Number Theory, Lecture 1

Integers, Divisibility, Primes

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Summary

Summary

Definition

- $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$
- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- $\mathbb{P} = \{1, 2, 3, \ldots\}$

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 $12 = 3 * 4$.

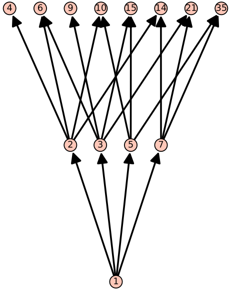
Lemma

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

Theorem

Retricted 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

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

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 $t = kd + r$, $0 \le r < d$. 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. $\square$

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: $a + b > 2$, $a \geq b$.

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

If $k = 0$, OK. Assume $k > 0$.

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)

Ever 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. $\square$

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. □

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 $v(n) = (a_1, a_2, a_3, \dots)$ 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

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

Lemma (Easy)

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

Algorithm

1. Given N, find all primes $\leq N$
2. $X = [2, N]$, $i = 1$, $P = \emptyset$
3. $p_i = \min(X)$.
4. Remove multiples of p_i from X
5. $P = P \cup \{p_i\}$
6. If $p_i \geq \sqrt{N}$, then terminate, otherwise $i = i + 1$, goto 3.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

- Any number have remainder 0,1,2, or 3, when divided by 4
- Except for 2, all primes are odd
- Thus, primes > 2 are either of the form $4n+1$ or $4n+3$
- $4n+3 = 4(n+1) - 1 = 4m - 1$.

Theorem

There are infinitely many primes of the form $4m-1$.

Proof

Proof.

Let $q_1, \ldots, q_r$ be the known such primes, put

$$N = 4q_1 q_2 \cdots q_r - 1$$

Then N odd, not divisible by any q_j. Factor N into primes:

$$N = u_1 u_2 \cdots u_s$$

If all $u_i = 4m_i + 1$ then

$$N = (4m_1 + 1)(4m_2 + 1) \cdots (4m_s + 1) = 4m + 1,$$

a contradiction. So some $u_j = 4m_j - 1$, $u_j | N$ so $u_j \not\in \{q_1, \ldots, q_r\}$, hence new. $\square$

Theorem (Dirichlet)

$a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$. *Then $a\mathbb{Z} + b$ contains infinitely many primes.*

Example

Obviously $6\mathbb{Z} + 3$ contains only one prime, 3, so condition necessary.

Dirichlet