Lecture 7

INTEGERS

Division Algorithm

Theorem

Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = qb + r$.
We call q and r the **quotient** *and* **remainder** *of a when divided by b respectively.*

Notation

We shall denote the quotient of a when divided by b as $a \mathbf{\ div\ } b$ and the remainder of a when divided by b as $a \bmod b$.

Proof.

1. Let $q = \lfloor \frac{a}{b} \rfloor$.
2. Then $q \in \mathbb{Z}$ and $q \leq \frac{a}{b} < q + 1$.
3. Thus $qb \leq a < qb + b$, or $0 \leq a - qb < b$.
4. Let $r = a - qb$. Then $a = qb + r$, and $r \in \mathbb{Z}$ (since $a, q, b \in \mathbb{Z}$) with $0 \leq r < b$ (from (3)).
5. If $q', r' \in \mathbb{Z}$ such that $0 \leq r' < b$ and $a = q'b + r'$, then:
   1. $q'b \leq a < q'b + b = (q' + 1)b$.
   2. $q' \leq \frac{a}{b} < q' + 1$.
   3. Since $q' \in \mathbb{Z}$, (5.2) implies that $q' = \lfloor \frac{a}{b} \rfloor = q$.
   4. $r' = a - q'b = a - qb = r$.
6. Thus q and r are unique.

□

Note

From the above proof, we see that $a \operatorname{\mathbf{div}} b = \lfloor \frac{a}{b} \rfloor$.

Division Algorithm for Negative Divisors

Let $a, b \in \mathbb{Z}$ with $b < 0$. By the division algorithm, we get

$$a = q|b| + r = q(-b) + r = (-q)b + r,$$

where $q = a \textbf{ div } |b|$ and $r = a \textbf{ mod } |b|$.

Thus we define $a \textbf{ div } b = -(a \textbf{ div } |b|)$ and $a \textbf{ mod } b = a \textbf{ mod } |b|$ when $b < 0$.

Exercise

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Prove that:

1. $a \textbf{ div } (-b) = -(a \textbf{ div } b)$.
2. $a \textbf{ mod } (-b) = a \textbf{ mod } b$.
3. $a \textbf{ mod } b = 0$ if and only if $\frac{a}{b} \in \mathbb{Z}$.

b-adic Expansion

Definition

Let $b, n \in \mathbb{Z}^+$ with $b \geq 2$. We say that n has a **b-adic expansion** (or **b-adic decomposition**) if there exist $k \in \mathbb{Z}^+$, $a_0, a_1, \ldots, a_k \in \mathbb{Z}$ with $1 \leq a_k < b$ and $0 \leq a_0, a_1, \ldots, a_{k-1} < b$ such that

$$n = a_0 b^0 + a_1 b^1 + \cdots + a_k b^k,$$

in which case, $a_0 b^0 + a_1 b^1 + \cdots + a_k b^k$ is a b-adic expansion of n.

Example

- $4 = 1(3^0) + 1(3^1)$ is a 3-adic expansion of 4.
- $9 = 1(2^0) + 1(2^3)$ is a 2-adic expansion of 9.

Theorem (Existence of b-adic expansion)

Let $b \in \mathbb{Z}_{\geq 2}$. Every $n \in \mathbb{Z}^+$ has a b-adic expansion.

Proof by strong induction.

1. For each $n \in \mathbb{Z}^+$, let $P(n) = (n$ has a b-adic expansion$)$.
2. $P(1)$ is true, since $1 = 1 \cdot b^0$.
3. Assume $P(1), P(2), \ldots, P(n)$.
4. Let $q = (n+1)$ **div** b and $r = (n+1)$ **mod** b. Then $q, r \in \mathbb{Z}$ with $0 \leq q \leq n$ and $0 \leq r < b$, and $n+1 = qb + r$.
5.
    1. Case 1: $q = 0$. Then $n+1 = r = rb^0$, a b-adic expansion of $n+1$. Thus $P(n+1)$ is true.
    2. Case 2: $q > 0$. By (3) and (4), $P(q)$ is true, so $q = a_0 b^0 + a_1 b^1 + \cdots + a_k b^k$. Then $n+1 = qb + r = rb^0 + a_0 b^1 + a_1 b^2 + \cdots + a_k b^{k+1}$ is a b-adic expansion of $n+1$, so $P(n+1)$ is true.
6. In all cases, $P(n+1)$ is true.
7. By (strong) MI, $P(n)$ is true for all $n \in \mathbb{Z}^+$.

$\square$

Theorem (Uniqueness of b-adic expansion)

Let $b, n \in \mathbb{Z}^+$ with $b \geq 2$. The b-adic expansion of n is unique.

Proof.

1. Let $\sum_{i=0}^{k} a_i b^i$ and $\sum_{i=0}^{l} a_i' b^i$ be two b-adic expansion of n.
2. Let $N = \max\{k, l\}$, and define $a_i = 0 = a_j'$ for all $i, j \in \mathbb{Z}$ with $k < i \leq N$ and $l < j \leq N$.
3. Then $\sum_{i=0}^{N} a_i b^i = n = \sum_{i=0}^{N} a_i' b^i$.
4. If $I := \{i \in \mathbb{Z} \mid 0 \leq i \leq N,\ a_i \neq a_i'\} \neq \varnothing$ then:
    1. Let $m = \max(I)$. Then $a_j = a_j'$ for all $j \in \mathbb{Z}$ with $m < j \leq N$.
    2. WLOG, assume $a_m < a_m'$, and so $a_m + 1 \leq a_m'$.
    3. Then

$$\begin{aligned} n = \sum_{i=0}^{m-1} a_i b^i + \sum_{i=m}^{N} a_i b^i &\leq \sum_{i=0}^{m-1} (b-1) b^i + \sum_{j=m}^{N} a_j b^j = b^m - 1 + \sum_{j=m}^{N} a_j b^j \\ &< (a_m + 1) b^m + \sum_{j=m+1}^{N} a_j b^j \leq a_m' b^m + \sum_{j=m+1}^{N} a_j' b^j \\ &\leq \sum_{i=0}^{N} a_i' b^i = n, \qquad \text{a contradiction.} \end{aligned}$$

5. Thus, $I = \varnothing$, and so $a_i = a_i'$ for all $i \in \mathbb{Z}$ with $0 \leq i \leq N$.

$\square$

b-adic Expansion Algorithm

To compute $a_0, a_1, \ldots, a_k$ in the b-adic expansion of $n = \sum_{i=0}^{k} a_i b^i$, we use the following algorithm:

1. while $n > 0$ do
    1. return $(n \textbf{ mod } b)$;
    2. $n := (n \textbf{ div } b)$;
2. enddo.

This uses the fact that $n \textbf{ mod } b = a_0$ (the coefficient of b^0 in the b-adic expansion of n) and $n \textbf{ div } b = \sum_{i=1}^{k} a_i b^{i-1}$, since

$$n = (\sum_{i=1}^{k} a_i b^{i-1})b + a_0,$$

and $a_0 \in \mathbb{Z}$ with $0 \leq a_0 < b$.

Example

We compute the 3-adic expansion of 143.

143	2
47	2
15	0
5	2
1	1
0	

Thus, $143 = 2(3^0) + 2(3^1) + 2(3^3) + 1(3^4)$.

Base b Representation

If $n = \sum_{i=0}^{k} a_i b^i$ is the b-adic expansion of n, we sometimes write

$$n = (a_k a_{k-1} \cdots a_0)_b.$$

This is the **base b representation** of n.

The names for the common b's for which we use such representations are:

b	Name
10	decimal
2	binary
3	ternary
8	octal
16	hexadecimal

In hexadecimal, the letters A, B, C, D, E, F are used to represent $10, 11, 12, 13, 14, 15$ respectively.

Example

We compute the binary and hexadecimal representation of 143.

143	1
71	1
35	1
17	1
8	0
4	0
2	0
1	1
0	

143	15
8	8
0	

Thus, $143 = (10001111)_2 = (8\mathsf{F})_{16}$.

We can also get the ternary representation of 143 from the 3-adic expansion of 143 worked out earlier: $143 = (12022)_3$.

Divisibility

Definition

Let $a, b \in \mathbb{Z}$. We say that a **divides** b (or a is a **divisor of** b, or b is **divisible by** a, or b is a **multiple of** a) if, and only if, there exists $k \in \mathbb{Z}$ such that $b = ak$.

Caution!

Ex: 0 | 0 but 0/ 0 doesn't exist.

$a \mid b$ is neither equivalent to $\frac{b}{a} \in \mathbb{Z}$ nor $b \ \mathbf{mod}\ a = 0$.

Example

Let $n \in \mathbb{Z}$.

1. Then $1 \mid n$ and $n \mid n$ (since $n = 1 \cdot n$), and $n \mid 0$ (since $0 = n(0)$).
2. If $n \mid 1$, then $n = \pm 1$.
3. If $0 \mid n$, then $n = 0$.

Lemma

Let $a, b, c \in \mathbb{Z}$.

1. $(a \mid b) \Leftrightarrow (-a \mid b) \Leftrightarrow (a \mid -b) \Leftrightarrow (-a \mid -b)$.
2. $(a \mid b) \wedge (b \mid a) \Rightarrow (a = b \vee a = -b)$.
3. $(a \mid b) \wedge (b \mid c) \Rightarrow (a \mid c)$.
4. $(a \mid b) \Rightarrow (ac \mid bc)$.
5. $(ac \mid bc) \wedge (c \neq 0) \Rightarrow (a \mid b)$.
6. $(a \mid b) \wedge (b \neq 0) \Rightarrow (|a| \leq |b|)$.

Proof.

Easy exercise. □

Common Divisors

Definition

Let $a, b, d \in \mathbb{Z}$. We say that d is a **common divisor** of a and b if and only if $(d \mid a) \wedge (d \mid b)$.

Example

1. The common divisors of 4 and 6 are ± 1 and ± 2.
2. Let $a, b, d \in \mathbb{Z}$. Then d is a common divisor of a and b if and only if $|d|$ is a common divisor of $|a|$ and $|b|$.

Lemma

Let $a, b, d \in \mathbb{Z}$. If d is a common divisor of a and b, then $d \mid (ax + by)$ for all $x, y \in \mathbb{Z}$.

Proof.

If $a = kd$ and $b = ld$ (where $k, l \in \mathbb{Z}$), then
$ax + by = kdx + ldy = d(kx + ly)$. Thus, if $x, y \in \mathbb{Z}$, then $kx + ly \in \mathbb{Z}$, so that $d \mid (ax + by)$. □

Note

An expression of the form $ax + by$ is called a (real) **linear combination** of a and b. The lemma above says a common divisor of a and b divides all **integer** linear combinations of a and b.

Greatest Common Divisor

Definition

Let $a, b \in \mathbb{Z}$. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is a common divisor of a and b that is the largest among all the common divisors of a and b.

Note

1. Let $D(a)$ (resp. $D(b)$) denote the set of divisors of a (resp. b), and let $CD(a, b)$ denote the set of common divisors of a and b.
   Suppose that $a \in \mathbb{Z}$ with $a \neq 0$. Then $D(a) \subseteq \{d \in \mathbb{Z} : |d| \leq |a|\}$, so that $D(a)$ is a finite set.
   Thus since $CD(a, b) = D(a) \cap D(b) \subseteq D(a)$, we see that $CD(a, b)$ is also a finite set, and is non-empty since $1 \in CD(a, b)$. Hence $\gcd(a, b)$ exists and is of course unique. Furthermore, $\gcd(a, b) > 0$.
2. $\gcd(0, 0)$ is undefined.

Example

1. If $a \in \mathbb{Z}$ with $a \neq 0$, then $\gcd(a,0) = |a| = \gcd(a,a)$.
2. If $a,b \in \mathbb{Z}$ with $a \neq 0$ and $a \mid b$, then $\gcd(a,b) = |a|$.
3. If $a,b \in \mathbb{Z}$ not both 0, then $\gcd(a,b) = \gcd(|a|,|b|)$.

Lemma

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then $\gcd(a, b) = \gcd(b, a - bx)$ for all $x \in \mathbb{Z}$. In particular, $\gcd(a, b) = \gcd(b, a \bmod b)$.

Proof.

1. If $x \in \mathbb{Z}$ then
   1. If d is a common divisor of a and b, then $d \mid b$ and $d \mid a(1) + b(-x) = a - bx$, so that d is a common divisor of b and $a - bx$.
   2. If d' is a common divisor of b and $a - bx$, then $d' \mid bx + (a - bx)(1) = a$ and $d' \mid b$, so that d' is a common divisor of a and b.
   3. By (1.1) and (1.2), the sets of common divisors of a and b, and of b and $a - bx$ are the same, and hence the largest elements in these two sets are the same.
   4. By definition of gcd, we have $\gcd(a, b) = \gcd(b, a - bx)$.
2. Let $x = a \operatorname{\mathbf{div}} b$. Then $x \in \mathbb{Z}$ and $a - bx = a \bmod b$. Now apply (1.4).

$\square$

Euclidean Algorithm

Consider the following algorithm:

1. while not ($a \mathbf{~mod~} b = 0$) do
   1. $r := a \mathbf{~mod~} b$;
   2. $a := b$;
   3. $b := r$;
2. enddo;
3. return $|b|$;

Let a_0 and b_0 ($\neq 0$) be the input values of a and b, and let a_i and b_i be the values of a and b after the i-th cycle in the above while loop. Then $b_i \in \mathbb{Z}^+$ and $b_i < b_{i-1}$, so that the while loop must terminate, say after m cycles (i.e. $a_m \mathbf{~mod~} b_m = 0$), and the algorithm returns $|b_m|$.

By the last lemma, we have $\gcd(a_{i-1}, b_{i-1}) = \gcd(a_i, b_i)$ for all i. Thus, $\gcd(a_0, b_0) = \gcd(a_m, b_m) = |b_m|$.

The above algorithm, called the **Euclidean algorithm**, thus computes $\gcd(a_0, b_0)$.

Theorem (Bézout's Identity)

(x, y) can be < 0

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then $\gcd(a, b)$ is an integer linear combination of a and b, i.e.

$$\exists x, y \in \mathbb{Z}\ \big(ax + by = \gcd(a, b)\big).$$

Proof by induction.

1. Let $P(n) =$ ('if the Euclidean algorithm takes n cycles in the while loop to compute $\gcd(a, b)$, then $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$').
2. $P(0)$ is true since if it takes 0 cycles then $\gcd(a, b) = |b| = a(0) + b(\pm 1)$.
3. Assume $P(n)$.
4. Suppose that it takes $n + 1$ cycles to compute $\gcd(a, b)$.
5. Then it takes n cycles to compute $\gcd(a_1, b_1)$, where a_1 and b_1 are the values of a and b after the first cycle.
6. Applying $P(n)$, $\gcd(a_1, b_1) = a_1x + b_1y$ for some $x, y \in \mathbb{Z}$.
7. $\gcd(a, b) = \gcd(a_1, b_1) = a_1x + b_1y = bx + (a \bmod b)y = bx + (a - qb)y = ay + b(x - qy)$. Since $y, x - qy \in \mathbb{Z}$, $P(n + 1)$ is true.
8. By MI, $P(n)$ is true for all $n \in \mathbb{Z}_{\geq 0}$.

$\square$

Euclidean Algorithm in Action

Example

Compute $\gcd(12091, 10807)$ and express it as an integer linear combination of 12091 and 10807.

Solution:

$$\begin{aligned}
12091 &= 1(10807) + 1284; \\
10807 &= 8(1284) + 535; \\
1284 &= 2(535) + 214; \\
535 &= 2(214) + 107; \\
214 &= 2(107) + 0.
\end{aligned}$$

$$\begin{aligned}
107 &= 535 - 2(214); \\
&= 535 - 2(1284 - 2(535)) = 5(535) - 2(1284); \\
&= 5(10807 - 8(1284)) - 2(1284) = 5(10807) - 42(1284); \\
&= 5(10807) - 42(12091 - 1(10807)) = 47(10807) - 42(12091).
\end{aligned}$$

Thus, $\gcd(12091, 10807) = 107 = (12091)(-42) + (10807)(47)$.

Corollary

Let $a, b \in \mathbb{Z}$, not both 0.

1. *Every common divisor of a and b divides $\gcd(a, b)$.*
2. $\gcd(a, b) = \min\{n \in \mathbb{Z}^+ \mid \exists x, y \in \mathbb{Z}\ (n = ax + by)\}$.

Proof.

1. Any common divisor of a and b divides all integer linear combinations of a and b.
2. $\gcd(a, b)$ is an integer linear combination of a and b (Bézout's Identity).
3. By (1) and (2), any common divisor of a and b divides $\gcd(a, b)$ (universal instantiation), giving part (1).
4. Let $S = \{n \in \mathbb{Z}^+ \mid \exists x, y \in \mathbb{Z}\ (n = ax + by)\}$.
5. By (2), $\gcd(a, b) \in S$.
6. If $n \in S$, then:
   1. $n = ax + by$ for some $x, y \in \mathbb{Z}$, so $\gcd(a, b) \mid n$ by (1).
   2. $\gcd(a, b) = |\gcd(a, b)| \leq |n| = n$, since $\gcd(a, b), n > 0$.
7. By (5) and (6.2), $\gcd(a, b) = \min(S)$, giving part (2).

□

Corollary

Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b) = 1$ if and only if there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Proof.

1. By Bézout's Identity, if $\gcd(a, b) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$.
2. Conversely, if there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$, then $1 \in \{n \in \mathbb{Z}^+ \mid \exists x, y \in \mathbb{Z}\ (n = ax + by)\}$, so that

   $$1 = \min\{n \in \mathbb{Z}^+ \mid \exists x, y \in \mathbb{Z}\ (n = ax + by)\} = \gcd(a, b)$$

   by the part (2) of the last corollary.

$\square$

Primes

Recall that:

- An integer $n \in \mathbb{Z}^+$ is **composite** if there exists $a, b \in \mathbb{Z}^+$ with $1 < a, b < n$ such that $n = ab$.
- An integer $n \in \mathbb{Z}$ is **prime** if $n \geq 2$ and n is not composite.

Note

An alternative definition of a prime integer:
A positive integer that has exactly two positive integer divisors (namely, 1 and itself).

Lemma

Let p and q be two prime integers. If $p \mid q$ then $p = q$.

Proof.

Since q is prime, q has exactly two positive integer divisors, namely q and 1. If $p \mid q$ then p is a positive integer divisor of q, and $p \neq 1$, so $p = q$. $\square$

Theorem

There are infinitely many prime integers.

Proof by contradiction.

1. Suppose that there exist only finite many prime integers; let them be $p_1, p_2, \ldots, p_k$.
2. Consider $N = p_1 p_2 \cdots p_k + 1$.
3. Since $N \in \mathbb{Z}_{\geq 2}$, it can be factorised into primes (Slide 14 of LECT6-1.pdf).
4. So there exists a prime integer p such that $p \mid N$.
5. By (1), $p = p_i$ for some $1 \leq i \leq k$.
6. By (5) and (2), $p \mid p_1 p_2 \cdots p_k = N - 1$.
7. By (4) and (6), $p \mid (N(1) + (N-1)(-1)) = 1$, a contradiction.

□

Lemma

Let p be a prime integer, and let $n \in \mathbb{Z}$. Then

$$\gcd(p, n) = \begin{cases} p, & \text{if } p \mid n; \\ 1, & \text{otherwise.} \end{cases}$$

Proof.

1. If $p \mid n$, then $\gcd(p, n) = |p| = p$.
2. If $p \nmid n$, then since p has only two positive divisors, namely 1 and p, 1 is the only positive common divisor of p and n. Thus $\gcd(p, n) = 1$.

$\square$

Definition

Let $a, b \in \mathbb{Z}$. We say that a and b are **coprime** (or **relatively prime**) if, and only if, $\gcd(a, b) = 1$.

Example

1. 3 and 4 are coprime. 4 and 6 are not coprime.
2. If $p, n \in \mathbb{Z}$ with p prime, then either $p \mid n$ or (p and n are coprime).
3. If $a, b \in \mathbb{Z}$, then a and b are coprime if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Lemma

Let $a, b, c \in \mathbb{Z}$, with a and b coprime.

1. *If a and c are coprime, then a and bc are coprime.*
2. *If $a \mid bc$, then $a \mid c$.*

Proof.

Since a and b are coprime, there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

1. If a and c are coprime, then $ax' + cy' = 1$ for some $x', y' \in \mathbb{Z}$, so that $by(ax' + cy') = by = 1 - ax$, giving $a(x + byx') + bc(yy') = 1$. Hence $\gcd(a, bc) = 1$ since $x + byx', yy' \in \mathbb{Z}$.
2. If $bc = ka$ for some $k \in \mathbb{Z}$, then since $c(ax + by) = c$, we get $c = acx + bcy = acx + kay = a(cx + ky)$, so that $a \mid c$ since $cx + ky \in \mathbb{Z}$.

$\square$

Corollary

Let $a, b, p \in \mathbb{Z}$ with p prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof by division into cases.

If $p \mid ab$, then:

1. Case 1 : $p \mid a$. Then $p \mid a$ or $p \mid b$ (generalisation).
2. Case 2 : $p \nmid a$. Then p and a are coprime, so that part (2) of the last lemma applies to give $p \mid b$. Thus $p \mid a$ or $p \mid b$ (generalisation).

In all cases, $p \mid a$ or $p \mid b$. $\square$

Corollary

Let $n, p \in \mathbb{Z}^+$ with p prime. If $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and $p \mid a_1 a_2 \cdots a_n$ then $p \mid a_i$ for some $i \in \{1, 2, \ldots, n\}$.

Proof by induction on n.

Exercise. $\square$

Theorem

Let $k \in \mathbb{Z}^+$. If $l \in \mathbb{Z}^+$ and $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$ are prime integers such that $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, then $k = l$, and after reordering the q_j's if necessary, $p_1 = q_1$, $p_2 = q_2$, ..., $p_k = q_k$.

Proof by induction on k.

1. For each $k \in \mathbb{Z}^+$, let $P(k)$ be the statement of the theorem.
2. For $P(1)$, if $p_1 = q_1 q_2 \cdots q_l$ where $p_1, q_1, q_2, \ldots, q_l$ are prime integers, then $l = 1$ (otherwise p_1 is composite, a contradiction), and so $p_1 = q_1$. Thus $P(1)$ is true.
3. Assume $P(k)$.

continue on next frame ...

Proof.

5. For $P(k+1)$, if $p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_l$ where $p_1, p_2, \ldots, p_{k+1}, q_1, q_2, \ldots, q_l$ are prime integers, then:
    1. $p_{k+1} \mid p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_l$, so that $p_{k+1} \mid q_j$ for some j.
    2. Thus $p_{k+1} = q_j$ by the Lemma on Slide 25.
    3. By reordering if necessary, we may assume $j = l$, i.e. $p_{k+1} = q_l$.
6. Cancelling p_{k+1} and q_l from $p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_l$, we get $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_{l-1}$.
7. By $P(k)$, $l - 1 = k$ and, after reordering if necessary, $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_k = q_k$.
8. Since $l - 1 = k$, $p_{k+1} = q_l = q_{k+1}$.
9. Thus $P(k+1)$ is true.
10. By MI, $P(k)$ is true for all $k \in \mathbb{Z}^+$.

$\square$

Fundamental Theorem of Arithmetic

Theorem

Every $n \in \mathbb{Z}_{\geq 2}$ can be factorised uniquely (up to order) into primes.

Proof.

Existence of prime factorisation is proved in Slide 14 of LECT6-1.pdf.
Uniqueness of prime factorisation is the subject of the last Theorem. □

Let $a, b \in \mathbb{Z}^+$. Using the fundamental theorem of arithmetic, we can find distinct prime integers $p_1, p_2, \ldots, p_k$, $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k \in \mathbb{Z}_{\geq 0}$ such that

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$
$$b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

Lemma

$a \mid b$ if and only if $a_1 \le b_1$, $a_2 \le b_2$, $\ldots$, $a_k \le b_k$.

Proof.

1. If $a_1 \le b_1$, $a_2 \le b_2$, $\ldots$, $a_k \le b_k$, then $a = bc$ where $c = p_1^{b_1-a_1} p_2^{b_2-a_2} \cdots p_k^{b_k-a_k} \in \mathbb{Z}$, so that $a \mid b$.
2. If $a \mid b$, say $b = ac$ where $c \in \mathbb{Z}$, then $c = \frac{b}{a} > 0$ so that $c \in \mathbb{Z}^+$.
   1. Case 1: $c = 1$. Then $a = b$, so that $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_k = b_k$ by uniqueness of prime factorisation.
   2. Case 2: $c \ge 2$. Since $c \mid b$, every prime divisor of c divides b, and so divides one of the prime divisors p_i of b by Slide 30, and hence equals to p_i by Slide 25. Thus $c = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$ for some $c_1, c_2, \ldots, c_k \in \mathbb{Z}_{\ge 0}$, and so

      $$\begin{aligned} p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} = b = ac &= (p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k})(p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}) \\ &= p_1^{a_1+c_1} p_2^{a_2+c_2} \cdots p_k^{a_k+c_k}. \end{aligned}$$

      By the uniqueness of prime factorisation of b, we get $b_1 = a_1 + c_1 \ge a_1$, $b_2 = a_2 + c_2 \ge a_2$, $\ldots$, $b_k = a_k + c_k \ge a_k$.

$\square$

Corollary

$$\gcd(a, b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_k^{\{a_k,b_k\}}.$$

Proof.

1. Let $D = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_k^{\{a_k,b_k\}}$.
2. By the last Lemma, $D \mid a$ and $D \mid b$.
3. If $d \mid a$ and $d \mid b$, then
   1. case 1: $d \leq 0$. Then $d < D$, since $D \geq 1$.
   2. case 1: $d > 0$. Then by the last lemma, $d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$, with $d_1 \leq a_1, b_1$, $d_2 \leq a_2, b_2$, …, $d_k = a_k, b_k$. Thus, $d_1 \leq min\{a_1, b_1\}$, $d_2 \leq \min\{a_2, b_2\}$, …, $d_k = \min\{a_k, b_k\}$, and hence

$$d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} \leq p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_k^{\{a_k,b_k\}} = D.$$

   In all cases, $d \leq D$.
4. Thus $D = \gcd(a, b)$.

□

Remarks

By the last Corollary, one can compute $\gcd(a, b)$ by finding the prime factorisations of a and b. This method is very fast for small numbers. However, for large numbers, determining their prime factorisations is VERY difficult, and the Euclidean algorithm is a very efficient method of computing their $\gcd$.

Summary

We have covered:

- Division algorithm
- b-adic expansion and base b representation
- Divisibility
- Common divisors and gcds
- Euclidean algorithm and Bézout's Identity
- Infinitude of primes
- Fundamental Theorem of Arithmetic