Some slides for 3rd Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

12-09-2011

Lemma 1.5.7

Let $m, n \in \mathbb{Z}$. Then there are integers $\lambda, \mu \in \mathbb{Z}$ such that

$$\lambda m + \mu n = \gcd(m, n)$$

Two integers $a, b \in \mathbb{Z}$ are called relatively prime if

$$\gcd(a, b) = 1$$

Exercise 14: If there are $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = 1$ then a and b are relatively prime.

Corollary 1.5.10

Suppose that $a \mid bc$, where $a, b, c \in \mathbb{Z}$ and a and b are relatively prime. Then $a \mid c$.

Lemma 1.5.7

Let $m, n \in \mathbb{Z}$. Then there are integers $\lambda, \mu \in \mathbb{Z}$ such that

$$\lambda m + \mu n = \gcd(m, n)$$

Corollary 1.5.11

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

- If a and b are relatively prime, $a \mid c$, $b \mid c$ then $ab \mid c$.
- If a and b are relatively prime and a and c are relatively prime then a and bc are relatively prime.

$$\mathbb{Z}/N = \{X \in \mathbb{N} : 0 \leq X < N\},$$

for $N \in \mathbb{N}$

Let $N = n_1 \cdots n_t \neq 0$, we define r the remainder map:

$$\begin{array}{rcl} r : \mathbb{Z}/N & \to & \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t \\ X & \mapsto & ([X]_{n_1}, \ldots, [X]_{n_t}) \end{array}$$

Lemma 1.6.3

Let $N = n_1 \cdots n_t$, with $n_1, \ldots, n_t \in \mathbb{N} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$ if $i \neq j$. Then the remainder map is bijective.

Theorem 1.6.4-The Chinese remainder theorem

Let $N = n_1 \cdots n_t$, with $n_1, \ldots, n_t \in \mathbb{Z} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$, for $i \neq j$. Consider the system

$$\begin{cases} X \equiv a_1 \pmod{n_1} \\ X \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ X \equiv a_t \pmod{n_t} \end{cases}$$

With $a_i \in \mathbb{Z}$. Then

1. The system has a solution $X \in \mathbb{Z}$.
2. If $X, Y \in \mathbb{Z}$ are solutions of the system then $X \equiv Y \pmod{N}$. If X is a solution of the system and $X \equiv Y \pmod{N}$ then Y is a solution of the system.

Proof:

- Consider n_j and N/n_j, they are relative prime for all j (Corollary 1.5.11).
- Consier the extended Euclidean algorithm to get λ_j, μ_j:

$$\lambda_j n_j + \mu_j \frac{N}{n_j} = 1$$

- Let $A_j = \mu_j \frac{N}{n_j}$ for all j.

$$A_j \equiv ?? \pmod{n_i}$$

Proof (1):

- Consider n_j and N/n_j, they are relative prime for all j (Corollary 1.5.11).
- Consier the extended Euclidean algorithm to get λ_j, μ_j:

$$\lambda_j n_j + \mu_j \frac{N}{n_j} = 1$$

- Let $A_j = \mu_j \frac{N}{n_j}$ for all j.

$$\begin{cases} A_j \equiv 1 \pmod{n_j} \\ A_j \equiv 0 \pmod{n_i}, \quad \text{for } i \neq j \end{cases}$$

Set $X = a_1 A_1 + \cdots + a_t A_t$.

Proof (2)

- We have two solutions $X, Y \in \mathbb{Z}$

$$\begin{cases} X \equiv a_j \pmod{n_j} & \text{for all } j \\ Y \equiv a_j \pmod{n_j} & \text{for all } j \end{cases}$$

- Hence $X \equiv Y \pmod{n_j}$ for all j
- Therefore $n_j \mid X - Y$, for all j.
- By corollary 1.5.11, $N = n_1 \cdots n_t \mid X - Y$, i.e.

$$X \equiv Y \pmod{N}$$

For the second part, assume X is a solution of the system and $X \equiv Y \pmod{N}$.

- Then $X \equiv Y \pmod{n_j}$, for all j
- Hence, Y is also a solution.

For the example:

X	$[\,]_2$	$[\,]_5$	$5a_1 - 4a_2$
0	0	0	$0 \equiv 0 \pmod{10}$
1	1	1	$1 \equiv 1 \pmod{10}$
2	0	2	$-8 \equiv 2 \pmod{10}$
3	1	3	$-7 \equiv 3 \pmod{10}$
4	0	4	$-16 \equiv 4 \pmod{10}$
5	1	0	$5 \equiv 5 \pmod{10}$
6	0	1	$-4 \equiv 6 \pmod{10}$
7	1	2	$-3 \equiv 7 \pmod{10}$
8	0	3	$-12 \equiv 8 \pmod{10}$
9	1	4	$-11 \equiv 9 \pmod{10}$