MA014G
Algebra and Discrete Mathematics A

Lecture Notes 3

Autumn 2007

Pia Heidtmann
070811

INTEGERS AND DIVISIBILITY

Definition

An integer b is said to be a factor (faktor) or divisor (deler) of an integer a if

$$a = bs$$

for some integer s.

We write $b|a$ and say that a is divisible (delbaar) by b or that a is a multiple (multipel) of b.

Similarly we write $b \nmid a$ if a is not divisible by b.

If $b|a$, the expression $a = bs$ is called a factorisation (faktorisering) of a.

EXAMPLE

12 has the factors $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$.

For example $4|12$

and we thus have the factorisation

$$12 = 4 \cdot 3$$

7 is not a divisor of 12, so we write $7 \nmid 12$.

The integers 1 and -1 are special because they are a factor of every integer.

1 and -1 are known as the units (enheter) in the set of integers $\mathbb{Z}$.

Every integer a has the factorisations

$$a = a \cdot 1 \quad \text{and} \quad a = (-a)(-1),$$

so a has the trivial factors $a, -a, 1$ and -1.

A factor of a other than $a, -a, 1$ and -1 is called a proper factor (äkta delare).

Definition

An integer a which has a proper factor is called a composite integer (sammansatt tal).

EXAMPLE

12 is a composite integer because for example

$$12 = 2 \cdot 6$$

so 2 and 6 are proper factors of 12.

-1 and 1 are not composite integers because they are only divisible by -1 and $+1$.

0 is a composite integer because for example $0 = 2 \cdot 0$ so 2 is a proper factor of 0.

EXAMPLE (cont.)

The proper factors of 20 are $\pm 2, \pm 4, \pm 5$ and ± 10.

7 has no proper factors as 7 is only divisible by ± 1 and ± 7.

Definition

An integer p that has no proper factors and is not a unit is called a prime number.

EXAMPLE

7 is a prime number because it has no proper factors and it is not one of the two units 1 and -1.

Note that prime numbers can be negative as well as positive:

EXAMPLE

-7 is a prime because it has no proper factors and it is not one of the two units 1 and -1.

-1 and 1 are not primes because they are units.

Some divisibility rules.

Let a, b and c be integers.

(i) If $c|a$ and $c|b$ then $c|(a+b)$ and $c|(a-b)$.

(ii) If $c|a$ and $a|b$ then $c|b$.

(iii) If $c|a$ then $c|ka$ for all integers k

(iv) If $c|a$ and $c|b$ then $c|(ax+by)$ for all integers x and y.

EXAMPLE

(i) $2|12$ and $2|4$ so $2|16$ and $2|8$ and $2|(-8)$

by divisibility rule (i).

(ii) $3|12$ and $12|36$ so $3|36$ by divisibility rule (ii)

(iii) $5|10$ so $5|20$, $5|30$, $5|40$, $5|50$, ...

$5|0$, $5|(-10)$, $5|(-20)$, $5|(-30)$, ...

by divisibility rule (ii)

(iv) $3|6$ and $3|(-3)$ so $3|(6x-3y)$ for all integers x and y

by divisibility rule (iv).

A prime number test

Given any number, for example 137. How do we find out whether it is a prime or a composite number?

Solution 1

Try all possible factors ≤ 136, that is try

$$2, 3, 4, 5, 6, 7, \ldots$$

Solution 2

Try only the positive primes ≤ 136, that is try

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

Solution 3 [Primality Test]

Let $n \geq 2$ be an integer.

IF n has no factor k where $1 < k \leq \sqrt{n}$

THEN n is a prime number.

$\sqrt{137} = 11.704699\ldots$

so we only need to check whether

$$2, 3, 5, 7 \text{ and } 11$$

divides 137. If not, 137 is prime.

$2 \nmid 137$ $3 \nmid 137$ $5 \nmid 137$ $7 \nmid 137$ $11 \nmid 137$ so 137 prime

(linjärkombinationer)

Linear Combinations

If m and n are integers we call all integers in the form

$$sm + tn$$

where s and t are also integers, a linear combination of m and n.

EXAMPLE

Let $m = 5$ and $n = 3$ then the following numbers are all linear combinations of m and n.

5 is a linear combination of m and n:

$$5 = 1 \cdot 5 + 0 \cdot 3,$$

i.e. we let $s = 1$ and $t = 0$.

3 is a linear combination of m and n:

$$3 = 0 \cdot 5 + 1 \cdot 3$$

i.e. we let $s = 0$ and $t = 1$.

1 is a linear combination of $m = 5$ and $n = 3$:

$$1 = 2 \cdot 5 + (-3) \cdot 3$$

i.e. we let $s = 2$ and $t = 3$

- Is there any integer k, which is NOT a linear combination of $n = 5$ and $m = 3$? No!

$$k = (2k)5 + (-3k) \cdot 3$$

- Note, the linear combinations in the above example are NOT unique, for example:

$$3 = 6 \cdot 5 + (-9) \cdot 3$$

A theorem about linear combinations

Theorem B3.3 in study guide

Let m and n be integers,

and let d be an integer which is a factor of both m and n,

that is $$d|m \text{ and } d|n.$$

THEN

d divides any linear combination of m and n,

that is $$d|(sm+tn)$$

for all possible choices of integers s and t.

Definition

Any integer d which is a factor of both m and n

is known as a common divisor of m and n.

(gemensam delare)

Greatest Common Divisors

Definition

Let m and n be integers, not both zero, and let s be a positive integer which satisfies the following two properties.

(i) $s|m$ and $s|n$

(ii) Whenever an integer d is such that $d|m$ and $d|n$ then $d|s$.

Then s is the (största gemensamma delaren) greatest common divisor of m and n.

We write

$$s = \gcd(m,n).$$

In Swedish we write

$$s = \mathrm{sgd}(m,n).$$

EXAMPLE

$\gcd(12,32)$ is 4 because

- 4 is positive

(i) $4|12$ and $4|32$.

(ii) 12 has factors $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$.

32 has factors $\pm1, \pm2, \pm4, \pm8, \pm16, \pm32$

so the common divisors of 12 and 32 are

$$\pm1, \pm2, \pm4$$

It is easy to check that all of these divide 4.

Main Theorem B.3.4

Let m and n be two integers, not both zero.
Then the greatest common divisor of m and n exists
and
there are integers s and t such that

$$\gcd(m,n) = sm + tn.$$

EXAMPLE

We found above that $\gcd(32,12) = 4$.

Put $s = 2$ and $t = -5$, then

$$4 = 2 \cdot 32 + (-5) \cdot 12,$$

so 4 is indeed a linear combination of 32 and 12
as Theorem B3.4 predicts.

Corollary B.3.5

Let m and n be integers, not both zero,
and let $g = \gcd(m,n)$.

Then those integers which can be written as a linear combination of m and n
are exactly the same as those integers which are multiples of $\gcd(m,n)$.

EXAMPLE

We found that $\gcd(12,32) = 4$, so the set

$$L = \{s12 + t32 \mid s,t \in \mathbb{Z}\}$$

and the set

$$M = \{4k \mid k \in \mathbb{Z}\}$$

are exactly the same.

Proof of corollary B9.5

Let $L = \{ sm + tn \mid s,t \in \mathbb{Z} \}$

and $M = \{ k \cdot \gcd(m,n) \mid k \in \mathbb{Z} \}$.

We must prove $M = L$. We do this by showing that $M \subseteq L$ and $L \subseteq M$.

$M \subseteq L$ Take any element $x \in M$. Then $x = kg$ where $g = \gcd(m,n)$.

But Main Thm. C4 says there exist $s,t \in \mathbb{Z}$ such that

$$g = sm + tn$$

Then $x = kg = k(sm+tn) = (ks)m + (kt)n$,

so x is a linear combination of m and n.

So $x \in L$.

$L \subseteq M$ Take any element $y \in L$, then

$$y = sm + tn$$

for some $s,t \in \mathbb{Z}$.

But $g = \gcd(m,n)$, so $g \mid m$ and $g \mid n$

and so there are integers a and b such that

$$m = ag \quad \text{and} \quad n = bg$$

Then

$$y = sm + tn = sag + tbg = (sa + tb)g$$

and we thus see that y is a multiple of g.

So $y \in M$. ∎

So one big question remains:

How do we find the gcd of two integers?

ANSWER: Euclid's Algorithm

- Let a and b be two positive integers. We want to compute $\gcd(a,b)$.
- Idea: Use the Division Theorem on successive remainders:

① $a = bq_1 + r_1$ where $0 \le r_1 \le b-1$ (divide a by b to get remainder r_1)

② $b = r_1 q_2 + r_2$ where $0 \le r_2 \le r_1 - 1$ (divide b by r_1 to get remainder r_2)

③ $r_1 = r_2 q_3 + r_3$ where $0 \le r_3 \le r_2 - 1$ (divide r_1 by r_2 to get remainder r_3)

④ $r_2 = r_3 q_4 + r_4$ where $0 \le r_4 \le r_3 - 1$ (divide r_2 by r_3 ...

[continue this until you get a remainder 0, say $r_n = 0$]

(n-1) $r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$

(n) $r_{n-2} = r_{n-1} q_n + r_n$ where $r_n = 0$ and $r_1, r_2, r_3, \dots, r_{n-1} \neq 0$.

- $\gcd(a,b) = r_{n-1}$, that is the last non-zero remainder.

Note: The algorithm works because if $a > b$ and $a = bq + r$ then $\gcd(a,b) = \gcd(b,r)$.

EXAMPLE

Find the greatest common divisor of 32 and 12:

$$32 = 12(2) + 8$$
$$12 = 8(1) + 4$$
$$8 = 4(2) + 0$$

So the last non-zero remainder is 4, hence $\gcd(32, 12) = 4$.

Find the greatest common divisor of 2406 and 654:

$$2406 = 654(3) + 444$$
$$654 = 444(1) + 210$$
$$444 = 210(2) + 24$$
$$210 = 24(8) + 18$$
$$24 = 18(1) + 6$$
$$18 = 6(3) + 0$$

So $\gcd(2406, 654) = 6$. (the last non-zero remainder)

EXAMPLE

Find gcd (90, 24)

$$90 = 24\,(3) + 18$$

$$24 = 18\,(1) + 6$$

$$18 = 6\,(3) + 0$$

So $\gcd(90, 24) = 6$.

We saw earlier (in Main Theorem B3.4) that because

$$6 = \gcd(90, 24)$$

then 6 can be written as a linear combination of 90 and 24.

How do we find this linear combination?

ANSWER: Work backwards through Euclid's algorithm:

$$\gcd(90, 24) = 6$$

$$18 = 6(3) + 0$$

$$24 = 18(1) + 6 \quad \Rightarrow \quad 6 = 24 + 18(-1)$$

$$90 = 24(3) + 18 \quad \Rightarrow \quad 18 = 90 + 24(-3)$$

So $6 = \gcd(90, 24) = 24 + 18(-1) = 24 + (90 + 24(-3))(-1)$

$$= 24(4) + 90(-1).$$

EXAMPLE

Find gcd(54, 33) and express it as a linear combination of 54 and 33.

$54 = 33(1) + 21 \quad \Rightarrow 21 = 54 - 33(1)$ ****

$33 = 21(1) + 12 \quad \Rightarrow 12 = 33 - 21(1)$ ***

$21 = 12(1) + 9 \quad \Rightarrow 9 = 21 - 12(1)$ **

$12 = 9(1) + \boxed{3} \quad \Rightarrow 3 = 12 - 9(1)$ *

$9 = 3(3) + 0$

So gcd(54, 33) = 3

Working backwards through the algorithm step by step we get :

$$\begin{aligned}
\gcd(54, 33) = \underline{3} &= \underline{12} - \underline{9} && \text{(by *)} \\
&= \underline{12} - [\underline{21} - \underline{12}] && \text{(by substituting **)} \\
&= \underline{12}(2) + \underline{21}(-1) && \text{(by collecting like terms)} \\
&= [\underline{33} - \underline{21}](2) + \underline{21}(-1) && \text{(by substituting ***)} \\
&= \underline{33}(2) + \underline{21}(-3) && \text{(collecting like terms)} \\
&= \underline{33}(2) + [\underline{54} - \underline{33}](-3) && \text{(substituting ****)} \\
&= \underline{33}(5) + \underline{54}(-3).
\end{aligned}$$

So $\underline{\gcd(54, 33) = 54(-3) + 33(5)}$

EXAMPLE

(a) Can 2 be written as a linear combination of 957 and 426?

(b) Write 30 as a linear combination of 957 and 426.

(a) We find gcd(957, 426) by Euclid's algorithm:

$$957 = 426(2) + 105 \quad \Rightarrow 105 = 957 + 426(-2) \quad ***$$

$$426 = 105(4) + 6 \quad \Rightarrow 6 = 426 + 105(-4) \quad **$$

$$105 = 6(17) + \boxed{3} \quad \Rightarrow 3 = 105 + 6(-17) \quad *$$

$$6 = 3(2) + 0$$

So gcd(957, 426) = 3

Since $3 \nmid 2$ we thus know by Corollary B35 that 2 cannot be written as a linear combination of 957 and 426.

(b) $$\gcd(957, 426) = 3 \overset{*}{=} 105 + 6(-17)$$

$$\overset{**}{=} 105 + [426 + 105(-4)](-17)$$

$$= 105(69) + 426(-17)$$

$$\overset{***}{=} [957 + 426(-2)](69) + 426(-17)$$

$$= 957(69) + 426(-155)$$

So $\gcd(957, 426) = \underline{3 = 957(69) + 426(-155)}$

Now $30 = 10 \cdot 3$ so 30 can be written as a linear combination of 957 and 426:

$$\underline{30} = 10 \cdot 3 = 10 \cdot [957(69) + 426(-155)]$$

$$= \underline{957(690) + 426(-1550)}$$

EXAMPLE

Let us find gcd (35, 12) :

$35 = 12(2) + 11 \quad \Rightarrow 11 = 35 + 12(-2)$

$12 = 11(1) + \boxed{1} \quad \Rightarrow 1 = 12 - 11$

$11 = 1(11) + 0$

So gcd (12, 35) = 1.

This means that 1 can be written as a linear combination of 35 and 12:

$1 = 12 - 11$

$= 12 - [35 + 12(-2)]$

$= 12(3) + 35(-1)$

So $\underline{1 = (-1)35 + (3)12}$

By Corollary B3.5 every integer can thus be written as a linear combination of 35 and 12:

$$\underline{k = (-k)35 + (3k)12}$$

When gcd (m, n) = 1 we say that m and n are relatively prime (relativ prima) or coprime.

When m and n are relatively prime their only common factors are the units 1 and -1.

THEOREM B3.7

Let m and n be non-zero integers. Then

m and n are relatively prime if and only if

there exist integers s and t such that $1 = sm + tn$.

Prime factorisation

Primes have a very important property, that we shall now prove:

Theorem B3.8

Let m and n be two non-zero integers and let p be a prime such that

$$p \mid mn.$$

Then $p \mid m$ or $p \mid n$ (or both).

EXAMPLE

Let $a = 24$, then there are lots of factorisations of 24 into two factors:

$$24 = (1)(24)$$
$$24 = (-1)(-24)$$
$$24 = (2)(12)$$
$$24 = (-2)(-12)$$
$$24 = (3)(8)$$
$$24 = (-3)(-8)$$
$$24 = (4)(6)$$
$$24 = (-4)(-6)$$
$$24 = (6)(4)$$
$$24 = (-6)(-4)$$
$$\vdots$$
$$24 = (-24)(-1)$$

The only primes dividing 24 are ± 2 and ± 3. Theorem B3.8 says that one of these 4 primes divide one of the factors in any of the above factorisations of 24.

Theorem 3.8

Let p be a prime such that $p \mid mn$. Then $p \mid m$ or $p \mid n$ (or both)

PROOF

Suppose that $p \mid mn$.

If $p \mid m$ the result is obvious.

If $p \nmid m$, we must show that $p \mid n$.

Consider $\gcd(m, p)$.

The divisors of p are just $1, -1, p$ and $-p$,

and $p \nmid m$, so this means $\gcd(m, p) = 1$.

By Theorem 3.4 we then know there exist integers s and t such that

$$1 = ms + pt$$

Multiply this equation by n on both sides to get

$$\begin{aligned} n &= (ms + pt)n \\ &= mns + ptn \\ &= (mn)s + p(tn) \quad \circledast \end{aligned}$$

Since $p \mid mn$ and $p \mid p$, $p \mid$ RHS of $\circledast$,

thus $p \mid$ LHS of $*$, that is $p \mid n$.

So if $p \nmid m$ then $p \mid n$. ■

Theorem B3.8 can be used to prove a very important theorem:

(Aritmetikens fundamentalsats)

The Fundamental Theorem of Arithmetic

Every integer (except 0) can be written as a product of precisely one unit and a finite number of positive primes.

More is true: This factorisation is unique apart from the order in which the factors occur.

EXAMPLE

$12 = \underset{\text{unit}}{1} \cdot 2 \cdot 2 \cdot 3$

That the factorisation is unique up to the order of the factors means that all the factorisations of 12 into one unit and positive primes

$12 = 1 \cdot 2 \cdot 3 \cdot 2 = 1 \cdot 3 \cdot 2 \cdot 2 = 1 \cdot 2 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 1 \cdot 2 = 3 \cdot 1 \cdot 2 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 1$

are fundamentally the same, they only differ in the order of the factors.

EXAMPLE

$(-12) = \underset{\text{unit}}{(-1)} \cdot 2 \cdot 2 \cdot 3$

More about linear combinations

In an earlier lecture we saw that the set of linear combinations of two non-zero integers m and n is precisely the set of all multiples of $g = \gcd(m,n)$.

This means that for any integer a we have that

if $\gcd(m,n) \nmid a$ then a cannot be written as a linear combination of m and n.

if $\gcd(m,n) \mid a$ then a CAN be written as a linear combination of m and n as follows:

① Use Euclid's algorithm to find $g = \gcd(m,n)$.

② Work backwards in Euclid's Algorithm to find integers s and t such that

$$g = sm + tn.$$

③ Divide a by g to find a quotient k such that

$$a = kg$$

④ Combining ③ and ② we get

$$a = kg = k(sm+tn)$$

$$\Downarrow$$

$$a = (ks)m + (kt)n.$$

EXAMPLE

$\gcd(10, 25) = 5$, so e.g. 885 can be written as a linear combination of 10 and 25 while e.g. 884 cannot.

① We first show $\gcd(10,25)=5$:

$$25 = 10(2) + \boxed{5}$$

$$10 = 5(2) + 0$$

So last non-zero remainder is $5 = \gcd(10, 25)$.

② Working backwards in Euclid's Algorithm we find

$$5 = 1 \cdot 25 + (-2) \cdot 10$$

③ Dividing 885 by 5 we find

$$885 = 5 \cdot 177$$

④ Combining ② and ③ we find

$$885 = 5 \cdot 177 = (1 \cdot \underline{25} + (-2)\underline{10}) \cdot 177 = \underline{177} \cdot \underline{\underline{25}} + (-354) \cdot \underline{\underline{10}}$$

So

$$885 = 177 \times 25 + (-354) \times 10$$

is a linear combination of 25 and 10.

One question remains: Is this the only way of writing 885 as a linear combination of 25 and 10?

The answer to this question is clearly 'NO' as for example

$$0 = (-10)\cdot 25 + (25)\cdot 10,$$

so adding this to

$$885 = 177\cdot 25 + (-354)\cdot 10$$

gives

$$0+885 = (-10)\cdot 25 + (25)\cdot 10 + 177\cdot 25 + (-354)\cdot 10$$

which can be written as

$$885 = 167\cdot 25 + (-329)\cdot 10$$

In fact there are infinitely many solutions because

$$0 = (-10k)\cdot 25 + (25k)\cdot 10$$

for any $k \in \mathbb{Z}$.