Abstract Algebra, Lecture 2

The integers

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Summary

Basic definitions

Definition

- The integers: $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$
- Natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
- Positive integers: $\mathbb{Z}_+ = \mathbb{P} = \{1, 2, 3, \dots\}$
- Rational numbers: $\mathbb{Q} = \{\, a/b \,|\, a, b \in \mathbb{Z},\ b \neq 0 \,\}$ with relation $a/b = c/d$ if and only if $ad = bc$
- Real numbers $\mathbb{R}$, constructed from $\mathbb{Q}$ using topology
- Complex numbers $\mathbb{C} = \mathbb{R}[i]$

Theorem (Well-ordering principle)

Any non-empty subset of $\mathbb{N}$ *contains a smallest element.*

Theorem (Induction principle)

Suppose that $S \subset \mathbb{N}$ *and*

(a) $0 \in S$

(b) *For all* $n \in \mathbb{N}$*, if* $n \in S$ *then* $n + 1 \in S$

Then: $S = \mathbb{N}$.

Equivalent formulation:

(a) $0 \in S$

(b) *For all* $n \in \mathbb{N}$*, if* $k \in S$ *for all* $k \in \mathbb{N}$ *with* $k < n$*, then* $n \in S$.

Then: $S = \mathbb{N}$.

Unless otherwise stated, $a, b, c, x, y, r, s \in \mathbb{Z}$, $n, m \in \mathbb{P}$.

Definition

$a|b$ if exists c s.t. $b = ac$.

Example

$3|12$ since $12 = 3 * 4$.

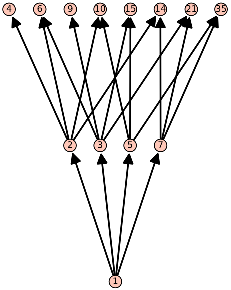
Lemma

- $a|0$,
- $0|a \iff a = 0$,
- $1|a$,
- $a|1 \iff a = \pm 1$,
- $a|b \wedge b|a \iff a = \pm b$
- $a|b \iff -a|b \iff a|-b$
- $a|b \wedge a|c \implies a|(b+c)$,
- $a|b \implies a|bc$.

Theorem

Restricted to $\mathbb{P}$, divisibility is a partial order, with unique minimal element 1.

Part of Hasse diagram



Id est,

1. $a|a$,
2. $a|b \wedge b|c \implies a|c$,
3. $a|b \wedge b|a \implies a = b$.

Definition

$n \in \mathbb{P}$ is a prime number if

- $n > 1$,
- $m|n \implies m \in \{1, n\}$

(positive divisors, of course $-1, -n$ also divisors)

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

Division algorithm

Theorem

$a, b \in \mathbb{Z}$, $b \neq 0$. Then exists unique k, r, quotient and remainder, such that

- $a = kb + r$,
- $0 \leq r < b$.

Example

$-27 = (-6) * 5 + 3.$

Proof, existence

Suppose $a, b > 0$. Fix b, induction over a, base case $a < b$, then

$$a = 0 * b + a.$$

Otherwise

$$a = (a - b) + b$$

and ind. hyp. gives

$$a - b = k'b + r', \quad 0 \leq r' < b$$

so

$$a = b + k'b + r' = (1 + k')b + r'.$$

Take $k = 1 + k'$, $r = r'$.

Proof, uniqueness

If

$$a = k_1 b + r_1 = k_2 b + r_2, \quad 0 \leq r_1, r_2 < b$$

then

$$0 = a - a = (k_1 - k_2) b + r_1 - r_2$$

hence

$$(k_1 - k_2) b = r_2 - r_1$$

$|RHS| < b$, so $|LHS| < b$, hence $k_1 = k_2$. But then $r_1 = r_2$.

Example

$a = 23, b = 5.$

$$\begin{aligned} 23 &= 5 + (23 - 5) = 5 + 18 \\ &= 5 + 5 + (18 - 5) = 2 * 5 + 13 \\ &= 2 * 5 + 5 + (13 - 5) = 3 * 5 + 8 \\ &= 3 * 5 + 5 + (8 - 5) = 4 * 5 + 3 \end{aligned}$$

$k = 4,\ r = 3.$

Greatest common divisor

Definition

$a, b \in \mathbb{Z}$. The greatest common divisor of a and b, $c = \gcd(a, b)$, is defined by

1. $c|a \wedge c|b$,
2. If $d|a \wedge d|b$, then $d \leq c$.

If we restrict to $\mathbb{P}$, the the last condition can be replaced with

2' If $d|a \wedge d|b$, then $d|c$.

Bezout's theorem

Theorem (Bezout)

Let $d = \gcd(a, b)$. *Then exists (not unique)* $x, y \in \mathbb{Z}$ *so that*

$$ax + by = d.$$

Proof.

$S = \{ ax + by | x, y \in \mathbb{Z} \}$, $d = \min S \cap \mathbb{P}$. If $t \in S$, then $t = kd + r$, $0 \leq r < d$. So $r = t - kd \in S \cap \mathbb{N}$. Minimiality of d, $r < d$ gives $r = 0$. So $d|t$.

But $a, b \in S$, so $d|a$, $d|b$, and if ℓ another common divisor then $a = \ell u$, $b = \ell v$, and

$$d = ax + by = \ell ux + \ell vy = \ell(ux + vy)$$

so $\ell | d$. Hence d is **greatest** common divisor. □

Étienne Bézout

Lemma

If $a = kb + r$ *then* $\gcd(a, b) = \gcd(b, r)$.

Proof.

If $c|a$, $c|b$ then $c|r$.

If $c|b$, $c|r$ then $c|a$. $\square$

Extended Euclidean algorithm, example

$$\begin{aligned} 27 &= 3 * 7 + 6 \\ 7 &= 1 * 6 + 1 \\ 6 &= 6 * 1 + 0 \end{aligned}$$

$$\begin{aligned} 6 &= 1 * 27 - 3 * 7 \\ 1 &= 7 - 1 * 6 \\ &= 7 - (27 - 3 * 7) \\ &= (-1) * 27 + 4 * 7 \end{aligned}$$

Xgcd

Algorithm

1. Initialize: Set $x = 1, y = 0, r = 0, s = 1$.
2. Finished?: If $b = 0$, set $d = a$ and terminate.
3. Quotient and Remainder: Use Division algorithm to write $a = qb + c$ with $0 \leq c < b$.
4. Shift: Set $(a, b, r, s, x, y) = (b, c, x - qr, y - qs, r, s)$ and go to Step 2.

Lemma

$\gcd(an, bn) = |n| \gcd(a, b)$.

Proof

Assume $a, b, n \in \mathbb{P}$. Induct on $a + b$. Basis: $a = b = 1$, $\gcd(a, b) = 1$, $\gcd(an, bn) = n$, OK.
Ind. step: $a + b > 2$, $a \geq b$.

$$a = kb + r, \quad 0 \leq r < b$$

Since $a \geq b$, $k > 0$.

Then

$$\gcd(a, b) = \gcd(b, r)$$
$$\gcd(an, bn) = \gcd(bn, rn)$$

since

$$an = kbn + rn, \quad 0 \leq rn < bn.$$

But

$$b + r = b + (a - kb) = a - b(k - 1) \leq a < a + b,$$

so ind. hyp. gives

$$n\gcd(b, r) = \gcd(bn, rn).$$

But $LHS = n\gcd(a, b)$, $RHS = \gcd(an, bn)$.

Lemma

If $a|bc$ and $\gcd(a,b) = 1$ then $a|c$.

Proof.

$$1 = ax + by,$$

so

$$c = axc + byc.$$

Since $a|RHS$, $a|c$. $\square$

Lemma

p prime, $p|ab$. Then $p|a$ or $p|b$.

Proof.

If $p \not| a$ then $\gcd(p, a) = 1$. Thus $p|b$ by previous lemma. $\square$

Infinitude of primes

Theorem (Euclides)

Every n is a product of primes. There are infinitely many primes.

Proof.

1 is regarded as the empty product. Ind on n. If n prime, OK. Otherwise, $n = ab$, $a, b < n$. So a, b product of primes. Combine.
Suppose $p_1, p_2, \ldots, p_s$ are known primes. Put

$$N = p_1 p_2 \cdots p_s + 1,$$

then $N = kp_i + 1$ for all known primes, so no known prime divide N. But N is a product of primes, so either prime, or product of unknown primes. □

Example

$$2 * 3 * 5 + 1 = 31$$

$$2 * 3 * 5 * 7 + 1 = 211$$

$$2 * 3 * 5 * 7 * 11 * 13 + 1 = 59 * 509$$

Example

$$2 * 3 * 5 + 1 = 31$$

$$2 * 3 * 5 * 7 + 1 = 211$$

$$2 * 3 * 5 * 7 * 11 * 13 + 1 = 59 * 509$$

Example

$$2 * 3 * 5 + 1 = 31$$
$$2 * 3 * 5 * 7 + 1 = 211$$
$$2 * 3 * 5 * 7 * 11 * 13 + 1 = 59 * 509$$

Fundamental theorem of arithmetic

Theorem

For any $n \in \mathbb{P}$, can uniquely (up to reordering) write

$$n = p_1 p_2 \cdots p_s, \qquad p_i \text{ prime }.$$

Proof.

Existence, Euclides. Uniqueness: suppose

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdot q_r.$$

Since $p_1 | n$, we have $p_1 | q_1 q_2 \cdots q_r$, which by lemma yields $p_1 | q_j$ some q_j, hence $p_1 = q_j$. Cancel and continue. $\square$

Exponent vectors

- Number the primes in increasing order, $p_1 = 2, p_2 = 3, p_3 = 5$, et cetera.
- Then $n = \prod_{j=1}^{\infty} p_j^{a_j}$, all but finitely many a_j zero.
- Let $v(n) = (a_1, a_2, a_3, \ldots)$ be this integer sequence.
- Then $v(nm) = v(n) + v(m)$.
- Order componentwise, then $n|m \iff v(n) \leq v(m)$.
- Have $v(\gcd(n, m)) = \min(v(n), v(m))$.

Example

$$
\begin{aligned}
\gcd(100, 130) &= \gcd(2^2 * 5^2, 2 * 5 * 13) \\
&= 2^{\min(2,1)} * 5^{\min(2,1)} * 13^{\min(0,1)} \\
&= 2^1 * 5^1 * 13^0 \\
&= 10
\end{aligned}
$$

Definition

- $a, b \in \mathbb{Z}$
- $m = \mathrm{lcm}(a, b)$ least common multiple if
  1. $m = ax = by$ (common multiple)
  2. If n common multiple of a, b then $m|n$

Lemma (Easy)

- $a, b \in \mathbb{P}$, $c, d \in \mathbb{Z}$
- $lcm(\prod_j p_j^{a_j}, \prod_j p_j^{b_j}) = \prod_j p_j^{\max(a_j, b_j)}$
- $ab = \gcd(a, b) lcm(a, b)$
- *If* $a|c$ *and* $b|c$ *then* $lcm(a, b)|c$
- *If* $c \equiv d \mod a$ *and* $c \equiv d \mod b$ *then* $c \equiv d \mod lcm(a, b)$