > 0 such that m ≡ 0 mod p

Proof of Lemma

Suppose $m = jk,\ 1 < j, k < m$
$(1 + 1 + \cdots + 1)(1 + 1 + \cdots + 1) = 1 + 1 + \cdots + 1 = 0$
j times k times j*k = m times
So either
$(1 + 1 + \cdots + 1) = 0\ or\ (1 + 1 + \cdots + 1) = 0$
j times k times

But j, k < m and m was the smallest number of "1"s whose sum was 0
Contradiction, so m is prime. ■

So every finite field has some prime characteristic p. We'll relate these to $\mathbb{Z}_p$. You can think of $\mathbb{Z}_p$ as being inside any field of characteristic p.

Ex: $\mathbb{Z}_3[x]/(x^2 + 1)$ "contains" $\mathbb{Z}_3$: {[0], [1], [2]}

If F has characteristic p ≠ 0, then
"1" = 1
"2" = 1+1
"3" = 1+1+1
"p-1" = $1 + \cdots + 1\ (p - 1\ times)$
"p" = 0

Proof of Theorem

1. is already done
2.
Construct a finite sequence $a_1, \ldots a_d \in F$ as follows:
$a_1 = 1$
If $F = \{1, 2, 3, \ldots p - 1, 0\}$, then stop.
In this case, every element of F has the form $m_1 a_1$, for some $m_1 \in \{0, 1, 2, \ldots, p - 1\}$

If this is not true, choose some a_2 which cannot be written in the form $m_1 a_1$ for $m_1 \in \{0, 1, 2, \ldots, p - 1\}$
If every element of F can be written in the from $m_1 a_1 + m_2 a_2, m_i = \{0, 1, \ldots, p - 1\}$ then stop.
Otherwise, choose a_3 not of this form.
Eventually we get $a_1, a_2, \ldots a_d \in F$
such that everything in F has the form
$$\sum_{i=1}^{d} m_i a_i\ , m_i = \{0, 1, \ldots, p - 1\}$$
And for each j, a_j cannot be represented in the form $\sum_{i=1}^{j-1} m_i a_i$
In fact, the representation of an element of F in the form
$$\sum_{i=1}^{d} m_i a_i$$
is unique.
If not, then there are some $m_i \in \{0, 1, 2, \ldots, p - 1\}$ and $n_i \in \{0, 1, 2, \ldots, p - 1\}$ such that
$$\sum_{i=1}^{d} m_i a_i = \sum_{i=1}^{d} n_i a_i$$
With $m_i \neq n_i$ for at least one i.
Let j be the largest value so that $m_j \neq n_j$
Then
$$\sum_{i=1}^{d} (m_i - n_i) a_i = 0$$
$$\sum_{i=1}^{j} (m_i - n_i) a_i = 0$$
$$-(m_j - n_j) a_j = \sum_{i=1}^{j-1} (m_i - n_i) a_i$$
Since $(m_j - n_j) \neq 0$, there is some $b \in \{1, 2, \ldots, p_1\}$ such that
$b\left(-(m_j - n_j)\right) = 1$
Then multiplying both sides by b,

$$a_j = \sum_{i=1}^{j-1} b(m_i - n_i)a_i\,, \qquad b(m_i - n_i) \in \{0, 1, \dots, p-1\}$$
This is impossible, by construction.

So if
$$\sum_{i=1}^{d} m_i a_i = \sum_{i=1}^{d} n_i a_i$$
then $m_i = n_i\ \forall i$

So every element of F can be written in one and only one way as
$$\sum_{i=1}^{d} m_i a_i\,, \qquad m_i \in \{0, 1, 2, \dots, p-1\}$$
So the number of elements in F is the same as the number of different sequences: $m_1, \dots m_d$ with $m_i \in \{0, 1, 2, \dots, p-1\}$
So
$\#F = p^d$
■

If F is a finite field, then #F is a prime power.

Primitive Roots

November-26-10 12:30 PM

Theorem - Primitive Roots

If F is a finite field with n elements, then there is some $a \in F$, a ≠ 0 such that
$F = \{0, a, a^2, a^3, \ldots a^{n-1}\}$
a is a "primitive root" for the field F

Order

If a ∈ F, a ≠ 0, define the order of a by
$ord(a) = \min\{e \geq 1 : a^e = 1\}$

If $1 \leq i, j \leq ord(a), and\ i \neq j\ then$
$a^i \neq a^j$

Example - Primitive roots

If $F = \mathbb{Z}_5$
2 is a primitive root
$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1$

Proof of Order statement

If $j > i$, then
$a^j = a^i \Rightarrow a^{j-i} = 1$
But $j - i \geq 1$ and $j - i < ord(a) = \min\{e \geq 1: a^e = 1\}$
So $a^j = a^i$ causes a contradiction, so $a^j \neq a^i$

So $\{a, a^2, a^3, \ldots, a^{ord(a)}\}$
are all distinct

a is a primitive root ⇔ ord(a) = n-1
(ord(a) ≤ n-1 by Fermat's little theorem)

Proof of Primitive Roots Theorem

Let $f(e) = \#\ of\ elements\ in\ F\ of\ order\ e$

First, notice that $a^d - 1 = 0$ iff $ord(a)|d$
This is true because if $d = ord(a) \times m$ then $a^d - 1 = a^{ord(a)\times m} - 1 = \left(a^{ord(a)}\right)^m - 1 = 1^m - 1 = 0$
Now assume $a^d - 1 = 0$
We can find integers s, t such that $\gcd(ord(a), d) = s \times ord\ (a) + t \times d$
$a^{\gcd(ord(a),d)} = a^{s\times ord(a)+t\times d} = \left(a^{ord(a)}\right)^s \times \left(a^d\right)^t = 1$
By definition, $ord(a) \leq \gcd(ord(a), d) \leq ord(a)$
$So\ \gcd(ord(a), d) = ord(a) \Rightarrow ord(a)|d$

Things with order dividing d ⇔ roots of $x^d - 1$

How many roots does $X^d - 1$ have in F? When $d|n - 1$

Every non-zero element of F satisfies
$a^{n-1} - 1 = 0$
So $X^{n-1} - 1 = 0$ has n -1 roots in F

$X^d - 1 | X^{n-1} - 1$
For any m,
$X^m - 1 = (X - 1)(X^{m-1} + X^{m-2} + \cdots + 1)$
If $n - 1 = dm, then$
$X^{n-1} - 1 = \left(X^d - 1\right)\left(X^{d(m-1)} + X^{d(m-2)} + \cdots + 1\right)$
# of roots is ≤ d(m-1)
$X^{n-1} - 1$ has exactly n-1 roots

$dm = \left(\#roots\ of\ X^d - 1\right) + (something \leq dm - d)$
exactly d, since ≤ d and ≥ d
There are exactly d elements of F with order dividing d (if d | n-1)

This means that for all d|n-1

$$\sum_{(e|d)} f(e) = d$$

Claim:

For each $d|n - 1$, $f(d) = \varphi(d)$
We know that for any d,

$$\sum_{(e|d)} \varphi(e) = d$$

Proof

$f(1) = 1, since$
$a^1 - 1 = 0 \Leftrightarrow a = 1$
$\varphi(1) = 1$, so it's true that $\varphi(1) = f(a)$

Now, assume that
$f(e) = \varphi(e)$ for all $e|(n - 1)$ with e < d.
Then

$$\sum_{(e|d)} f(e) = d = \sum_{(e|d)} \varphi(e)$$

$$\varphi(d) + \sum_{\substack{e|d \\ e<d}} \varphi(e) = f(d) + \sum_{\substack{(e|d) \\ e<d}} f(e) = d$$

By the induction hypothesis:

$$\sum_{\substack{(e|d) \\ e<d}} \varphi(e) = \sum_{\substack{(e|d) \\ e<d}} f(e)$$

$So\ \varphi(d) = f(d)\ \forall$ d|n-1
So there are $\varphi(n - 1) \geq 1$ elements of order n-1 ■

(In fact, $\varphi(n-1)$ is usually almost as big as n-1)

Isomorphism of Fields

November-29-10 12:33 PM

Isomorphism

If F_1 and F_2 are fields, then an isomorphism is a function
$f: F_1 \to F_2$

1. f is a bijection
2. $f(x+y) = f(x) + f(y)\ \forall x, y$
   $f(xy) = f(x)f(y)$
   $f(0) = 0$
   $f(1) = 1$

Isomorphic

We say that F_1 and F_2 are iff there exists an isomorphism $f: F_1 \to F_2$

Isomorphism as an Equivalence Relation

Isomorphism is an equivalence relation so:

1. for any field F, F is isomorphic to itself (the isomorphism is f(x) = x)
2. if $f: F_1 \to F_2$ is an isomorphism, then $f^{-1}: F_2 \to F_1$ is an isomorphism. So the property is symmetric.
3. If F_1 and F_2 are isomorphic, and F_2 and F_3 are isomorphic, then F_1 and F_3 are isomorphic.

Example

$F_1 = \mathbb{Z}_2$

+	**0**	**1**
0	0	1
1	1	0

×	**0**	**1**
0	0	0
1	0	1

If F_2 is isomorphic to $\mathbb{Z}_2$ that means that $F_2 = \{a, b\}$
$a = f(0)$
$b = f(1)$

+	**a**	**b**
a	a	b
b	b	a

×	**a**	**b**
a	a	a
a	a	b

"Isomorphic" = same fields, but elements have different names

Every finite field has p^d elements, for some prime p and some d ≥ 1

Claim:

If $\#F_1 = \#F_2$, then F_1 and F_2 are isomorphic.

Example:

Let $F_1 = \mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$
And let $F_2 = \mathbb{Q}[x]/(x^2+1)$
Then F_1 and F_2 are isomorphic
Define $f: F_2 \to F_1$ as follows:
$f([g]) = g(i)$
Is this well defined? THIS IS MADNESS
No… THIS IS ALGEBRA!

If $[g_1] = [g_2]$ then, by definition,
$g_1(x) = g_2(x) + (x^2+1)h(x)$
So $g_1(i) = g_2(i) + (i^2+1)h(i) = g_2(i)$
So it is well defined

Every congruence class has a representative of degree ≤ 1
Every element of $\mathbb{Q}[x]/(x^2+1)$ is of the form $[a+bx]$, for $a, b \in \mathbb{Q}$
$f([a+bx]) = a + bi, so\ f: F_2 \to F_1$
This also shows that f is onto since for any $a + bi \in F_1, a + bi = f([a+bx])$
Also, f is one-to-one. Suppose that $f([g_1]) = f([g_2])$
Then $g_1(i) = g_2(i)$, so i is a root of $g_1(x) - g_2(x)$.
Since x^2+1 is irreducible and $i^2 + 1 = 0$, we must have
$x^2 + 1 | g_1(x) - g_2(x)$
So $[g_1] = [g_2]$
f is one-to-one and onto

$f([a+bx] + [c+dx]) = f([(a+c) + (b+d)x]) = (a+c) + (b+d)i$
$f([a+bx]) + f([c+dx]) = a + bi + c + di = (a+c) + (b+d)i$
$f([a+bx])f([c+dx]) = (a+bi)(c+di) = ac + (bc+da)i + bdi^2 = (ac - bd) + (bc+da)i$
$f([a+bx][c+dx]) = f([(a+bx)(c+dx)]) = f([ac + (bc+ad)x + x^2])$
$[bdx^2] = [-bd]$ because $x^2 + 1 | bdx^2 + bd$
$f([a+bx][c+dx]) = f([(ac-bd) + (bc+da)x]) = (ac-bd) + (bc+da)i$

So F_1 and F_2 are isomorphic

F_2: things of the form [a+bx] with a, b ∈ $\mathbb{Q}$ and $[x]^2 = -1$
F_1: things of the form a+bi with $a, b \in \mathbb{Q}$ and $i^2 = -1$

Uniqueness of Fields

We're going to show that, up to this equivalence relation of isomorphism, there is exactly one field with p^d elements, for each prime p and d ≥ 1

*Prime Gaussian Integers

November-29-10 4:31 PM

$\mathbb{Z}[i] = \{a + bi \;\; a, b \in \mathbb{Z}\}$
$N(a + bi) = a^2 + b^2$

Theorem

Let p be an odd prime integer. TFAE (the following are equivalent)

1. $p \equiv 1(mod\ 4)$
2. $x^2 + 1 \equiv 0\ (mod\ p)$ has a solution
3. $\exists n, m \in \mathbb{Z}, p \nmid n, p \nmid m \;/\; p|n^2 + m^2$
4. $p = a^2 + b^2$
5. $p = (a + ib)(a - ib)\ in\ \mathbb{Z}[x]$

Wilson's Theorem

p prime, then $(p-1)! \equiv -1\ (mod\ p)$

Theorem

The primes in $\mathbb{Z}[i]$ are:

1. The elements of prime order: the primes $\pm 1 \pm$i of norm 2 and x such that N(x)=p, p prime in $\mathbb{Z}$, $p \equiv 1\ (mod\ 4)$
2. The elements $\pm$p, $\pm$ ip , p prime integer and $p \equiv 3\ (mod\ 4)$

Proof of Theorem

1⇒2
RTP: $x^2 \equiv -1\ (mod\ p)$
$p = 1 + 4n, x = (2n)!$
$(4n)! = (p-1)! = -1\ (mod\ p)$

$$(4n!) = \prod_{j=1}^{2n} j(4n + 1 - j) = (4n)(2(4n-1))(3(4n-2)\ldots(2n(4n+1-2n))$$

$$\prod_{j=1}^{2n} j(4n + 1 - j) \equiv \left(\prod_{j=1}^{2n} j\right)\left(\prod_{j=1}^{2n} -j\right)(-1)^{2n} = [(2n)!]^2$$

2⇒3
$\exists n \;/\; n^2 + 1 \equiv 0\ (mod\ p)$ Let m = 1 then $p|n^2 + m^2$
3⇒4
$p|n^2 + m^2 = (n + im)(n - im)$
Suppose p is prime in $\mathbb{Z}[i] \Rightarrow p|n + im$ or $p|n - im$
Claim $p|n$ and $p|m$
$p(x + iy) = n + im \Rightarrow px = n, py = m$

Then p is not prime in $\mathbb{Z}[i]$
$\exists x \in \mathbb{Z}[i]$, x is not a unit, not p. x|p
$\Rightarrow N(x)|N(p) = p^2 \Rightarrow N(x) = p$
$x = a + ib \Rightarrow N(x) = a^2 + b^2 = p$
5⇔4
4⇒1
$n^2 = 0, 1\ (mod\ 4)$

$$p = a^2 + b^2 \equiv \begin{cases} 0 \\ 1\ (mod\ 4) \\ 2 \end{cases}$$

But p is odd so $p\,! \equiv 0, 2\ (mod\ 4)$

Proof of Theorem

1. N(x) is prime ⇒ x is prime
   For N(x) to be prime, $x \neq a \in \mathbb{Z}$ or $x \neq ib \in i\mathbb{Z}$
   $\Rightarrow x = a + ib, a, b$ are not both even
   $p = N(x) = a^2 + b^2 \Rightarrow p \equiv \begin{cases} 1 \\ 2 \end{cases} (mod\ 4)$
   $p \equiv 1\ (mod\ 4)$
   $p \equiv 2\ (mod\ 4) \Rightarrow N(x) = 2 \Rightarrow x = \pm 1 \pm i$
2. Suppose p $\in \mathbb{Z}$, prime $p \equiv 3\ (mod\ 4)$
   Suppose p is not prime in $\mathbb{Z}[i] \Rightarrow \; p = xy$
   $p^2 = N(p) = N(x)N(y) \Rightarrow N(x), N(y) = p = a^2 + b^2$
   So $p\,! \equiv 3\ (mod\ p)$ a contradiction
   ⇒ p is prime in $\mathbb{Z}[i]$ and so are its associates -p, $\pm$ ip

And the primes from (1) and (2) are the only ones in $\mathbb{Z}[i]$
Let $x = n + im$ prime in $\mathbb{Z}[i]$
$\Rightarrow x^{\sim} = n - im$ primes as well

$N(x) = xx^{\sim}$ either prime in $\mathbb{Z} \rightarrow 1$ or not prime in $\mathbb{Z}$
$xx^{\sim} = pq$
$xx^{\sim}$ is the product of two primes and $\mathbb{Z}[i]$ has unique factorization so p and q are prime
x = up ⇒ $x^{\sim} = u^{\sim}p$
$x^{\sim} = vq$
For u, v units
$u^{\sim}p = vq \Rightarrow p = u^{\sim -1}vq \Rightarrow p = q$
$x = \pm p\ or\ x = \pm ip$

Want to see that $p \equiv 3\ (mod\ 4)$
If $p \equiv 1\ (mod\ 4) \Rightarrow then\ p\ is\ not\ prime\ in\ \mathbb{Z}[i]$
$p\,! \equiv 0\ (mod\ 4) p\ prime$
$p\,! \equiv 2\ (mod\ 4) p = 2\ case\ 1$

Uniqueness of Fields

December-01-10 12:31 PM

Theorem 6.2

Let F be a finite field with p^d elements.
For some polynomials $\mathbb{Q}[x] \in \mathbb{Z}_p[x]$, with deg(q) = d, F is isomorphic to $\mathbb{Z}_p[x]/(q)$

Corollary

If F_1 and F_2 are finite fields, and $\#F_1 = \#F_2$, then F_1 and F_2 are isomorphic.

Proof

F has a primitive root a ∈ F, so
$F = \left\{0, a^1, a^2, a^3, \dots, a^{p^d-1}\right\}$
also know that F contains a "copy" of $\mathbb{Z}_p$, $\{0, 1, 2, \dots, p-1\} \subseteq F$

We know that a ∈ F is a root of $x^{p^d} - x = 0$ (even, $x^{p^d} - 1$)
So there is some $q(x) \in \mathbb{Z}_p[x]$ with $q(x) | x^{p^d} - x$ and $q(a) = 0$
$q(x)$ monic and irreducible
(q is a monic factor of $x^{p^d} - x$ such that a is a root of q)

$\mathbb{Z}_p[x]/(q)$ is a field
Define a function $f: \mathbb{Z}_p[x]/(q) \to F$ by $f([g]) = g(a)$

This is well defined because if $[g_1] = [g_2]$, $g_{1(x)} - g_2(x) = q(x)h(x)$ for some $h(x) \in \mathbb{Z}_p[x]$
$So\ g_1(a) = g_2(a) + q(a)h(a)$, but $q(a) = 0$ so $g_1(a) = g_2(a)$
So $f([g_1]) = f([g_2])$ and f is well-defined.

It's also true that f is one-to-one. Suppose that $f([g_1]) = f([g_2])$
Then $g_1(a) = g_2(a)$, so $g_1(a) - g_2(a) = 0$
So $g_1(x) - g_2(x) \in \mathbb{Z}_p[x]$ has a root at x = a, so $q(x) | g_1(x) - g_2(x)$
That means $[g_1] = [g_2]$
We've shown that $f: \mathbb{Z}_p[x]/(q) \to F$ is one-to-one

Why is f onto?
$f([0]) = 0$
Also, for any integer k≥ 1
$f([x^k]) = a^k$
$F = \left\{0, a_1, a_2, \dots, a^{p^d-1}\right\}, so\ f\ is\ onto$

Check addition and multiplication
$f([g_1] + [g_2]) = f([g_1 + g_2]) = (g_1 + g_2)(a) = g_1(a) + g_2(a)$
$f([g_1]) + f([g_2]) = g_1(a) + g_2(a)$
So $f([g_1] + [g_2]) = f([g_1]) + f([g_2])$ for any $[g_1], [g_2] \in \mathbb{Z}_p[x]/q$

$f([g_1][g_2]) = f([g_1 \times g_2]) = (g_1 \times g_2)(a) = g_1(a) \times g_2(a)$
$f([g_1]) \times f([g_2]) = g_1(a) \times g_2(a)$
So $f([g_2][g_1]) = f([g_1]) \times f([g_2])$ for any $[g_1], [g_2] \in \mathbb{Z}_p[x]/q$
$f([0]) = 0, f([1]) = 1$

So $f: \mathbb{Z}_p[x]/q \to F$ is an isomorphism

F has p^d elements and $\mathbb{Z}_p[x]/(q)$ has $p^{deq(q)}$ elements
So the isomorphism between $p^d and\ \mathbb{Z}_p[x]/(q)$ is one-to-one and onto so $\deg(q) = d$
■

Proof of Corollary

We know that there is some prime p and some $d \geq 1$ with
$\#F_1 = \#F_2 = p^d$
F_1 is isomorphic to $\mathbb{Z}_p[x]/(q)$ for some monic, irreducible $q(x) \in \mathbb{Z}_p[x]$ dividing $x^{p^d} - x$,
$\deg(q) = d$
Write $x^{p^d} - x = q(x)h(x)$ in $\mathbb{Z}_p[x]$

Now, every element of F_2 is a root of $x^{p^d} - x$, so this has p^d roots in F_2
$\deg(h) = p^d - d$, so h(x) has no more than $p^d - d$ roots in F_2
So $q(x)$ at least $d \geq 1$ roots in F_2

Define $f: \mathbb{Z}_p[x]/(q) \to F_2$ by $f([g]) = g(b)$, where b is a root of $q(x)$ in F_2
All of the steps to show that f is well-defined, one-to-one, and that addition and multiplication work are the same.

Need to show that f is onto.
$f: \mathbb{Z}[x]/(q) \to F_2$ is one-to-one, and the two sets have the same number of elements so f is onto.

Therefore, f is an isomorphism and it follows that $\mathbb{Z}_p[x]/(q), F_2, F_1$ are all isomorphic.
■

Finite Fields and Cryptography

December-03-10 12:32 PM

Summary

If F is a finite field, then #F $= p^d$ for some prime p, and some integer d ≥ 1

If #F $= p^d$ then F can be constructed as $\mathbb{Z}_p[x]/(q)$ for some irreducible $q(x) \in \mathbb{Z}_p[x]$

Any two finite fields of the same size are isomorphic.

Need to know that there is at least one field of size p^d for each p and each d.

True, but no time to prove - in the notes

Then for every p prime and every d ≥ 1, there is a unique (up to isomorphism) field with p^d elements. Then the field with p^d elements is written as $\mathbb{F}_{p^d}$ or $GF(p^d)$

If $\deg(q) = d$ and $q \in \mathbb{Z}_p[x]$ is irreducible, then $\mathbb{Z}_p[x]/(q)$ is a field with p^d elements.
Need to show that $\mathbb{Z}_p[x]$ contains irreducible polynomials of every degree.

It is not obvious, for example, in $\mathbb{R}[x]$ it is not true that there are irreducible polynomials of every degree. There are none of degree 3, for example.

Application of Finite Fields - Cryptography

Diffie-Hellman Key Exchange

Diffie- Hellman key exchange can be done with any finite field.
Alice and Bob want to generate a common secret.

Alice and Bob choose a finite field F and an element g ∈ F (preferably a primitive root)
Alice chooses a, and publishes g^a
Bob chooses b, and publishes g^b
Both know g^{ab}

What makes it hard for other people to find g^{ab}?

Finite Field Discrete Logarithm Problem (FFDLP):

Given g and h in a finite field, solve $h = g^a$ for a, if possible.

FFDLP is thought to be hard.

But why bother with finite fields when integers modulo a prime work?

- It's easy to write computer programs to do computation in $\mathbb{F}_{2^n}$
- More choices

* ElGamal Public Key

Alice want to create a public key
Alice chooses a finite field F, and a primitive root $a \in F$ and some k ≥ 1. She computes $b = a^k$ and publishes F, a, and b. Alice can easily compute a^k through successive squaring.

If Bob wants to send the message $m \in F$, Bob chooses r ≥ 1 and sends $e_1 = a^r$ and $e_2 = mb^r$

Alice computes $e_1^{-k} e_2 = a^{-rk} \times m \times a^{rk} = m$

For Eve to find k, Eve needs to solve the FFDLP