Digitalteknik EITF65

Lecture 4: Computing with integers and some abstract algebra

August 27, 2020

Euclid's division theorem

$\mathbb{Z}$ set of integers, $n \in \mathbb{Z}$

Theorem (3.1)

Let n be an integer and d a positive integer. Then there exist two unique integers q and r such that

$$n = qd + r, \quad 0 \leq r < d$$

We call

- q *quotient*
- r *reminder*
- d *divisor*

The remainder is written as $R_d(n) = r$. *(or $n \bmod d$)*

How to compute n mod d

The general procedure is known as *long division*.

Example

Divide 43 by 8. Then 43 can be split in an integer part (quotient) and a remainder.

$$\left\lfloor \frac{43}{8} \right\rfloor = \lfloor 5.3750 \rfloor = 5$$

$$43 - 5 \cdot 8 = 3$$

$$43 = 5 \cdot 8 + 3$$

$$R_8(43) = R_8(5 \cdot 8 + 3) = 3$$

Example

Divide -43 by 8. Then -43 can be split in an integer part (quotient) and a reminder.

$$\left\lfloor \frac{-43}{8} \right\rfloor = \lfloor -5.3750 \rfloor = -6$$

$$-43 - (-6) \cdot 8 = 5$$

Hence,

$$-43 = (-6) \cdot 8 + 5$$

We write

$$R_8(-43) = R_8((-6) \cdot 8 + 5) = 5$$

Example

Divide 24 by 4

$$\left\lfloor \frac{24}{4} \right\rfloor = \lfloor 6 \rfloor = 6$$

Hence,

$$24 = 6 \cdot 4 + 0$$

The remainder is $R_4(24) = 0$ and we say that 4 divides 24,

$$4 \mid 24.$$

Remainder

Example

$$R_8(43) = R_8(5 \cdot 8 + 3) = 3$$
$$R_8(43 + 7 \cdot 8) = R_8(5 \cdot 8 + 3 + 7 \cdot 8) = R_8(12 \cdot 8 + 3) = 3$$

Properties of the remainder

Theorem (3.2)

For all choices of the integers n, i, and d

$$R_d(n + id) = R_d(n).$$

Proof.

$$R_d(n) = R_d(qd + r) = r$$
$$R_d(n + id) = R_d(\underbrace{qd + r}_{n} + id) = R_d((q + i)d + r) = r$$

□

Greatest Common Divisor

Definition (GCD)

Given two integers n_1 and n_2, the set of common divisors is

$$\text{cd}(n_1, n_2) = \{m \in \mathbb{Z} \big| m|n_1 \text{ and } m|n_2\}$$

The greatest common divisor (gcd) is

$$\gcd(n_1, n_2) = \max\{\text{cd}(n_1, n_2)\}.$$

Properties of gcd:

- $\gcd(n_1, n_2)$ is a unique integer (undefined for $n_1 = n_2 = 0$).
- $\gcd(\pm n_1, \pm n_2) = \gcd(n_1, n_2)$
- $\gcd(n, 0) = |n|$
- If $\gcd(n_1, n_2) = 1$ we say that n_1 and n_2 are relatively prime.

Common divisors

Example

Consider the integers $n_1 = 231$ and $n_2 = 84$. Since

$$231 = 3 \cdot 77 \Rightarrow 3 \mid 231$$
$$84 = 3 \cdot 28 \Rightarrow 3 \mid 84$$

3 is a common divisor of 231 and 84, $3 \in \mathrm{cd}(231, 84)$.
The complete set of common divisors is

$$\mathrm{cd}(231, 84) = \{\pm 1, \pm 3, \pm 7, \pm 21\}$$

The greatest common divisor is

$$\gcd(231, 84) = 21$$

Least Common Multiple

Definition (LCM)

Given two integers n_1 and n_2, the set of common multiples is

$$\text{cm}(n_1, n_2) = \{m \in \mathbb{Z}^+ \big| n_1|m \text{ and } n_2|m\}$$

The least common multiple (lcm) is

$$\text{lcm}(n_1, n_2) = \min\{\text{cm}(n_1, n_2)\}.$$

$$\gcd(n_1, n_2)\text{lcm}(n_1, n_2) = n_1 n_2$$

Euclid's recursion

Theorem (3.3)

For all choices of the integers n_1, n_2, and i

$$\gcd(n_1, n_2) = \gcd(n_1 - in_2, n_2)$$

Corollary (3.4 Euclid's recursion)

For all choices of the integers n_1 and $n_2 (\neq 0)$

$$\gcd(n_1, n_2) = \gcd(n_2, R_{n_2}(n_1))$$

Euclid's algorithm

Euclid's algorithm

To derive $\gcd(n_1, n_2)$, where $n_1, n_2 \in \mathbb{Z}^+$, use Euclid's division theorem repeatedly

$$r_{i-2} = q_i r_{i-1} + r_i,$$

where $r_{-2} = n_1$ and $r_{-1} = n_2$. The last reminder that is nonzero ($\neq 0$) is the gcd.

$$\begin{array}{rl|l}
n_1 &= q_0 n_2 + r_0 & = \gcd(n_1, n_2) = \gcd(n_2, r_0) \\
n_2 &= q_1 r_0 + r_1 & = \gcd(r_0, r_1) \\
r_0 &= q_2 r_1 + r_2 & = \gcd(r_1, r_2) \\
&\vdots & \vdots \\
r_{i-2} &= q_i r_{i-1} + r_i & = \gcd(r_{i-1}, r_i) \\
r_{i-1} &= q_{i+1} r_i & = \gcd(r_i, 0) = r_i
\end{array}$$

Euclid's algorithm (Ex)

Example

Let $n_1 = 1311$ and $n_2 = 391$.

$$
\begin{aligned}
& & \gcd(1311, 391) \\
1311 &= 3 \cdot 391 + 138 & &= \gcd(391, 138) \\
391 &= 2 \cdot 138 + 115 & &= \gcd(138, 115) \\
138 &= 1 \cdot 115 + 23 & &= \gcd(115, 23) \\
115 &= 5 \cdot 23 + 0 & &= \gcd(23, 0) = 23
\end{aligned}
$$

Hence, $\gcd(1311, 391) = 23$.

Bezout's identity

Theorem (3.6)

If n_1 and n_2 are two nonzero integers there exist two integers s and t such that

$$\gcd(n_1, n_2) = s \cdot n_1 + t \cdot n_2$$

The numbers s and t are not unique.

Derive Bezout's identity

Rewrite the steps in Euclid's algorithm:

$$
\begin{aligned}
n_1 &= q_0 n_2 + r_0 && \Rightarrow && r_0 &= n_1 - q_0 n_2 \\
n_2 &= q_1 r_0 + r_1 && \Rightarrow && r_1 &= n_2 - q_1 r_0 \\
r_0 &= q_2 r_1 + r_2 && \Rightarrow && r_2 &= r_0 - q_2 r_1 \\
&\vdots && && &\vdots \\
r_{i-2} &= q_i r_{i-1} + r_i && \Rightarrow && r_i &= r_{i-2} - q_i r_{i-1} \\
(r_{i-1} &= q_{i+1} r_i && \Rightarrow && 0 &= r_{i-1} - q_{i+1} r_i)
\end{aligned}
$$

Start with the second last row

$$\text{gcd} = r_i = r_{i-2} - q_i r_{i-1}$$

and substitute into the above row.

Bezout's identity (Ex)

Example

Find s and t such that $23 = s \cdot 1311 + t \cdot 391$

$$\begin{aligned} 23 &= 138 - 1 \cdot 115 \\ &= 138 - 1(391 - 3 \cdot 138) = -391 + 3 \cdot 138 \\ &= -391 + 3(1311 - 3 \cdot 391) = 3 \cdot 1311 - 10 \cdot 391 \end{aligned}$$

$\Rightarrow s = 3,\ t = -10.$

Bezout's identity (Ex)

Example (cont'd)

In the same way derive

$$0 = -17 \cdot 1311 + 57 \cdot 391$$

Use this to see that s and t are not unique

$$\begin{aligned} 23 &= 23 + 0 = 3 \cdot 1311 - 10 \cdot 391 - 17 \cdot 1311 + 57 \cdot 391 \\ &= -14 \cdot 1311 + 47 \cdot 391 \end{aligned}$$

$\Rightarrow s = -14,\ t = 47.$

Euclid's extended algorithm

Let n_1 and n_2 be two positive integers. Initialise the algorithm with

$$r_{-2} = n_1 \quad s_{-2} = 1 \quad t_{-2} = 0$$
$$r_{-1} = n_2 \quad s_{-1} = 0 \quad t_{-1} = 1$$

For $i \geq 0$ derive

$$q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \qquad s_i = s_{i-2} - q_i s_{i-1}$$
$$r_i = r_{i-2} - q_i r_{i-1} \qquad t_i = t_{i-2} - q_i t_{i-1}$$

Continue until $r_{i+1} = 0$. Then

$$\gcd(n_1, n_2) = r_i \text{ and } r_i = s_i n_1 + t_i n_2$$

From the proof we have: $r_j = s_j n_1 + t_j n_2, \quad \forall j.$

Euclid's extended algorithm (Ex)

Example

Let $n_1 = 1311$ and $n_2 = 391$.

i	q_i	r_i	s_i	t_i
-2	$-$	1311	1	0
-1	$-$	391	0	1
0	3	138	1	-3
1	2	115	-2	7
2	1	23	3	-10
3	5	0	-17	57

Hence,

$$\gcd(1311, 391) = 23 \text{ and } 23 = 3 \cdot 1311 - 10 \cdot 391$$

We also get that $0 = -17 \cdot 1311 + 57 \cdot 391$

Algebraic structures

Definition

An algebraic structure consists of a set $\mathcal{S}$ and one or more operations that are closed under $\mathcal{S}$ (i.e., the answer is an element of $\mathcal{S}$).

Computing modulo m

Definition

The set of integers modulo m, denoted $\mathbb{Z}_m$, and the two operations $\oplus$ and $\otimes$ are defined as:

- $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$
- $a \oplus b = R_m(a + b)$
- $a \otimes b = R_m(a \cdot b)$

$\mathbb{Z}_6$ tabulars

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

Example of operations are:

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Group

Definition

The algebraic structure $(G, *)$ is a commutative group if

$$a * b = b * a \qquad \text{(commutative)}$$
$$(a * b) * c = a * (b * c) \qquad \text{(associative)}$$
$$a * 0 = a \qquad \text{(0 exists)}$$
$$a * (-a) = 0 \qquad \text{($-a$ exists)}$$

What is $*$?

Ring

Definition

The algebraic structure $(R, +, \cdot)$ is a ring if the following criteria are fulfilled:

Addition:

$$a + b = b + a \quad \text{(commutative)}$$
$$(a + b) + c = a + (b + c) \quad \text{(associative)}$$
$$a + 0 = a \quad \text{(0 exists)}$$
$$a + (-a) = 0 \quad \text{($-a$ exists)}$$

Multiplication:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{(associative)}$$
$$a \cdot 1 = 1 \cdot a = a \quad \text{(1 exists)}$$

Combination:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{(distributive)}$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Cancellation law

Theorem (3.7)

Let $(R, +, \cdot)$ be a ring and $a, b, c \in R$. Then the cancellation law is fulfilled, i.e., if

$$a + b = a + c$$

then

$$b = c$$

See proof in book.

Commutative rings

Definition (3.3)

$(R, +, \cdot)$ is a commutative ring if it is a ring and multiplication is commutative,

$$a \cdot b = b \cdot a \qquad a, b \in R$$

0, 1, and $-a$ are unique

Theorem (3.8)

In a ring $(R, +, \cdot)$ the elements

- 0 *(zero)*
- 1 *(one)*
- $-a$ *(additive inverse)*

are unique.

See proofs in book.

Units

Definition (3.4)

An element a in a ring $(R, +, \cdot)$ is called a unit if it has a multiplicative inverse, i.e., if there is an element $a^{-1} \in R$ such that

$$aa^{-1} = a^{-1}a = 1$$

Theorem (3.9)

Let $(R, +, \cdot)$ be a ring. If the element $a \in R$ has a multiplicative inverse a^{-1} then this inverse is unique.

See proof in book.

Units (cont)

Example

Consider the multiplication table for $(\mathbb{Z}_2, \oplus, \otimes)$:

$\otimes$	0	1
0	0	0
1	0	1

The (non-zero) element 1 is a unit.

gcd

$\gcd(2, 1) = 1$

Units (cont)

Example

Consider the multiplication table for $(\mathbb{Z}_3, \oplus, \otimes)$:

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

The elements 1 and 2 are units.

gcd

$\gcd(3,1) = 1 \qquad \gcd(3,2) = 1$

Units (cont)

Example

Consider the multiplication table for $(\mathbb{Z}_4, \oplus, \otimes)$:

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

The elements 1 and 3 are units but the element 2 is not a unit.

gcd

$\gcd(4,1) = 1$ $\quad$ $\gcd(4,3) = 1$

$\gcd(4,2) = 2$

Units (cont)

Example

Consider the multiplication table for $(\mathbb{Z}_5, \oplus, \otimes)$:

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The elements 1, 2, 3 and 4 are units.

gcd

$\gcd(5,1) = 1 \quad \gcd(5,2) = 1 \quad \gcd(5,3) = 1 \quad \gcd(5,4) = 1$

Units (cont)

Example

Consider the multiplication table for $(\mathbb{Z}_6, \oplus, \otimes)$:

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The elements 1 and 5 are units while 2, 3 and 4 are not units

gcd

$\gcd(6,1) = 1 \quad \gcd(6,5) = 1$

$\gcd(6,2) = 2 \quad \gcd(6,3) = 3 \quad \gcd(6,4) = 2$

Theorem (3.10)

An element $a \in \mathbb{Z}_m$ is a unit if and only if m and a are relatively prime, $\gcd(m, a) = 1$.

We can find it using Bezout's identity!

Example: Find 37^{-1} in $(\mathbb{Z}_{101}, \oplus, \otimes)$

37^{-1} in $(\mathbb{Z}_{101}, \oplus, \otimes)$

Example

In $(\mathbb{Z}_{101}, \oplus, \otimes)$ find 37^{-1}. Since 101 is a prime the inverse exists. Use Euclid's extended algorithm to get

i	q_i	r_i	s_i	t_i
-2		101	1	0
-1		37	0	1
0	2	27	1	-2
1	1	10	-1	3
2	2	7	3	-8
3	1	3	-4	11
4	2	1	11	-30

$\Rightarrow 1 = 11 \cdot 101 + (-30) \cdot 37$, or equivalently

$$1 = R_{101}(11 \cdot 101 + (-30) \cdot 37) = R_{101}((-30) \cdot 37)$$
$$= R_{101}(R_{101}(-30) \cdot 37) = 71 \otimes 37$$

$$\Rightarrow 37^{-1} = 71$$

Fields

Definition (3.5)

$(F, +, \cdot)$ is a field if it is a commutative ring and all elements $a \neq 0$ are units.

Corollary (3.11)

$(\mathbb{Z}_p, \oplus, \otimes)$ *is a field if and only if* p *is a prime.*

Prime numbers

Definition

A prime is an integer (>1) that does not contain any other factors than it self and 1.

In other words, the positive integer p is a prime if and only if

$$\gcd(p, i) = 1, \qquad 1 \leq i < p$$

Field

Definition

The algebraic structure $(F, +, \cdot)$ is a field if the following criterias are fulfilled:

Addition:

$$a + b = b + a \quad \text{(commutative)}$$
$$(a + b) + c = a + (b + c) \quad \text{(associative)}$$
$$a + 0 = a \quad \text{(0 exists)}$$
$$a + (-a) = 0 \quad \text{($-a$ exists)}$$

Multiplication:

$$a \cdot b = b \cdot a \quad \text{(commutative)}$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{(associative)}$$
$$a \cdot 1 = a \quad \text{(1 exists)}$$
$$a \cdot a^{-1} = 1 \quad \text{(a^{-1} exists)}$$

Combination:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{(distributive)}$$