Some slides for 3rd Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

15-09-2010

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

$$\begin{cases} X \equiv a_1 (\mathrm{mod}\ n_1) \\ X \equiv a_2 (\mathrm{mod}\ n_2) \\ \quad \vdots \\ X \equiv a_t (\mathrm{mod}\ n_t) \end{cases}$$

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 $X \equiv Y (\mathrm{mod}\ N)$. If X is a solution of the system and $X \equiv Y (\mathrm{mod}\ N)$ 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.

$$A_j \equiv ?? (\mathrm{mod}\ n_i)$$

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.

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

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:

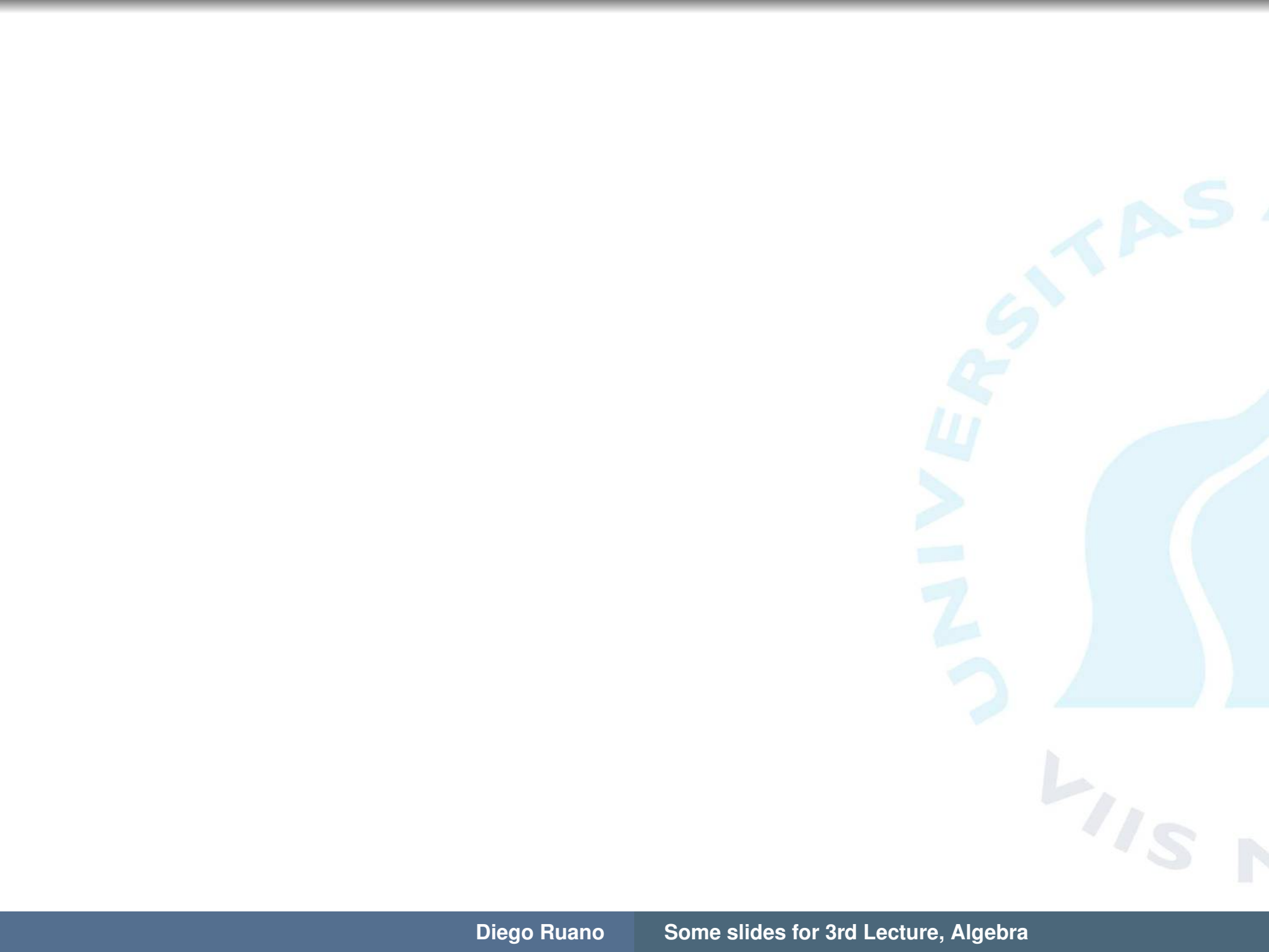
X	$[\,]_2$	$[\,]_5$	$5a_1 - 4a_2$
0	0	0	$0 \equiv 0 (\mathrm{mod}\ 10)$
1	1	1	$1 \equiv 1 (\mathrm{mod}\ 10)$
2	0	2	$-8 \equiv 2 (\mathrm{mod}\ 10)$
3	1	3	$-7 \equiv 3 (\mathrm{mod}\ 10)$
4	0	4	$-16 \equiv 4 (\mathrm{mod}\ 10)$
5	1	0	$5 \equiv 5 (\mathrm{mod}\ 10)$
6	0	1	$-4 \equiv 6 (\mathrm{mod}\ 10)$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

Euler's theorem

For RSA:

- $N = p \cdot q$, p and q primes..
- e a number for encription, d a number for decription.
- Public: N, e. Private: d.
- Message: $X, 0 \leq X < N$.
- Encription: $f(X) = [X^e]_N$
  Decription: $f(X) = [X^d]_N$.
  $g(f(X)) = X$.

Question: How do we choose e and d?
Answer: Using Euler's φ function



Proposition 1.7.1

Let $m, n \in \mathbb{N}$, relative prime. Then

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Proof:

- Let $N = mn$, consider remainder map

$$r : \mathbb{Z}/N \to \mathbb{Z}/m \times \mathbb{Z}/n$$

- Claim:

$$r((\mathbb{Z}/N)^*) = (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$$

Hence, the result holds because r is biyective.

The claim: $r((\mathbb{Z}/N)^*) = (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$

$$\gcd(X, N) = 1 \Leftrightarrow \gcd([X]_m, 1) = 1, \gcd([X]_n, 1) = 1$$

- By Proposition 1.5.1(ii),

$$\begin{cases} \gcd(X, m) = \gcd([X]_m, m) \\ \gcd(X, n) = \gcd([X]_n, n) \end{cases}$$

- But, by Corollary 1.5.11,

$$\left.\begin{array}{r} \gcd(X, m) = 1 \\ \gcd(X, n) = 1 \end{array}\right\} \Leftrightarrow \gcd(X, nm) = 1$$

Theorem 1.7.2 (Euler)

Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ relative prime. Then

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$$

Proof:

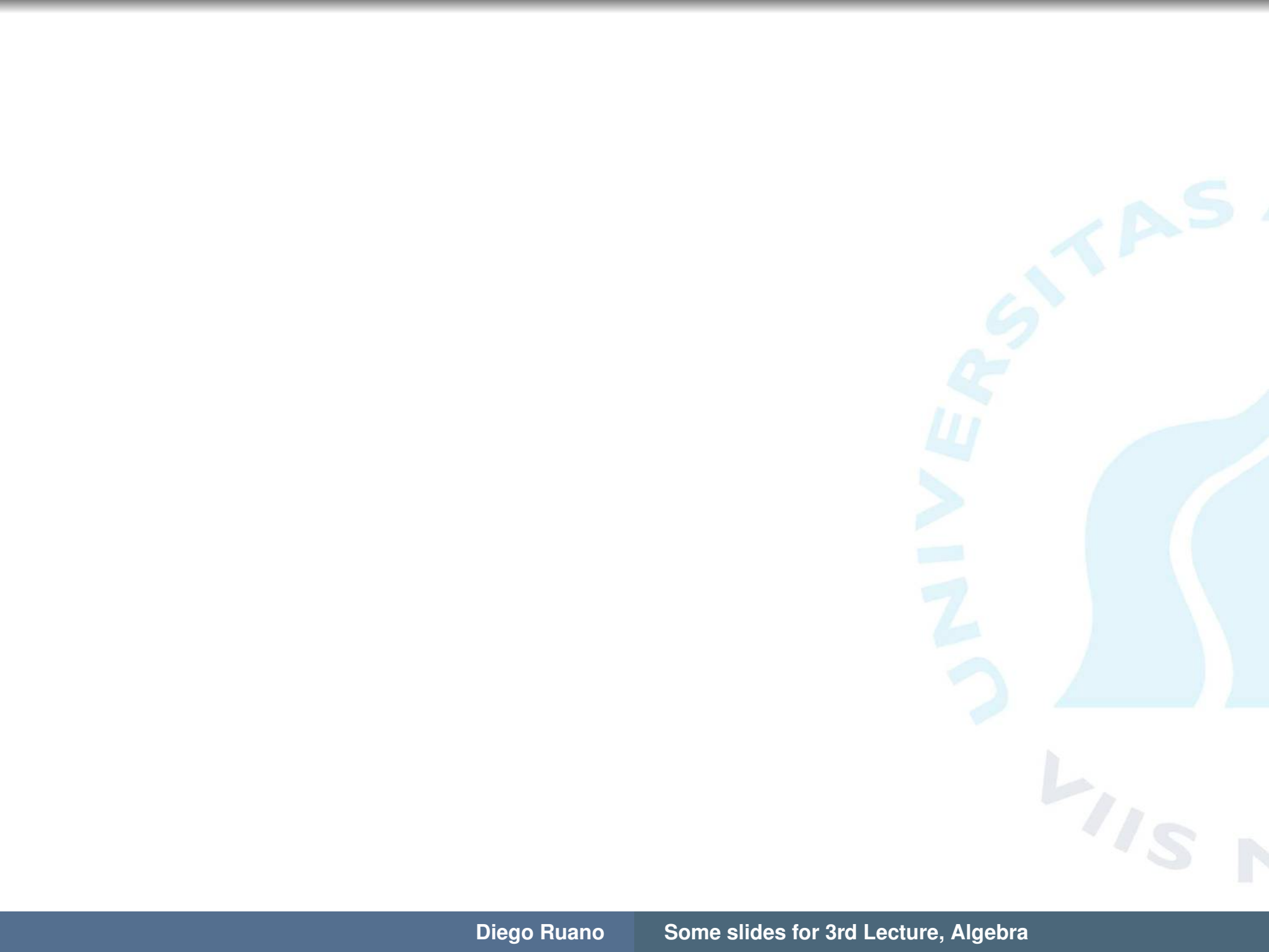
- List the numbers (lower than n) relative prime to n:

$$0 < a_1 < \cdots < a_{\varphi(n)} < n$$

Claim: $\{[aa_1]_n, \ldots, [aa_{\varphi(n)}]_n\} = \{a_1, \ldots, a_{\varphi(n)}\}$

- $[aa_i]_n = [aa_j]_n \Rightarrow n \mid a(a_i - a_j) \Rightarrow n \mid (a_i - a_j) \Rightarrow i = j$.
- $\gcd(n, aa_i) = 1 \Rightarrow \gcd(n, [aa_i]_n) = 1$

- Hence $[aa_1]_n \cdots [aa_{\varphi(n)}]_n = a_1 \cdots a_{\varphi(n)}$
- Then $aa_1 \cdots aa_{\varphi(n)} \equiv a_1 \cdots a_{\varphi(n)} (\mathrm{mod}\ n)$, but $aa_1 \cdots aa_{\varphi(n)} = a^{\varphi(n)} a_1 \cdots a_{\varphi(n)}$.
- That is, $n \mid a_1 \cdots a_{\varphi(n)} (a^{\varphi(n)} - 1)$.
- By corollary 1.5.10, $n \mid (a^{\varphi(n)} - 1)$.
- That is, $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$



Lemma 1.8.1

Every non-zero natural number $n \in \mathbb{N} \setminus \{0\}$ is a product of prime numbers.

Proof by induction:

1. 1 is the empty product of prime numbers by definition.
2. Assume that for $m < n$, m is product of primes. Is n prime?
   - Yes. Then $n = n$ is product of primes.
   - No. Then $n = n_1 n_2$. With $n_1, n_2 < n$. Apply induction hypothesis.

Theorem 1.8.2 (Euclid)

There are infinitely many prime numbers

Proof:

- Assume that $p_1, \ldots, p_n$ are all the prime numbers.
- Set $N = p_1 \cdots p_n + 1$
- By previous lemma, there exists p such that $p \mid N$.
- However, $p_i \nmid N$ for all i. Therefore, we have a new prime.

Lemma 1.8.3

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

Proof:

- If $p \mid a$ where finish.
- If $p \nmid a$, then $\gcd(a, p) = 1$

Hence by corollary 1.5.10 $p \mid b$.