Algebraic algorithms

Freely using the textbook: Victor Shoup's "A Computational Introduction to Number Theory and Algebra"

Péter Gács

Computer Science Department
Boston University

Fall 2005

The class structure

See the course homepage.

Mathematical preliminaries
Logic

Logical operations: $\wedge$, $\neg$, $\vee$, $\Rightarrow$, $\Leftrightarrow$. $\forall$, $\exists$.

Example

x divides y, or y is divisible by x: $x|y \Leftrightarrow \exists z(x * z = y)$.

Sets

Notation: $\{2, 3, 5\}$. $x \in A$. The empty set.
Some important sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Example

x divides y more precisely: $x|y \Leftrightarrow \exists z \in \mathbb{Z}(x * z = y)$.

Set notation using conditions:

$$\{\, x \in \mathbb{Z} : 3|x \,\} = \{\, 3x : x \in \mathbb{Z} \,\}.$$

Note that x has a different role on the left-hand side and on the right-hand side. The x in this notation is a bound variable: its meaning is unrelated to everything outside the braces.

Example

Composite numbers: $\{\, xy : x, y \in \mathbb{Z} \setminus \{-1, 1\} \,\}$.

$A \subseteq B$, $A \subset B$ will mean the same! Proper subset: $A \subsetneq B$.
Set operations: $A \cup B$, $A \cap B$, $A \setminus B$. Disjoint sets: $A \cap B = \emptyset$.
The set of all subsets of a set A is denoted by 2^A.

Functions

The notation $f : A \to B$.

Example

$g(x) = 1/(x^2 - 1)$. It maps from $\mathbb{R} \setminus \{-1, 1\}$, to $\mathbb{R}$, so

$$g : \mathbb{R} \setminus \{-1, 1\} \to \mathbb{R}. \tag{1}$$

$\text{Domain}(g) = \mathbb{R} \setminus \{-1, 1\}$.

In general,

$$\text{Range}(f) = \{ f(x) : x \in \text{Domain}(f) \}.$$

In the example,

$$\text{Range}(g) = (-\infty, -1] \cup (0, \infty) = \mathbb{R} \setminus (-1, 0].$$

Note that $(0, \infty)$ is an open interval.

We could write $g : \mathbb{R} \setminus \{-1, 1\} \to \mathbb{R} \setminus (-1, 0)$, but (1) is correct, too: it says that g is a function mapping from $\mathbb{R} \setminus \{-1, 1\}$ into $\mathbb{R}$. On the other hand, g is mapping onto $\mathbb{R} \setminus (-1, 0)$. An “onto” function is also called surjective.

Injective and surjective

A function is one-to-one (injective) if $f(x) = f(y)$ implies $x = y$.

Theorem

If a set A is finite then a function $f : A \to A$ is onto if and only if it is one-to-one.

The proof is left for exercise.
The theorem is false for infinite A.

Example

A one-to-one function that is not onto: the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 2x$.
An onto function that is not one-to-one: exercise.

We will also use the notation

$$x \mapsto 2x$$

to denote this function. (The $\mapsto$ notation is similar to the lambda notation used in the logic of programming languages.)
A function is called invertible if it is onto and one-to-one. For an invertible function $f : A \to B$, the inverse function $f^{-1} : B \to A$ is always defined uniquely: $f_{-1}(b) = a$ if and only if $f(a) = b$.
An invertible function $f : A \to A$ is also called a permutation.

Tuples

Ordered pair (x, y), unordered pair $\{x, y\}$. (The (x, y) notation conflicts with the same notation for open intervals. So, sometimes $\langle x, y\rangle$ is used.) The Cartesian product

$$A \times B = \{\, (x, y) : x \in A, y \in B \,\}.$$

A function of two arguments: we will use the notation

$$f : A \times B \to C$$

when $f(x, y) \in C$ for $x \in A$, $y \in B$. Indeed, f can be regarded as a one-argument function of the ordered pair (x, y).
Ordered triple, and so on. Sequence $(x_1, \dots, x_n)$.

Inverse image

For a function $f : A \to B$, and a set $C \subseteq A$ we will write

$$f(C) = \{ f(x) : x \in A \}.$$

Thus, $\text{Range}(f) = f(A)$.
Example: $2\mathbb{Z}$ is the set of even numbers.
For $D \in B$, we will write

$$f^{-1}(D) = \{ x : f(x) \in D \}.$$

Note that this makes sense even if the function is not invertible.
However, $f^{-1}(D)$ is always a set, and it may be empty.

Example

If $f : \mathbb{Z} \to \mathbb{Z}$ is the function with $f(x) = 2\lfloor x/2 \rfloor$ then $f^{-1}(0) = \{0, 1\}$, $f^{-1}(\{1\}) = \emptyset = \{\}$, $f^{-1}(2) = \{2, 3\}$, $f^{-1}(\{3\}) = \emptyset$, and so on.

Partitions

A partition of a set A is a finite sequence $(A_1, \dots, A_n)$ of pairwise disjoint subsets of A such that $A_1 \cup \cdots \cup A_n = A$. Given any function $f : A \to \{1, \dots, n\}$, it gives rise to a partition $(f^{-1}(\{1\}), \dots, f^{-1}(\{n\}))$. And every partition defines such a function.

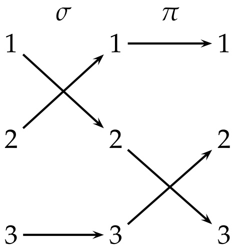
We will also talk about infinite partitions. A partition in this case is a function $p : B \to 2^A$ such that $\bigcup_{b \in B} p(b) = A$ and for $b \neq c$ we have $p(b) \cap p(c) = \emptyset$.

Operations

Functions are sometimes are also called operations. Especially, functions of the form $f : A \to A$ or $g : A \times A \to A$. For example, $(x, y) \mapsto x + y$ for $x, y \in \mathbb{R}$ is the addition operation.

Associativity. Example: functions $f : A \to A$, with the compositon operation.

Commutativity. Same example, say the permutations σ, π over $\{1, 2, 3\}$ on the right do not commute.



Distributivity. Examples: $*$ through $+$, further $\cap$ though $\cup$ and $\cup$ through $\cap$.

Relations

A binary relation is a set $R \subseteq A \times B$. We will write $(x, y) \in R$ also as $R(x, y)$ (with Boolean value). Thus

$$R(x, y) \Leftrightarrow (x, y) \in R.$$

Frequently, infix notation. Example: $x < y$, where $< \subset \mathbb{R} \times \mathbb{R}$.
Ternary relation: $R \in A \times B \times C$.
Interesting properties of binary relations over a set A.
Reflexive.
Symmetric.
Transitive.
A binary relation can be represented by a graph. If the relation is symmetric the graph can be undirected, otherwise it must be directed. In all cases, at most one edge can be between nodes.

Equivalence relation

Equivalence relation over a set A: reflexive, symmetric transitive.
Example: equality. Other example: reachability in a graph.

Theorem

A relation $R \subset A \times A$ is an equivalence relation if and only if there is a function $f : A \to B$ such that $R(x, y) \Leftrightarrow f(x) = f(y)$.

Proof: exercise.
Each set of the form $C_x = \{ y : R(x, y) \}$ is called an equivalence class.
An equivalence relation partitions the underlying set into the equivalence classes.
In a partition into equivalence classes, we frequently pick a representative in each class. Example: rays and unit vectors.

Preorder, partial order

A relation $\leqslant$ is antisymmetric if $a \leqslant b$ and $b \leqslant a$ implies $a = b$.
Preorder $\leqslant$: reflexive, transitive.
A preorder is a partial order if it is antisymmetric. Simplest example: $\leqslant$ among real numbers.

Example

The relation $\subseteq$ among subsets of a set A is a partial order.

In a preorder, we can introduce a relation $\sim$: $x \sim y$ if $x \leqslant y$ and $y \leqslant x$. This is an equivalence relation, and the relation induced by $\leqslant$ on the equivalence classes is a partial order.

Example

The relation $x|y$ over the set $\mathbb{Z}$ of integers is a preorder. For every integer x, its equivalence class is $\{x, -x\}$.

Asymptotic analysis

$O(), o(), \Omega(), \Theta()$. More notation: $f(n) \ll g(n)$ for $f(n) = o(g(n))$, $f(n) \overset{*}{<} g(n)$ for $f(n) = O(g(n))$ and $\overset{*}{=}$ for ($\overset{*}{<}$ and $\overset{*}{>}$).
The relation $\overset{*}{<}$ is a preorder. On the equivalence classes of $\overset{*}{=}$ it turns into a partial order.
The most important function classes: log, logpower, linear, power, exponential. These are not all equivalence classes under $\overset{*}{=}$.

Some simplification rules

- Addition: take the maximum. Do this always to simplify expressions. *Warning*: do it only if the number of terms is constant!
- An expression $f(n)^{g(n)}$ is generally worth rewriting as $2^{g(n)\log f(n)}$. For example, $n^{\log n} = 2^{(\log n)\cdot(\log n)} = 2^{\log^2 n}$.
- But sometimes we make the reverse transformation:

$$3^{\log n} = 2^{(\log n)\cdot(\log 3)} = (2^{\log n})^{\log 3} = n^{\log 3}.$$

The last form is easiest to understand, showing n to a constant power $\log 3$.

Examples

$$n/\log\log n + \log^2 n \stackrel{*}{=} n/\log\log n.$$

Indeed, $\log\log n \ll \log n \ll n^{1/2}$, hence $n/\log\log n \gg n^{1/2} \gg \log^2 n$.

Order the following functions by growth rate:

$$\begin{aligned}
& n^2 - 3\log\log n && \stackrel{*}{=} n^2, \\
& \log n/n, && \\
& \log\log n, && \\
& n\log^2 n, && \\
& 3 + 1/n && \stackrel{*}{=} 1, \\
& \sqrt{(5n)}/2^n, && \\
& (1.2)^{n-1} + \sqrt{n} + \log n && \stackrel{*}{=} (1.2)^n.
\end{aligned}$$

Solution:

$$\begin{aligned}
\sqrt{(5n)}/2^n \ll \log n/n \ll 1 \ll \log\log n \\
\ll n/\log\log n \ll n\log^2 n \ll n^2 \ll (1.2)^n.
\end{aligned}$$

Sums: the art of simplification

Arithmetic series.
Geometric series: its rate of growth is equal to the rate of growth of its largest term.

Example

$$\log n! = \log 2 + \log 3 + \cdots + \log n = \Theta(n \log n).$$

Indeed, upper bound: $\log n! < n \log n$.
Lower bound:

$$\begin{aligned} \log n! &> \log(n/2) + \log(n/2+1) + \cdots + \log n > (n/2)\log(n/2) \\ &= (n/2)(\log n - 1) = (1/2)n \log n - n/2. \end{aligned}$$

Examples

Prove the following, via rough estimates:

- $1 + 2^3 + 3^3 + \cdots + n^3 = \Theta(n^4)$.
- $1/3 + 2/3^2 + 3/3^3 + 4/3^4 + \cdots < \infty$.

Example

$$1 + 1/2 + 1/3 + \cdots + 1/n = \Theta(\log n).$$

Indeed, for $n = 2^{k-1}$, upper bound:

$$1 + 1/2 + 1/2 + 1/4 + 1/4 + 1/4 + 1/4 + 1/8 + \dots$$
$$= 1 + 1 + \cdots + 1 \text{ (} k \text{ times)}.$$

Lower bound:

$$1/2 + 1/4 + 1/4 + 1/8 + 1/8 + 1/8 + 1/8 + 1/16 + \dots$$
$$= 1/2 + 1/2 + \cdots + 1/2 \text{ (} k \text{ times)}.$$

Random access machine

Fixed number K of registers R_j, $j = 1, \dots, K$. Memory: one-way infinite tape: cell i contains natural number $T[i]$ of arbitrary size.

Program: a sequence of instructions, in the "program store": a (potentially) infinite sequence of registers containing instructions. A program counter.

`read j`	$R_0 = T[R_j]$	(this is random access)
`write j`		
`store j`	$R_j = R_0$	
`load j`		
`add j`	$R_0 \mathrel{+}= R_j$	
`add =c`	$R_0 \mathrel{+}= c$	
`sub j`	$R_0 = \lvert R_0 - R_j \rvert^+$	
`sub =c`		
`half`	$R_0 \mathrel{/}= 2$	
`jump s`		
`jpos s`	if $R_0 > 0$ then jump s	
`jzero s`		
`halt`		

In our applications, we will impose some bound k on the number of cells.

The size of the numbers stored in each cell will be bounded by k^c for some constant c. Thus, the wordsize of the machine will be logarithmic in the size of the memory, allowing to store the address of any position in a cell.

Basic integer arithmetic

Length of numbers

$$\operatorname{len}(n) = \begin{cases} \lfloor \log |n| \rfloor + 1 & \text{if } n \neq 0, \\ 1 & \text{otherwise.} \end{cases}$$

This is essentially the same as $\log n$, but is always defined. We will generally use $\operatorname{len}(n)$ in expressing complexities.

Upper bounds

On the complexity of addition, multiplication, division (with remainder), via the algorithms learned at school.

Theorem

The complexity of computing $(a, b) \mapsto (q, r)$ *in the division with remainder* $a = qb + r$ *is* $O(\text{len}(q)\text{len}(b))$.

Proof.

The long division algorithm has $\leqslant \text{len}(q)$ iterations, with numbers of length $\leqslant \text{len}(b)$. □

Theorem (Fundamental theorem of arithmetic)

Unique prime decomposition $\pm p_1^{e_1} \dots p_k^{e_k}$.

The proof is not trivial, we will lead up to it. We will see analogous situations later in which the theorem does not hold.

Example

Irreducible family: one or two adult and some minors.
Later: the ring $\mathbb{Z}[\sqrt{-5}]$.

The above theorem is equivalent to the following lemma:

Lemma (Fundamental)

If p *is prime and* $a, b \in \mathbb{Z}$ *then* $p|ab$ *if and only if* $p|a$ *or* $p|b$.

In class, we have shown the equivalence.

Ideals

If I, J are ideals so is $aI + bJ$.
$a\mathbb{Z} \subseteq b\mathbb{Z}$ if and only if $b|a$.
Careful: generally $a\mathbb{Z} + b\mathbb{Z} \neq (a+b)\mathbb{Z}$.

Example

$2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$.

Principal ideal

The following theorem is the crucial step in the proof of the Fundamental Theorem.

Theorem

In $\mathbb{Z}$, every ideal I is principal.

Proof.

Let d be the smallest positive integer in I. The proof shows $I = d\mathbb{Z}$, using division with remainder. □

Corollary

If $d > 0$ and $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ then $d = \gcd(a, b)$. In particular, we found that

(a) *Every other divisor of a, b divides $\gcd(a, b)$.*

(b) *For all a, b there are $s, t \in \mathbb{Z}$ with $\gcd(a, b) = sa + tb$.*

The proof of the theorem is non-algorithmic. It does not give us a method to calculate $\gcd(a, b)$: in particular, it does not give us the s, t in the above corollary. We will return to this.

Theorem

For a, b, c *with* $\gcd a, c = 1$ *and* $c|ab$ *we have* $c|b$.

This theorem implies the Fundamental Lemma announced above.

Proof.

Using $1 = sc + ta$, hence $b = scb + tab$. □

Some consequences of unique factorization

There are infinitely many primes.
The notation $\nu_p(a)$. gcd and minimum, lcm and maximum.

$$\operatorname{lcm}(a, b) \cdot \gcd(a, b) = |ab|$$

Pairwise relatively prime numbers.
Representing fractions in lowest terms.
Lowest common denominator.

Rings

Unless stated otherwise, commutative, with a unit element. The detailed properties of rings will be deduced later (see Section 9 of Shoup, in particular Theorem 9.2). We use rings here only as examples.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- The set of (say, 2×2) matrices over $\mathbb{R}$ is also a ring, but is not commutative.
- The set $2\mathbb{Z}$ is also a ring, but has no unit element.
- If R is a commutative ring, then $R[x, y]$, the set of polynomials in x, y with coefficients in R, is also a ring.

Theorem

Let R be a ring. Then:

(i) *the multiplicative identity is unique.*

(ii) $0 \cdot a = 0$ *for all* a *in* R.

(iii) $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$.

(iv) $(-a)(-b) = ab$ *for all* $a, b \in R$.

(v) $(na)b = a(nb) = n(ab)$ *for all* $n \in \mathbb{Z}$, $a, b \in R$.

Ideals.

Example

A non-principal ideal: $x\mathbb{Z}[x,y] + y\mathbb{Z}[x,y]$ in $\mathbb{Z}[x,y]$.

Example

Non-unique irreducible factorization in a ring. Let the ring be $\mathbb{Z}[\sqrt{-5}]$.

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

How to show that $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ are irreducible? Let $N(a + b\sqrt{-5}) = a^2 + 5b^2$, then it is easy to see that $N(xy) = N(x)N(y)$, since $N(z)$ is the square absolute value of the complex number z. It is always integer here.
If $N(z) = 1$ then $z = \pm 1$.
If $N(z) > 1$ then $N(z) \geqslant 4$.
For $z = 2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$, we have $N(z) = 4, 9, 6, 6$. The only nontrivial factors of these numbers are 2 and 3, but there is no z with $N(z) \in \{2, 3\}$.

The basic Euclidean algorithm

Assume $a \geqslant b \geqslant 0$ are integers.

$$\begin{aligned} a = r_0, \quad b &= r_1, \\ r_{i-1} &= r_i q_i + r_{i+1} \quad (0 < r_{i+1} < r_i), \quad (1 \leqslant i < \ell) \\ &\vdots \\ r_{\ell-1} &= q_\ell r_\ell \end{aligned}$$

Upper bound on the number ℓ of iterations:

$$\ell \leqslant \log_\phi b + 1,$$

where $\phi = (1 + \sqrt{5})/2 \approx 1.62$. We only note $\ell = O(\log b)$ which is obvious from

$$r_{i+1} \leqslant r_{i-1}/2.$$

Theorem

Euclid's algorithm runs in time $O(\mathrm{len}(a)\mathrm{len}(b))$.

This is stronger than the upper bound seen above.

Proof.

We have

$$\mathrm{len}(b)\sum_{i=1}^{\ell}\mathrm{len}(q_i) \leqslant \mathrm{len}(b)\sum_{i=1}^{\ell}(1+\log(q_i)) \leqslant \mathrm{len}(b)(\ell+\log(\prod_{i=1}^{\ell} q_i)).$$

Now,

$$a = r_0 \geqslant r_1 q_1 \geqslant r_2 q_2 q_1 \geqslant \cdots \geqslant r_\ell q_\ell \cdots q_1.$$

□

The extended Euclidean algorithm

$$s_0 = 1, \qquad t_0 = 0,$$
$$s_1 = 0, \qquad t_1 = 1,$$
$$s_{i+1} = s_{i-1} - s_i q_i, \qquad \text{same for } t_i.$$

Theorem

The following relations hold.

(i) $s_i a + t_i b = r_i$.

(ii) $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$.

(iii) $\gcd(s_i, t_i) = 1$.

(iv) $t_i t_{i+1} \leqslant 0$, $|t_i| \leqslant |t_{i+1}|$, *same for* s_i.

(v) $r_{i-1}|t_i| \leqslant a$, $r_{i-1}|s_i| \leqslant b$.

Proof.

(i),(ii): induction. (i) follows from (ii). (iv): induction. (v): combining (i) for i and $i - 1$. □

Matrix representation

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = Q_i \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}.$$

Define $M_i = Q_i \cdots Q_1$, then

$$M_i = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix}.$$

Now the relation $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$ above says $\det M_i = \prod_{j=1}^{i} \det Q_i = (-1)^i$.

Congruences

$a \equiv b \pmod{m}$ if $m | b - a$.
More generally, in a ring with some ideal I, we write $a \equiv b \pmod{I}$ if $(b - a) \in I$.

Theorem

The relation $\equiv$ has the following properties, when I is fixed.

(a) *It is an equivalence relation.*

(b) *Addition and multiplication of congruences.*

Example (From Emil Kiss)

Is the equation $x^2 + 5y = 1002$ solvable among integers?
This seems hard until we take the remainders modulo 5, then it says: $x^2 \equiv 2 \pmod{5}$. The squares modulo 5 are $0, 1, 4, 4, 1$, so 2 is not a square.

The ring of congruence classes

For an integer x, let

$$[x]_m = \{ y \in \mathbb{Z} : y \equiv x \pmod{m} \}$$

denote the residue class of x modulo m. We choose a representative for each class $[x]_m$: its smallest nonnegative element.

Example

The set $[-3]_5$ is $\{\dots, -8, -3, 2, 7, \dots\}$. Its representative is 2.

Definition of the operations $+, \cdot$ on these classes. This is possible due to the additivity and multiplicativity of $\equiv$.
The set of classes with these operations is turned into a ring which we denote by $\mathbb{Z}_m$. We frequently write $\mathbb{Z}_m = \{0, 1, \dots, (m-1)\}$, that is we use the representative of class $[i]_m$ to denote the class.

Division of congruences

Does $c \cdot a \equiv c \cdot b \pmod{m}$ imply $a \equiv b \pmod{m}$ when $c \not\equiv 0 \pmod{m}$? Not always.

Example

$2 \cdot 3 = 6 \equiv 0 \equiv 2 \cdot 0 \pmod{6}$, but $3 \not\equiv 0 \pmod{6}$.

The numbers 2,3 are called here zero divisors. In general, an element $x \neq 0$ of a ring R is a zero divisor if there is an element $y \neq 0$ in R with $x \cdot y = 0$.

Theorem

In a finite ring R, if b is not a zero divisor then the equation $x \cdot b = c$ has a unique solution for each c: that is, we can divide by b.

Proof.

The mapping $x \to x \cdot b$ is one-to-one. Indeed, if it is not then there would be different elemnts x, y with $x \cdot b = y \cdot b$, but $(x - y) \cdot b \neq 0$, since b is not a zero divisor.
At the beginning of class, we have seen that in a finite set, if a class is one-to-one then it is also onto. Therefore for each c there is an x with $x \cdot b = c$. The one-to-one property implies that x is unique. □

Observe that this proof is non-constructive: it does not help finding x from b, c.
Actually we only need to find b^{-1}, that is the solution of $x \cdot b = 1$

Finding the inverse

Proposition

An element of $b \in \mathbb{Z}_m$ is not a zero divisor if and only if $\gcd(b, m) = 1$.

To find the inverse x of b, we need to solve the equation $x \cdot b + y \cdot m = 1$. Euclid's algorithm gives us these x, y, and then $x \equiv b^{-1} \pmod{m}$.

Example

Inverse of 8 modulo 15.

Characterizing the set of all solutions of the equation

$$a \cdot x \equiv b \pmod{m}.$$

Corollary (Cancellation law of congruences)

If $\gcd(c, m) = 1$ *and* $ac \equiv bc \pmod{m}$ *then* $a \equiv b \pmod{m}$.

Examples

- We have $5 \cdot 2 \equiv 5 \cdot (-4) \pmod{6}$. This implies $2 \equiv -4 \pmod{6}$.
- We have $3 \cdot 5 \equiv 3 \cdot 3 \pmod{6}$, but $5 \not\equiv 3 \pmod{6}$.

What can we do in the second case? Simplify as follows.

Proposition

For all a, b, c *the relation* $ac \equiv bc \pmod{mc}$ *implies* $a \equiv b \pmod{m}$.

The proof is immediate.
In the above example, from $3 \cdot 5 \equiv 3 \cdot 3 \pmod{6}$ we can imply $5 \equiv 1 \pmod{2}$.

Chinese remainder theorem

Consider two diferent moduli: m_1 and m_2. Do all residue classes of m_1 intersect with all residue classes of m_2? That is, given a_1, a_2, we are looking for an x with

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}.$$

There is not always a solution. For example, there is no x with

$$x \equiv 0 \pmod{2}, \quad x \equiv 1 \pmod{4}.$$

But if m_1, m_2 are coprime, there is always a solution. More generally:

Theorem

If $m_1, \ldots, m_k$ are relatively prime with $M = m_1 \cdots m_k$ then for all $a_1, \ldots, a_k \in \mathbb{Z}$ there is a unique $0 \leqslant x < M$ with $x \equiv a_i \pmod{m_i}$ for all $i = 1, \ldots, k$.

Proof.

Let $I(n) = \{0, \ldots, n-1\}$. The sets $U = I(M)$ and $V = I(m_1) \times \cdots \times I(m_k)$ both have size M. We define a mapping $f : U \to V$ as follows:

$$f(x) = (x \bmod m_1, \ldots, x \bmod m_k).$$

Let us show that this mapping is one-to-one. Indeed, if $f(x) = f(y)$ for some $x \leqslant y$ then $x \equiv y \pmod{m_i}$ and hence $m_i | (y - x)$ for each i. Since m_i are relatively prime this implies $M | (y - x)$, hence $y - x = 0$. Since the sets are finite and have the same size, it follows that the mapping f is also invertible, which is exactly the statement of the theorem. □

Note that the theorem is not constructive (just like the theorem about the modular inverse).

Chinese remainder algorithm

How to find the x in the Chinese remainder theorem?
Let $M_i = M/m_i$, for example $M_1 = m_2 \cdots m_k$. Let m_i' be $(M_i)^{-1}$ modulo m_i (it exists). Let

$$x = a_1 M_1 m_1' + \cdots + a_k M_k m_k' \bmod M.$$

Let us show for example $x \equiv a_1 \pmod{m_1}$. We have $a_i M_i m_i' \equiv 0 \pmod{m_1}$ for each $i > 1$, since $m_1 | M_i$.
On the other hand, $a_1 M_1 m_1' \equiv a_1 \cdot 1 \pmod{m_1}$.

Fractions in $\mathbb{Z}_m$

Look at the equation $r \equiv yt \pmod{m}$, where m, y is given. Typically there is no unique solution for r, t; however, the quotient r/t (as a rational number) is uniquely determined if r, t are required to be small compared to m.

Theorem (Rational reconstruction)

Let $r^*, t^* > 0$ and y be integers with $2r^*t^* < m$. Let us call the pair (r, t) of integers admissible if $|r| \leqslant r^*$, $0 < t \leqslant t^*$, and $r \equiv yt \pmod{m}$. Then, there is a rational number q_y such that $r/t = q_y$ for all admissible pairs (r, t).

Proof.

Suppose that both (r_1, t_1) and (r_2, t_2) are admissible pairs: we want to prove $r_1/t_1 = r_2/t_2$. We have, modulo m:

$$r_1 \equiv t_1 y,$$
$$r_2 \equiv t_2 y.$$

Linear combination gives $r_1 t_2 - r_2 t_1 \equiv 0$, hence $m | (r_1 t_2 - r_2 t_1)$. Since $m > 2r^* t^*$ this implies $r_1 t_2 = r_2 t_1$. Dividing by $t_1 t_2$ gives the result. □

Finding an admissible pair (if it exists) under the condition

$$n \geqslant 4r^* t^*,$$

by the Euclidean algorithm: see the book.

Error correction

Let $m_1, \dots, m_k$ be mutually coprime moduli, $M = m_1 \cdots m_k$. Let $0 < Z < M$ and $0 < P$ be integers. A set $B \subset \{1, \dots, k\}$ is called P-admissible if $\prod_{i \in B} m_i \leqslant P$.

Example

If $(m_1, m_2, m_3, m_4) = (2, 3, 5, 7)$ and $P = 8$ then the admissible sets are $\{1\}, \{2\}, \{1, 2\}, \{3\}, \{4\}$.

Let y be an arbitrary integer. An integer $0 \leqslant z \leqslant Z$ is called (Z, P)-admissible for y if the set of indices

$$B = \{\, i : z \not\equiv y \pmod{m_i} \,\}$$

is P-admissible. We can say y has errors compared to z in the residues $y \bmod m_i$ for $i \in B$.

An admissible z can be recovered from y, provided Z, P are small:

Theorem

If $M > 2PZ^2$ then for every y and there is at most one z that is (Z, P)-admissible for it.

Proof.

Let $t = \prod_{i \in B} m_i$. Then it is easy to see that

$$tz \equiv ty \pmod{M}$$

holds. Let $r = tz$, $r^* = PZ$, $t^* = P$, then $|tz| \leqslant r^*$ and $t \leqslant t^*$ while $M > 2r^*t^*$. The Rational Reconstruction Theorem implies therefore that $z = r/t$ is uniquely determined by y. □

If the stronger condition $M > 4P^2Z$ is required then following the book, the value z can also be found efficiently using the Euclidean algorithm.

Euler's phi function

See the definition in the book. Computing it for p, p^{α}, pq.
The multiplicative order of a residue.

Theorem (Euler)

For $a \in \mathbb{Z}_m^*$ we have $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof.

Corollary

Fermat's little theorem.

Some properties of phi

Theorem

For positive integers m, n *with* $\gcd(m, n) = 1$ *we have* $\phi(mn) = \phi(m)\phi(n)$.

Proof.

One-to-one map between $\mathbb{Z}_{mn}^*$ and $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$. □

Application: formula for $\phi(n)$.

Theorem

We have $\sum_{d|n} \phi(d) = n$.

Proof.

To each $0 \leqslant k < n$ let us assign the pair (d, k') where $d = \gcd(k, n)$ and $k' = k/d$. Then for each divisor d of n, the numbers k' occurring in some (d, k') will run through each element of $\mathbb{Z}^*_{n/d}$ once, hence $\sum_{d|n} \phi(n/d) = n$. □

Modular exponentiation

In the exponents, we compute modulo $\phi(m)$.

Examples

- For prime $p > 2$ and $\gcd(a, p) = 1$, we have $a^{\frac{p-1}{2}} \equiv \pm 1$.
- For composite m, this is no more the case. If $m = pq$ with primes $p, q > 2$ then $x^2 \equiv 1$ has 4 solutions, since $x \bmod p = \pm 1$ and $x \bmod q = \pm 1$ can be independently of each other. See $p = 3, q = 5$.

Fast modular exponentiation: the repeated squaring trick.

Primitive root (generator).

Example

If g is a primitive root modulo a prime $p > 2$ then $a^{\frac{p-1}{2}} \equiv -1$.

Theorem

Primitive root exists for m if and only if $m = 2, 4, p^{\alpha}, 2p^{\alpha}$ for odd prime p.

Proof later.
When there is a primitive root, the multiplicative structure (group) $\mathbb{Z}_m^*$ is the same as (isomorphic to) the additive group $\mathbb{Z}_{\phi(m)}^+$.

Chebyshev's theorem

Binomial coefficients. The definition of $\pi(n), \vartheta(n)$.

Proposition

$$4^n/(n+1) < \binom{2n}{n} < \binom{2n+1}{n+1} < 4^n.$$

Lemma (Upper bound on $\vartheta(n)$)

We have $\vartheta(n) \leqslant 2n$.

Proof.

We have $\vartheta(2m+1) - \vartheta(m+1) \leqslant \log\binom{2m+1}{m+1} \leqslant 2m$. From here, induction using $\vartheta(2m-1) = \vartheta(2m)$. □

Proposition

$$\nu_p(n!) = \sum_{k \geqslant 1} \lfloor n/p^k \rfloor.$$

Lemma (Lower bound in $\pi(n)$)

$$\pi(n) \geqslant (1/2)n/\log n.$$

Proof.

For $N = \binom{2m}{m}$ we have

$$\nu_p(N) = \sum_{k \geqslant 1} (\lfloor 2m/p^k \rfloor - 2\lfloor m/p^k \rfloor).$$

Recall the exercise showing $0 \leqslant \lfloor 2x \rfloor - 2\lfloor x \rfloor \leqslant 1$, hence this is sum is between 0 and $\leqslant \log_p(2m)$. So,

$$\begin{aligned} m \leqslant \log N \leqslant \sum_{p \leqslant 2m} \nu_p(N) \log p &\leqslant \sum_{p \leqslant 2m} \log_p(2m) \log p \\ &= \sum_{p \leqslant 2m} \log(2m) = \pi(2m) \log(2m), \end{aligned}$$

$$(1/2)(2m)/\log(2m) \leqslant \pi(2m).$$

For odd n, note $\pi(2m-1) = \pi(2m)$ and that $x \log x$ is monotone. □

Theorem

We have $\vartheta(n) \approx \pi(n)\log n$, *that is* $\frac{\vartheta(n)}{\pi(n)\log n} \to 1$.

Proof.

$\vartheta(n) \leqslant \pi(n)\log n$ is immediate. For the lower bound, cut the sum at $p \geqslant n^{\lambda}$ for some constant $0 < \lambda < 1$. □

From all the above, we found

Theorem (Chebyshev)

We have $\pi(n) \stackrel{*}{=} \frac{n}{\log n}$.

Abelian groups

Proposition

Identity and inverse are unique.

Examples

$\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+, n\mathbb{Z}^+, \mathbb{Z}_n^+, \mathbb{Z}_n^*$.
$\mathbb{Q}^* \setminus \{0\}$ and $[0, \infty) \cap \mathbb{Q}^*$ for multiplication.

Examples

Non-abelian groups:

- 2×2 integer matrices with determinant ± 1
- 2×2 integer matrices with determinant 1
- All permutations of $\{1, \ldots, n\}$.

To create new groups

Cyclic groups, examples. Generators of a cyclic group.
Direct product $G_1 \times G_2$.

Example

The set of all ± 1 strings of length n with respect to termwise multiplication: this is "essentially the same" as $\mathbb{Z}_2^n$.

When is a direct product of two cyclic groups cyclic? Examples.

Subgroups

A subset closed with respect to addition and inverse. Then it is also a group.

Examples

- mG (or G^m in multiplicative notation).
- $G\{m\} = \{ g \in G : mg = 0 \}$.

Theorem

Every subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$.

We proved this already since subgroups of $(\mathbb{Z}, +)$ are just the ideals of $(\mathbb{Z}, +, *)$

Theorem

If H is finite then it is a subgroup already if it is closed under addition.

Creating new subgroups

$H_1 + H_2$, $H_1 \cap H_2$.

Example

Let $G = G_1 \times G_2$, $\overline{G}_1 = G_1 \times \{0_{G_2}\}$, $\overline{G}_2 = \{0_{G_1}\} \times G_2$. Then $\overline{G}_i$ are subgroups of G, and

$$\overline{G}_1 \cap \overline{G}_2 = \{0_G\}, \qquad \overline{G}_1 + \overline{G}_2 = G.$$

So in a way, the direct product can, with the sum notation, be also called the direct sum.

Congruences

$a \equiv b \pmod{H}$ if $b - a \in H$.
We have seen for rings earlier already that if H is an ideal, this is an equvalence relation and you can add congruences. The same proof shows that if H is a subgroup you can do this.
The equivalence classes $a + H$ are called cosets.

Theorem

All cosets have the same size as H.

Proof.

If $C = a + H$ then $x \mapsto a + x$ is a bijection between H and C. □

Corollary (Lagrange theorem, for commutative groups)

If G is finite and H is its subgroup then $|H|$ divides $|G|$.

Corollary

For any element a, *its order* $\operatorname{ord}_G(a)$ *is the order of the cyclic group generated by* a, *hence it divides* $|G|$ *if* $|G|$ *is finite.*
Thus, we always have $|G| \cdot a = 0$.

The quotient group

Group operation among congruence classes, just as modulo m. This is the group G/H.

Examples

- If $G = G_1 \times G_2$ then recall $\overline{G}_1, \overline{G}_2$. Each element of $G/\overline{G}_1$ can be written as $(0, g_2) + \overline{G}_1$ for some g_2. So, elements of $\overline{G}_2$ form a set of representatives for the cosets, and these representatives form a subgroup.
- $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$. The class representatives do not form a subgroup.
- $\mathbb{Z}_4/2\mathbb{Z}_4$ consists of the classes $[0] = \{0, 2\}, [1] = \{1, 3\}$. The class representatives do not form a subgroup.

Two-dimensional picture.

Isomorphism, homomorphism

Isomorphism.

Example

$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. But $2\mathbb{Z}_4 \cong \mathbb{Z}_2$, $\mathbb{Z}_4/2\mathbb{Z}_4 \cong \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$.

Homomorphism, image, kernel.

Examples

- The multiplication map, $\mathbb{Z} \to m\mathbb{Z}$. Its kernel is $\mathbb{Z}\{m\}$.
- For $a = (a_1, a_2) \in \mathbb{Z}^2$, let $\phi_a : G \times G \to G$ be defined as $(g_1, g_2) \mapsto a_1 g_1 + a_2 g_2$.
- This also defines a homomorphism $\psi_g : \mathbb{Z}^2 \to G$, if we fix $g = (g_1, g_2) \in G^2$ and view a_1, a_2 as variable.

Properties of a homomorphism

Proposition

Let $\rho : G \to G'$ *be a homomorphism.*

(i) $\rho(0_G) = 0_{G'}$, $\rho(-g) = -\rho(g)$, $\rho(ng) = n\rho(g)$.

(ii) *For any subgroup* H *of* G, $\rho(H)$ *is a subgroup of* G'.

(iii) $\ker(\rho)$ *is a subgroup of* G.

(iv) ρ *is injective if and only if* $\ker(\rho) = \{0_G\}$.

(v) $\rho(a) = \rho(b)$ *if and only if* $a \equiv b \pmod{\ker(\rho)}$.

(vi) *For every subgroup* H' *of* G', $\rho^{-1}(H')$ *is a subgroup of* G *containing* $\ker(\rho)$.

Composition of homomorphisms. Homomorphisms into and from $G_1 \times G_2$.

Theorem

For any subgroup H of an Abelian group G, the map $\rho : G \to G/H$, where $\rho(a) = a + H$ is a surjective homomorphism, with kernel H, called the natural map from G to G/H.
Conversely, for any homomorphism ρ, the factorgroup $G/\ker(\rho)$ is isomorphic to $\rho(G)$.

Examples

- The image of the multiplication map $\mathbb{Z}_8 \to \mathbb{Z}_8$, $a \mapsto 2a$ is the subgroup $2\mathbb{Z}_8$ of $\mathbb{Z}_8$. The kernel is $\mathbb{Z}_8\{2\}$, and we have $\mathbb{Z}_8/\mathbb{Z}_8\{2\} \cong 2\mathbb{Z}_8 \cong \mathbb{Z}_4$.
- (Chinese Remainder Theorem) For $m_1, \ldots, m_k$, the map $\mathbb{Z} \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ given by taking the remainders modulo m_i. Surjective iff the m_i are pairvise relatively prime.

Theorem

Let H_1, H_2 *be subgroups of* G*. The the map* $\rho : H_1 \times H_2 \to H_1 + H_2$ *with* $\rho(h_1, h_2) = h_1 + h_2$ *is a surjective group homomorphism that is an isomorphism iff* $H_1 \cap H_2 = \{0\}$*.*

Cyclic groups, classification

For a generator a of cyclic G, look at homomorphism $\rho_a : \mathbb{Z} \to G$, defined by $z \mapsto za$. Then $\ker(\rho_a)$ is either $\{0\}$ or $m\mathbb{Z}$ for some m. In the first case, $G \cong \mathbb{Z}$, else $G \cong \mathbb{Z}_m$

Examples

- An element n of $\mathbb{Z}_m$ generates a subgroup of order $m/\gcd(m, n)$.
- $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ is cyclic iff $\gcd(m_1, m_2) = 1$.

Subgroups

All subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z}$.

Theorem

On subgroups of a finite cyclic group $G = \mathbb{Z}_m$:

(i) *All subgroups are of the form $dG = G\{m/d\}$ where $d|m$, and $dG \subseteq d'G$ iff $d'|d$.*

(ii) *For any divisor d of m, the number of elements of order d is $\phi(d)$.*

(iii) *For any integer n we have $nG = dG$ and $G\{n\} = G\{d\}$ where $d = \gcd(m, n)$.*

Theorem

(i) *If G is of prime order then it is cyclic.*

(ii) *Subgroups of a cyclic group are cyclic.*

(iii) *Homomorphic images of a cyclic group are cyclic.*

The exponent of an Abelian group G: the smallest $m > 0$ with $mG = \{0\}$, or 0 if there is no such $m > 0$.

Theorem

Let m be the exponent of G.

(i) *m divides $|G|$.*

(ii) *If $m \neq 0$ is then the order of every element divides it.*

(iii) *G has an element of order m.*

Theorem

(i) *If prime p divides $|G|$ then G contains an element of order p.*

(ii) *The primes dividing the exponent are the same as the primes dividing the order.*

Rings

We have introduced rings earlier, now we will learn more about them.

Example

Complex numbers: pairs (a, b) with $a, b \in \mathbb{R}$, and the known operations.
Conjugation: a ring isomorphism. Norm: $z\bar{z} = a^2 + b^2$, and its properties.

Characteristic: the exponent of the additive group.

Units and fields

An element is a unit if it has a multiplicative inverse. The set of units of ring R is denoted by R^*. This is a group.

Examples

- For $z \in \mathbb{C}$, we have $z^{-1} = \bar{z}/N(z)$.
- Units in $\mathbb{Z}$, $\mathbb{Z}_m$.
- The Gaussian integers, and units among them.
- Units in $R_1 + R_2$.

Zero divisors and integral domains

R is an integral domain if it has no zero divisors.

Examples

- When is $\mathbb{Z}_m$ an integral domain?
- When is an element of $R_1 \times R_2$ a zero divisor?

Theorem

(i) $a|b$ *implies unique quotient.*

(ii) $a|b$ *and* $b|a$ *implies they differ by a unit.*

Theorem

(i) *The characteristic of an integral domain is a prime.*

(ii) *Any finite integral domain is a field.*

(iii) *Any finite field has prime power cardinality.*

Subrings

Examples

- Gaussian integers
- $\mathbb{Q}_m$.

Polynomial rings

The ring $R[\mathtt{X}]$.
The formal polynomial versus the polynomial function. In algebra, $\mathtt{X}$ is frequently called an indeterminate to make the distinction clear.
For each $a \in R$, the substitution $\rho_a : R[\mathtt{X}] \to R$ defined by $\rho_a(f(\mathtt{X})) = f(a)$ is a ring homomorphism.

Example

$\mathbb{Z}_2[\mathtt{X}]$ is our first example of a ring with finite characteristic that is not a field.

Degree $\deg(f)$. Leading coefficient $\mathrm{lc}(f)$. Monic polynomial: when the leading coefficient is 1. Constant term.
Degree Convention: $\deg(0) = -\infty$.
$\deg(fg) \leqslant \deg(f) + \deg(g)$, equality if the leading coefficients are not zero divisors.

Proposition

If D is an integral domain then $(D[\mathtt{X}])^* = D^*$.

Warning: different polynomials can give rise to the same polynomial function. Example: $\mathtt{X}^p - \mathtt{X}$ over $\mathbb{Z}_p$ defines the 0 function.

Theorem (Division with remainder)

Let $f, g \in R[\mathtt{X}]$ with $g \neq 0_R$ and $\mathrm{lc}(g) \in R^*$. Then there is a q with

$$f = q \cdot g + r, \qquad \deg(r) < \deg(g).$$

Notice the resemblance to and difference from number division.

The long division algorithm.

Theorem

Dividing by $\mathtt{X} - \alpha$*:*

$$f(\mathtt{X}) = q \cdot (\mathtt{X} - \alpha) + f(\alpha).$$

Roots of a polynomial.

Corollary

(i) α *is a root of* $f(\mathtt{X})$ *iff* $f(\mathtt{X})$ *is divisible by* $\mathtt{X} - \alpha$.

(ii) *In an integral domain, a polynomial of degree* n *has at most* n *roots.*

Theorem

If D is an integral domain then every finite subgroup G of D^* is cyclic.

Proof.

The exponent of m of G is equal to G, since $\mathtt{X}^m - 1$ has at most m roots. By an earlier theorem, G has an element whose order is the exponent. □

Corollary

Modulo any prime p, there is a primitive root.

Ideals and homomorphisms

We defined ideals earlier, this is partly a review.
Generated ideal (a), (a, b, c). Principal ideal.
Congruence modulo an ideal. Quotient ring.

Example

Let f be a monic polynomial, consider $E = R[\mathtt{X}]/(f \cdot R[\mathtt{X}]) = R[\mathtt{X}]/(f)$.

- $\mathbb{R}[X]/(\mathtt{X}^2 + 1) \cong \mathbb{C}$.
- $\mathbb{Z}_2[\mathtt{X}]/(\mathtt{X}^2 + \mathtt{X} + 1)$. Elements are $[0], [1], [\mathtt{X}], [\mathtt{X} + 1]$. Multiplication using the rule $\mathtt{X}^2 \equiv \mathtt{X} + 1$. Since $\mathtt{X}(\mathtt{X} + 1) \equiv 1$ every element has an inverse, and E is a field of size 4.

Prime ideal: If $ab \in I$ implies $a \in I$ or $b \in I$.
Maximal ideal.

Examples

- In the ring $\mathbb{Z}$, the ideal $m\mathbb{Z}$ is a prime ideal if and only if m is prime. In this case it is also maximal.
- In the ring $\mathbb{R}[X, Y]$, the ideal (X) is prime, but not maximal. Indeed, $(X) \subsetneq (X, Y) \neq \mathbb{R}[X, Y]$

Proposition

(i) *I is prime iff R/I is an integral domain.*
(ii) *I is maximal iff R/I is a field.*

Proposition

Let $\rho : R \to R'$ be a homomorphism.

(i) *Images of subrings are subrings. Images of ideals are ideals of $\rho(R)$.*

(ii) *The kernel is an ideal. ρ is injective (an embedding) iff it is $\{0\}$.*

(iii) *The inverse image of an ideal is an ideal containing the kernel.*

Proposition

The natural map $\rho : R \to R/I$ is a homomorphism.
Isomorphism between $R/\ker(\rho)$ and $\rho(R)$.

Examples

- $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is not only a group homomorphism but also a ring homomorphism.
- The mapping for the Chinese Remainder Theorem.

Polynomial factorization and congruences

(See 17.3-4 of Shoup)
We will consider elements of $F[\mathtt{X}]$ over a field F.
The associate relation between elements of $F[\mathtt{X}]$.

Theorem

Unique factorization in $F[\mathtt{X}]$. The monic irreducible factors are unique.

The proof parallels the proof of unique factorization for integers, using division with remainder.

- Every ideal is principal.
- If f, g are relatively prime then there are s, t with

$$f \cdot s + g \cdot t = 1. \tag{2}$$

- Polynomial p is irreducible iff $p \cdot F[\mathtt{X}]$ is a prime ideal, and iff it is a maximal ideal, so iff $F[\mathtt{X}]/(p)$ is a field.
  Warning: here we cannot use counting argument (as for integers) to show the existence of the inverse. We rely on (2) directly.
- Congruences modulo a polynomial. Inverse.
- Chinese remainder theorem. Interpolation.

The following theorem is also true, but its proof is longer (see 17.8 of Shoup).

Theorem

There is unique factorization over the following rings as well:

$$\mathbb{Z}[x_1, \ldots, x_n], F[x_1, \ldots, x_n],$$

where F is an arbitrary field.

Complex and real numbers

Theorem

Every polynomial in $\mathbb{C}[\mathtt{X}]$ has a root.

We will not prove this. It implies that all irreducible polynomials in $\mathbb{C}$ have degree 1.

Theorem

Every irreducible polynomial over $\mathbb{R}$ has degree 1 or 2.

Proof.

Let $f(\mathtt{X})$ be a monic polynomial with no real roots, and let

$$f(\mathtt{X}) = (\mathtt{X} - \alpha_1) \cdots (\mathtt{X} - \alpha_n)$$

over the complex numbers. Then

$$f(\mathtt{X}) = \overline{f(\mathtt{X})} = (\mathtt{X} - \overline{\alpha}_1) \cdots (\mathtt{X} - \overline{\alpha}_n).$$

Since the factorization is unique, the conjugation just permuted the roots. All the roots are in pairs: $\beta_1, \overline{\beta}_1$, $\beta_2, \overline{\beta}_2$, and so on. We have

$$(\mathtt{X} - \beta)(\mathtt{X} - \overline{\beta}) = \mathtt{X}^2 - (\beta + \overline{\beta})\mathtt{X} + \beta\overline{\beta}.$$

Since these coefficients are their own conjugates, they are real. Thus f is the product of real polynomials of degree 2. □

Roots of unity

Complex multiplication: addition of angles.
Roots of unity form a cyclic group (as a finite subgroup of the multiplicative group of a field).
Primitive nth root of unity: a generator of this group. One such generator is the root with the smallest angle.

Proposition

If ε is a root of unity different from 1 then $\sum_{i=1}^{n} \varepsilon^i = 0$.

Fourier transform

Interpolation is particularly simple if the polynomial is evaluated at roots of unity.