CENG 535 - Computational Number Theory

Basic Properties of the Integers

Hüseyin Hışıl
huseyinhisil.net
huseyin.hisil@yasar.edu.tr

Faculty of Engineering, Computer Engineering Department,
Yasar University, Izmir

Fall, 2012-2013

Outline

Declaration

These slides are heavily dependent on Victor Shoup's freely available book:

`http://shoup.net/ntb/ntb-v2.pdf`

A Computational Introduction to Number Theory and Algebra

2$^{\text{nd}}$ Edition, New York University, ISBN: 9780521516440

Publication date: December 2008

Declaration

Special thanks goes to **Bünyamin İzzet İnan** for helping the instructor with the preparation of these slides.

Outline

Divisibility

A central concept in number theory is divisibility.

Consider the integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

For $a, b \in \mathbb{Z}$, we say that a divides b if $az = b$ for some $z \in \mathbb{Z}$.

If a divides b, we write $a \mid b$, and we may say that a is a divisor of b, or that b is a multiple of a, or that b is divisible by a.

If a does not divide b, then we write $a \nmid b$.

0/0 is defined and it is called the indeterminate.

6/0 is undefined!

Divisibility

Theorem 1 (p1,t1.1)

For all $a,b,c \in \mathbb{Z}$, we have

1. $0 \mid a$ *if and only if* $a = 0$,
2. $a \mid a$, $1 \mid a$, *and* $a \mid 0$,
3. $a \mid b$ *if and only if* $-a \mid b$ *if and only if* $a \mid -b$,
4. $a \mid b$ *and* $a \mid c$ *implies* $a \mid (b+c)$,
5. $a \mid b$ *and* $b \mid c$ *implies* $a \mid c$.

Divisibility

Theorem 1 (p1,t1.1)

For all $a, b, c \in \mathbb{Z}$, we have

1. $0 \mid a$ *if and only if* $a = 0$,
2. $a \mid a$, $1 \mid a$, *and* $a \mid 0$,
3. $a \mid b$ *if and only if* $-a \mid b$ *if and only if* $a \mid -b$,
4. $a \mid b$ *and* $a \mid c$ *implies* $a \mid (b + c)$,
5. $a \mid b$ *and* $b \mid c$ *implies* $a \mid c$.

These properties can be easily derived from the definition of divisibility, We leave the proof as an easy exercise.

Divisibility

Statement: If $a \mid b$ and $b \neq 0$, then $1 \leq |a| \leq |b|$.

Divisibility

Statement: If $a \mid b$ and $b \neq 0$, then $1 \leq |a| \leq |b|$.

Proof: Assume $a \cdot z = b \neq 0$ for some integer z. Then $a \neq 0$ and $z \neq 0$; it follows that $1 \leq |a|$, $1 \leq |z|$, and so $|a| \leq |a| \cdot |z| = |b|$. **Q.E.D.**

Divisibility

Statement: If $a \mid b$ and $b \neq 0$, then $1 \leq |a| \leq |b|$.

Proof: Assume $a \cdot z = b \neq 0$ for some integer z. Then $a \neq 0$ and $z \neq 0$; it follows that $1 \leq |a|$, $1 \leq |z|$, and so $|a| \leq |a| \cdot |z| = |b|$. **Q.E.D.**

"Q.E.D."	=	"quod erat demonstrandum"
	=	"which was to be demonstrated"

Divisibility

Theorem 2 (p2,t1.2)

For all $a \neq 0, b \neq 0 \in \mathbb{Z}$,

$$\text{we have } a \mid b \text{ and } b \mid a \text{ if and only if } a = \pm b.$$

Divisibility

Theorem 2 (p2,t1.2)

For all $a \neq 0, b \neq 0 \in \mathbb{Z}$,

$$\textit{we have } a \mid b \textit{ and } b \mid a \textit{ if and only if } a = \pm b.$$

Proof: $:\Leftarrow$ Assume that $a = b$ then $a = 1 \cdot b$ and $b = 1 \cdot a$. By the definition of divisiblity $a \mid b$ and $b \mid a$.
Assume that $a = -b$ then $a = -1 \cdot b$ and $b = -1 \cdot a$. By the definition of divisiblity $a \mid b$ and $b \mid a$.
$:\Rightarrow$ Assume that $a \mid b$ and $b \mid a$. Then, $a \mid b$ implies $|a| \leq |b|$ and $b \mid a$ implies $|b| \leq |a|$. Thus, $|a| = |b|$, and so $a = \pm b$. **Q.E.D.**

Divisibility

Theorem 2 (p2,t1.2)

For all $a \neq 0, b \neq 0 \in \mathbb{Z}$,

$$\textit{we have } a \mid b \textit{ and } b \mid a \textit{ if and only if } a = \pm b.$$

Proof: $:\Leftarrow$ Assume that $a = b$ then $a = 1 \cdot b$ and $b = 1 \cdot a$. By the definition of divisiblity $a \mid b$ and $b \mid a$.
Assume that $a = -b$ then $a = -1 \cdot b$ and $b = -1 \cdot a$. By the definition of divisiblity $a \mid b$ and $b \mid a$.
$:\Rightarrow$ Assume that $a \mid b$ and $b \mid a$. Then, $a \mid b$ implies $|a| \leq |b|$ and $b \mid a$ implies $|b| \leq |a|$. Thus, $|a| = |b|$, and so $a = \pm b$. **Q.E.D.**

Statement: For every $a \in \mathbb{Z}$, we have $a \mid 1$ if and only if $a = \pm 1$.

Divisibility

Theorem 2 (p2,t1.2)

For all $a \neq 0, b \neq 0 \in \mathbb{Z}$,

$$\textit{we have } a \mid b \textit{ and } b \mid a \textit{ if and only if } a = \pm b.$$

Proof: $:\Leftarrow$ Assume that $a = b$ then $a = 1 \cdot b$ and $b = 1 \cdot a$. By the definition of divisiblity $a \mid b$ and $b \mid a$.
Assume that $a = -b$ then $a = -1 \cdot b$ and $b = -1 \cdot a$. By the definition of divisiblity $a \mid b$ and $b \mid a$.
$:\Rightarrow$ Assume that $a \mid b$ and $b \mid a$. Then, $a \mid b$ implies $|a| \leq |b|$ and $b \mid a$ implies $|b| \leq |a|$. Thus, $|a| = |b|$, and so $a = \pm b$. **Q.E.D.**

Statement: For every $a \in \mathbb{Z}$, we have $a \mid 1$ if and only if $a = \pm 1$.

Proof: This follows from the first statement by setting $b := 1$, and noting that $1 \mid a$. **Q.E.D.**

Fundamental theorem of arithmetic

Theorem 3 (p2,t1.3)

Every non-zero integer n can be expressed as

$$n = \pm p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_1, e_2, \ldots, e_r$ are positive integers. Moreover, this expression is unique, up to a reordering of the primes.

We will prove Theorem 3 at the end of this chapter.

Cancellation Law

Statement: The product of any two non-zero integers is again non-zero.

Proof: Exercise on your own.

The above statement leads to the cancellation law:

Statement: If $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $ab = ac$, then $b = c$.

Cancellation Law

Statement: The product of any two non-zero integers is again non-zero.

Proof: Exercise on your own.

The above statement leads to the cancellation law:

Statement: If $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $ab = ac$, then $b = c$.

Proof: Assume $ab = ac \neq 0$. We have $a(b - c) = 0$. So, $a \neq 0$ implies $b - c = 0$, and hence $b = c$. **Q.E.D.**

Primes and Composites

Let n be a positive integer. Trivially, 1 and n divide n.

If $n > 1$ and no other positive integers besides 1 and n divide n, then we say n is prime.

If $n > 1$ but n is not prime, then we say that n is composite.

The number 1 is not considered to be either prime or composite.

Division with remainder property

Theorem 4 (p3,t1.4)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

Proof: Consider the non-empty set S of non-negative integers of the form $a - bt$ with $t \in \mathbb{Z}$. Since every non-empty set of non-negative integers contains a minimum, we define r to be the smallest element of S. By definition, r is of the form $r = a - bq$ for some $q \in \mathbb{Z}$, and $r \geq 0$. Also, we must have $r < b$, since otherwise, $r - b$ would be an element of S smaller than r, contradicting the minimality of r; indeed, if $r \geq b$, then we would have $0 \leq r - b = a - b(q + 1)$.
That proves the existence of r and q.

...

Division with remainder property

Theorem 4 (p3,t1.4)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

Proof: ...

For uniqueness, suppose that $a = bq + r$ and $a = bq' + r'$, where $0 \leq r < b$ and $0 \leq r' < b$.

Then subtracting these two equations and rearranging terms, we obtain $r' - r = b(q - q')$.

Thus, $r' - r$ is a multiple of b; however, $0 \leq r < b$ and $0 \leq r' < b$ implies $|r' - r| < b$; therefore, the only possibility is $r' - r = 0$.

Moreover, $0 = b(q - q')$ and $b \neq 0$ implies $q - q' = 0$.

Q.E.D.

Floors and ceilings

Let us briefly define the usual floor and ceiling functions, denoted $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$, respectively.

These are functions from $\mathbb{R}$ (the real numbers) to $\mathbb{Z}$.

For $x \in \mathbb{R}$, $\lfloor x \rfloor$ is the greatest integer $m \leq x$.

Also, $\lceil x \rceil$ is the smallest integer $m \geq x$.

The mod operator

Now let $a, b \in \mathbb{Z}$ with $b > 0$.

Let q and r be the unique integers that satisfy $a = bq + r$ and $0 \leq r < b$ from Theorem 4.

We define

$$a \ \text{mod} \ b := r$$

that is, a mod b denotes the remainder in dividing a by b.

Statement: $b \mid a$ if and only if $a \bmod b = 0$.

Proof: Exercise on your own.

The mod operator

Statement: $(a \bmod b) = a - b\lfloor a/b \rfloor$.

The mod operator

Statement: $(a \bmod b) = a - b\lfloor a/b \rfloor$.

Proof: Dividing both sides of the equation $a = bq + r$ by b, we obtain $a/b = q + r/b$. Since $q \in \mathbb{Z}$ and $r/b \in [0, 1)$, we see that $q = \lfloor a/b \rfloor$. Thus, $(a \bmod b) = a - b\lfloor a/b \rfloor$. **Q.E.D.**

Exercises

1. Let $a, b, d \in \mathbb{Z}$ with $d \neq 0$. Show that $a \mid b$ if and only if $da \mid db$.
2. Let n be a composite integer. Show that there exists a prime p dividing n, with $p \leq \sqrt{n}$.
3. Let m be a positive integer. Show that for every real number $x \geq 1$, the number of multiples of m in the interval $[1, x]$ is $\lfloor x/m \rfloor$; in particular, for every integer $n \geq 1$, the number of multiples of m among $1, \ldots, n$ is $\lfloor n/m \rfloor$.
4. Let $x \in \mathbb{R}$. Show that $2\lfloor x \rfloor \leq \lfloor 2x \rfloor \leq 2\lfloor x \rfloor + 1$.
5. Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}$ with $n > 0$. Show that $\lfloor \lfloor x \rfloor / n \rfloor = \lfloor x/n \rfloor$; in particular, $\lfloor \lfloor a/b \rfloor / c \rfloor = \lfloor a/(bc) \rfloor$ for all positive integers a, b, c.
6. Let $a, b \in \mathbb{Z}$ with $b < 0$. Show that $(a \bmod b) \in (b, 0]$.

Outline

Ideals of $\mathbb{Z}$

We continue by introducing the notion of an ideal of $\mathbb{Z}$.

An ideal of $\mathbb{Z}$ is a non-empty set of integers that is closed under addition, and closed under multiplication by an arbitrary integer.

In technical terms:

$$\text{A non-empty set } I \subseteq \mathbb{Z} \text{ is an ideal of } \mathbb{Z}$$

$$\Longleftrightarrow$$

$$\forall a, b \in I \text{ and } \forall z \in \mathbb{Z},\ a + b \in I \text{ and } az \in I.$$

Basic Properties of Ideals of $\mathbb{Z}$

Statement: Every ideal I contains 0.

Basic Properties of Ideals of $\mathbb{Z}$

Statement: Every ideal I contains 0.

Proof: Let I be an ideal. By the definition of an ideal, I is a non-empty set. Now, let $a \in I$. We have $0 = a \cdot 0 \in I$. **Q.E.D.**

Basic Properties of Ideals of $\mathbb{Z}$

Statement: Every ideal I contains 0.

Proof: Let I be an ideal. By the definition of an ideal, I is a non-empty set. Now, let $a \in I$. We have $0 = a \cdot 0 \in I$. **Q.E.D.**

Statement: If an ideal I contains an integer a then it also contains $-a$.

Basic Properties of Ideals of $\mathbb{Z}$

Statement: Every ideal I contains 0.

Proof: Let I be an ideal. By the definition of an ideal, I is a non-empty set. Now, let $a \in I$. We have $0 = a \cdot 0 \in I$. **Q.E.D.**

Statement: If an ideal I contains an integer a then it also contains $-a$.

Proof: Let $a \in I$. Now, $-a = a \cdot (-1) \in I$. **Q.E.D.**

Basic Properties of Ideals of $\mathbb{Z}$

Statement: Every ideal I contains 0.

Proof: Let I be an ideal. By the definition of an ideal, I is a non-empty set. Now, let $a \in I$. We have $0 = a \cdot 0 \in I$. **Q.E.D.**

Statement: If an ideal I contains an integer a then it also contains $-a$.

Proof: Let $a \in I$. Now, $-a = a \cdot (-1) \in I$. **Q.E.D.**

Statement: If $a, b \in I$ then $a - b \in I$.

Basic Properties of Ideals of $\mathbb{Z}$

Statement: Every ideal I contains 0.

Proof: Let I be an ideal. By the definition of an ideal, I is a non-empty set. Now, let $a \in I$. We have $0 = a \cdot 0 \in I$. **Q.E.D.**

Statement: If an ideal I contains an integer a then it also contains $-a$.

Proof: Let $a \in I$. Now, $-a = a \cdot (-1) \in I$. **Q.E.D.**

Statement: If $a, b \in I$ then $a - b \in I$.

Proof: Exercise on your own.

Basic Properties of Ideals of $\mathbb{Z}$

Statement: $\{0\}$ and $\mathbb{Z}$ are ideals of $\mathbb{Z}$.

Basic Properties of Ideals of $\mathbb{Z}$

Statement: $\{0\}$ and $\mathbb{Z}$ are ideals of $\mathbb{Z}$.

Proof: Exercise on your own.

Basic Properties of Ideals of $\mathbb{Z}$

Statement: $\{0\}$ and $\mathbb{Z}$ are ideals of $\mathbb{Z}$.

Proof: Exercise on your own.

Statement: An ideal I is equal to $\mathbb{Z}$ if and only if $1 \in I$.

Basic Properties of Ideals of $\mathbb{Z}$

Statement: $\{0\}$ and $\mathbb{Z}$ are ideals of $\mathbb{Z}$.

Proof: Exercise on your own.

Statement: An ideal I is equal to $\mathbb{Z}$ if and only if $1 \in I$.

Proof: $1 \in I$ implies that for every $z \in Z$, we have $z = 1 \cdot z \in I$, and hence $I = \mathbb{Z}$; conversely, if $I = \mathbb{Z}$, then in particular, $1 \in I$.

Principal Ideals

For $a \in \mathbb{Z}$, define

$$a\mathbb{Z} := \{az : z \in \mathbb{Z}\}$$

that is the set of all multiples of a.

Statement: $a\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Principal Ideals

For $a \in \mathbb{Z}$, define

$$a\mathbb{Z} := \{az : z \in \mathbb{Z}\}$$

that is the set of all multiples of a.

Statement: $a\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proof: Assume $a = 0$. Then $a\mathbb{Z} = \{0\}$. Assume $a \neq 0$. Then $a\mathbb{Z}$ consists of the distinct integers

$$\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots.$$

Now, for all $az, az' \in a\mathbb{Z}$ and $z'' \in \mathbb{Z}$, we have $az + az' = a(z + z') \in a\mathbb{Z}$ and $(az)z'' = a(zz'') \in a\mathbb{Z}$. **Q.E.D.**

Principal Ideals

For $a \in \mathbb{Z}$, define

$$a\mathbb{Z} := \{az : z \in \mathbb{Z}\}$$

that is the set of all multiples of a.

Statement: $a\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proof: Assume $a = 0$. Then $a\mathbb{Z} = \{0\}$. Assume $a \neq 0$. Then $a\mathbb{Z}$ consists of the distinct integers

$$\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots.$$

Now, for all $az, az' \in a\mathbb{Z}$ and $z'' \in \mathbb{Z}$, we have $az + az' = a(z + z') \in a\mathbb{Z}$ and $(az)z'' = a(zz'') \in a\mathbb{Z}$. **Q.E.D.**

The ideal $a\mathbb{Z}$ is called the ideal generated by a, and an ideal of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$ is called a principal ideal.

More on Ideals

Statement: For all $a, b \in \mathbb{Z}$, we have $b \in a\mathbb{Z}$ if and only if $a \mid b$.

More on Ideals

Statement: For all $a, b \in \mathbb{Z}$, we have $b \in a\mathbb{Z}$ if and only if $a \mid b$.

Proof: Exercise on your own.

More on Ideals

Statement: For all $a, b \in \mathbb{Z}$, we have $b \in a\mathbb{Z}$ if and only if $a \mid b$.

Proof: Exercise on your own.

Statement: For every ideal I, we have $b \in I$ if and only if $b\mathbb{Z} \subseteq I$.

More on Ideals

Statement: For all $a, b \in \mathbb{Z}$, we have $b \in a\mathbb{Z}$ if and only if $a \mid b$.

Proof: Exercise on your own.

Statement: For every ideal I, we have $b \in I$ if and only if $b\mathbb{Z} \subseteq I$.

Proof: Exercise on your own.

More on Ideals

Statement: For all $a, b \in \mathbb{Z}$, we have $b \in a\mathbb{Z}$ if and only if $a \mid b$.

Proof: Exercise on your own.

Statement: For every ideal I, we have $b \in I$ if and only if $b\mathbb{Z} \subseteq I$.

Proof: Exercise on your own.

Statement: $b\mathbb{Z} \subseteq a\mathbb{Z}$ if and only if $a \mid b$.

More on Ideals

Statement: For all $a, b \in \mathbb{Z}$, we have $b \in a\mathbb{Z}$ if and only if $a \mid b$.

Proof: Exercise on your own.

Statement: For every ideal I, we have $b \in I$ if and only if $b\mathbb{Z} \subseteq I$.

Proof: Exercise on your own.

Statement: $b\mathbb{Z} \subseteq a\mathbb{Z}$ if and only if $a \mid b$.

Proof: Exercise on your own.

More on Ideals

Let I_1 and I_2 be ideals of $\mathbb{Z}$.

$$I_1 + I_2 := \{a_1 + a_2 : a_1 \in I_1, a_2 \in I_2\}.$$

Statement: $I_1 + I_2$ is also an ideal of $\mathbb{Z}$.

More on Ideals

Let I_1 and I_2 be ideals of $\mathbb{Z}$.

$$I_1 + I_2 := \{a_1 + a_2 : a_1 \in I_1, a_2 \in I_2\}.$$

Statement: $I_1 + I_2$ is also an ideal of $\mathbb{Z}$.

Proof: Assume $a_1 + a_2 \in I_1 + I_2$ and $b_1 + b_2 \in I_1 + I_2$.

Then we have $(a_1 + a_2) + (b_1 + b_2) = (a_1 + b_1) + (a_2 + b_2) \in I_1 + I_2$,

and for every $z \in \mathbb{Z}$, we have $(a_1 + a_2)z = a_1 z + a_2 z \in I_1 + I_2$.

Examples on Ideals

Example 5

Consider the principal ideal $3\mathbb{Z}$. This consists of all multiples of 3; i.e. $3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$.

Example 6

Consider the ideal $3\mathbb{Z} + 5\mathbb{Z}$. Since it contains 1, it contains all integers; i.e. $3\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$.

Example 7

Consider the ideal $4\mathbb{Z} + 6\mathbb{Z}$. This ideal contains $4 \cdot (-1) + 6 \cdot 1 = 2$, and therefore, it contains all even integers. It does not contain any odd integers, since the sum of two even integers is again even. Thus, $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.

Note: "i.e." = "id est" = "that is".

More on Principle Ideals

In the previous two examples, we defined an ideal that turned out upon closer inspection to be a principal ideal. This was no accident: the following theorem says that all ideals of $\mathbb{Z}$ are principal.

Theorem 8 (p6,t1.6)

Let I be an ideal of $\mathbb{Z}$. Then there exists a unique non-negative integer d such that $I = d\mathbb{Z}$.

Proof: We first prove the existence part of the theorem. If $I = \{0\}$, then $d = 0$ does the job, so let us assume that $I \neq \{0\}$. Since I contains non-zero integers, it must contain positive integers, since if $a \in I$ then so is $-a$.

...

More on Principle Ideals

...

Let d be the smallest positive integer in I. We want to show that $I = d\mathbb{Z}$. We first show that $I \subseteq d\mathbb{Z}$. To this end, let a be any element in I. It suffices to show that $d \mid a$. Using the division with remainder property, write $a = dq + r$, where $0 \le r < d$. Then by the closure properties of ideals, one sees that $r = a - dq$ is also an element of I, and by the minimality of the choice of d, we must have $r = 0$. Thus, $d \mid a$. We have shown that $I \subseteq d\mathbb{Z}$. The fact that $d\mathbb{Z} \subseteq I$ follows from the fact that $d \in I$. Thus, $I = d\mathbb{Z}$. That proves the existence part of the theorem.

For uniqueness, note that if $d\mathbb{Z} = e\mathbb{Z}$ for some non-negative integer e, then $d \mid e$ and $e \mid d$, from which it follows that $d = \pm e$; since d and e are non-negative, we must have $d = e$. **Q.E.D.**

Outline

Greatest Common Divisor (GCD)

For $a, b \in \mathbb{Z}$, we call $d \in \mathbb{Z}$ a common divisor of a and b if $d \mid a$ and $d \mid b$.

A common divisor d of a and b is called the greatest common divisor of a and b if

- d is non-negative,
- all other common divisors of a and b divide d.

Greatest Common Divisor (GCD)

Theorem 9 (p6,t1.7)

For all $a, b \in \mathbb{Z}$, there exists a unique greatest common divisor d of a and b, and moreover, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Proof: We apply Theorem 8 to the ideal $I := a\mathbb{Z} + b\mathbb{Z}$. Let $d \in \mathbb{Z}$ with $I = d\mathbb{Z}$, as in that theorem. We wish to show that d is a greatest common divisor of a and b. Note that $a, b, d \in I$ and d is non-negative. Since $a \in I = d\mathbb{Z}$, we see that $d \mid a$; similarly, $d \mid b$. So we see that d is a common divisor of a and b.

...

Greatest Common Divisor (GCD)

...
Since $d \in I = a\mathbb{Z} + b\mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$.

Now suppose $a = a'd'$ and $b = b'd'$ for some $a', b', d' \in \mathbb{Z}$. Then the equation $as + bt = d$ implies that $d'(a's + b't) = d$, which says that $d' \mid d$.

Thus, any common divisor d' of a and b divides d. That proves that d is a greatest common divisor of a and b.

For uniqueness, note that if e is a greatest common divisor of a and b, then $d \mid e$ and $e \mid d$, and hence $d = \pm e$; since both d and e are non-negative by definition, we have $d = e$. **Q.E.D.**

Relatively prime numbers

For $a, b \in \mathbb{Z}$, we write $\gcd(a, b)$ for the greatest common divisor of a and b. We say that $a \in \mathbb{Z}$ are relatively prime if $\gcd(a, b) = 1$, which is the same as saying that the only common divisors of a and b are ± 1.

More on GCD

The following is essentially just a restatement of Theorem 9.

Theorem 10 (p7,t1.8)

Let $a, b, r \in \mathbb{Z}$ and let $d := gcd(a, b)$. Then there exist $s, t \in \mathbb{Z}$ such that $as + bt = r$ if and only if $d \mid r$. In particular, a and b are relatively prime if and only if there exist integers s and t such that $as + bt = 1$.

Proof: We have

$$\begin{aligned} & as + bt = r \text{ for some } s, t \in \mathbb{Z} \\ \iff & r \in a\mathbb{Z} + b\mathbb{Z} \\ \iff & r \in d\mathbb{Z} \text{ (by Theorem 9)} \\ \iff & d \mid r. \end{aligned}$$

That proves the first statement. The second statement follows from the first, setting $r := 1$. **Q.E.D.**

More on GCD

Theorem 11 (p7,t1.9)

Let $a, b, c \in \mathbb{Z}$ such that $c \mid ab$ and $\gcd(a, c) = 1$. Then $c \mid b$.

Proof: Suppose that $c \mid ab$ and $\gcd(a, c) = 1$.

Then since $\gcd(a, c) = 1$, by Theorem 10 we have $as + ct = 1$ for some $s, t \in \mathbb{Z}$.

Multiplying this equation by b, we obtain $abs + cbt = b$.

Since c divides ab by hypothesis, and since $c \mid cbt$, it follows that $c \mid abs + cbt$, and hence that c divides b. **Q.E.D.**

More on GCD

Theorem 12 (p8,t1.10)

Let p be prime, and let $a, b \in \mathbb{Z}$. Then $p \mid ab$ implies that $p \mid a$ or $p \mid b$.

Proof: Assume that $p \mid ab$. If $p \mid a$, we are done, so assume that $p \nmid a$. By the above observation, $\gcd(a,p) = 1$, and so by Theorem 11, we have $p \mid b$. **Q.E.D.**

More on GCD

Corollary: If $a_1, \ldots, a_k$ are integers, and if p is a prime that divides the product $a_1 \cdots a_k$, then $p \mid a_i$ for some $i = 1, \ldots, k$.

Proof: This can be proved by induction on k. For $k = 1$, the statement is trivially true. Now let $k > 1$, and assume that statement holds for $k - 1$. Then by Theorem 12, either $p \mid a_1$ or $p \mid a_2 \cdots a_k$; if $p \mid a_1$, we are done; otherwise, by induction, p divides one of $a_2, \ldots, a_k$. **Q.E.D.**

Exercise I

1. Let I be a non-empty set of integers that is closed under addition (i.e., $a+b \in I$ for all $a,b \in I$). Show that I is an ideal if and only if $-a \in I$ for all $a \in I$.
2. Show that for all integers a, b, c, we have:
   1. $\gcd(a,b) = \gcd(b,a)$;
   2. $\gcd(a,b) = |a| \iff a \mid b$;
   3. $\gcd(a,0) = \gcd(a,a) = |a|$ and $\gcd(a,1) = 1$;
   4. $\gcd(ca,cb) = |c| \cdot \gcd(a,b)$.
3. Show that for all integers a,b with $d := \gcd(a,b) = 0$, we have $\gcd(a/d, b/d) = 1$.
4. Let n be an integer. Show that if a,b are relatively prime integers, each of which divides n, then ab divides n.
5. Show that two integers are relatively prime if and only if there is no one prime that divides both of them.

Exercise II

6. Let $a, b_1, \ldots, b_k$ be integers. Show that $\gcd(a, b_1 \cdots b_k) = 1$ if and only if $\gcd(a, b_i) = 1$ for $i = 1, \ldots, k$.
7. Let p be a prime and k an integer, with $0 < k < p$. Show that the binomial coefficient

$$\binom{n}{k} = \frac{p!}{k!(p-k)!}$$

is divisible by p.
8. Let $a, b, c \in \mathbb{Z}$ such that $c \mid ab$ and $\gcd(a, c) = 1$. Prove that $c|b$.
9. Let p be prime, and let $a, b \in \mathbb{Z}$. Then $p \mid ab$ implies that $p \mid a$ or $p \mid b$.
10. Let $a_1, \ldots, a_k$ be integers, and if p is a prime that divides the product $a_1, \ldots, a_k$, then $p \mid a_i$ for some $i = 1, \ldots, k$.

Outline

Fundamental theorem of arithmetic

Theorem 3 revisited: Every non-zero integer n can be expressed as

$$n = \pm p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_1, e_2, \ldots, e_r$ are positive integers. Moreover, this expression is unique, up to a reordering of the primes.

Remark 1: The theorem intuitively says that the primes act as the "building blocks" out of which all non-zero integers can be formed by multiplication (and negation).

Fundamental theorem of arithmetic

Theorem 3 revisited: Every non-zero integer n can be expressed as

$$n = \pm p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_1, e_2, \ldots, e_r$ are positive integers. Moreover, this expression is unique, up to a reordering of the primes.

Remark 2: The reader may be so familiar with this fact that he may feel it is somehow "self evident", requiring no proof; however, this feeling is simply a delusion.

Fundamental theorem of arithmetic

Theorem 3 revisited: Every non-zero integer n can be expressed as

$$n = \pm p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_1, e_2, \ldots, e_r$ are positive integers. Moreover, this expression is unique, up to a reordering of the primes.

Proof:

- We may clearly assume that n is positive, since otherwise, we may multiply n by -1 and reduce to the case where n is positive.
- The proof of the existence: This amounts to showing that every positive integer n can be expressed as a product (possibly empty) of primes.

...

Fundamental theorem of arithmetic

...

If $n = 1$, the statement is true, as n is the product of zero primes.

Now let $n > 1$, and assume that every positive integer smaller than n can be expressed as a product of primes.

If n is a prime, then the statement is true, as n is the product of one prime.

Assume, then, that n is composite, so that there exist $a, b \in \mathbb{Z}$ with $1 < a < n$, $1 < b < n$, and $n = ab$.

By the induction hypothesis, both a and b can be expressed as a product of primes, and so the same holds for n.

We continue with the uniqueness part of the theorem.

...

Fundamental theorem of arithmetic

...We now prove the uniqueness part.

Let $p_1, \ldots, p_r, q_1, \ldots, q_s$ be (not necessarily distinct) primes such that

$$p_1 \cdots p_r = q_1 \cdots q_s.$$

If $r = 1$, we must have $s = 1$ and we are done.

Now suppose $r > 1$, and that the statement holds for $r - 1$.

Since $r > 1$, we must have $s > 1$.

Also, as $p_1 \mid p_1 \cdots p_r$, we have $p_1 \mid q_1 \cdots q_s$.

It follows from (the corollary to) Theorem 12 that $p_1 \mid q_j$ for some $j = 1, \ldots, s$, and moreover, since q_j is prime, we must have $p_1 = q_j$.

Thus, we may cancel p_1 from the left-hand side of $p_1 \cdots p_r = q_1 \cdots q_s$ and q_j from the right-hand side of $p_1 \cdots p_r = q_1 \cdots q_s$. The statement now follows from the induction hypothesis. **Q.E.D.**

Number of Primes

Theorem 13 (p10,t1.11)

There are infinitely many primes.

Proof: Suppose that there were only finitely many primes; call them $p_1, \ldots, p_k$. Set $M := p_1 \cdots p_k$ and $N := M + 1$. Consider a prime p that divides N. There must be at least one such prime p, since $N \geq 2$, and every positive integer can be written as a product of primes. Clearly, p cannot equal any of the p_i's, since if it did, then p would divide M, and hence also divide $N - M = 1$, which is impossible.
Therefore, the prime p is not among $p_1, \ldots, p_k$, which contradicts our assumption that these are the only primes. **Q.E.D.**

End of session.