Lecture 2

Sylwia Cichacz

Akademia Górniczo-Hutnicza w Krakowie

October 24, 2021, Kraków

Fermat's Little Theorem

From Wikipedia

Fermat's Little Theorem

$\phi(p) = p - 1$ for $p \in \mathbb{P}$.

From Wikipedia

$p = 17$

$25^{16} \equiv 1 \pmod{17}$

Theorem: Fermat's Little Theorem

If $p \in \mathbb{P}$ and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer n we have

$$n^p \equiv n \pmod{p}.$$

Euler's totient

$34^{67} \bmod 15 = 4^{67} \bmod 15$

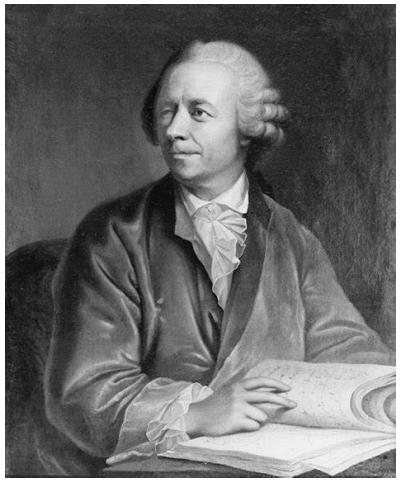
$= 4^{8 \cdot 8} \cdot 4^3 \bmod 15$

$= (4^8)^8 \cdot 4^2 \cdot 4 \bmod 15$

$= 1^8 \cdot 16 \cdot 4 \pmod{15}$

$= 1 \cdot 1 \cdot 4 \pmod{15}$

$\equiv 4 \pmod{15}$



From Wikipedia

Ex:

$n = 15 = 3 \cdot 5$

$\phi(n) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

$a^8 = 1 \bmod 15.$

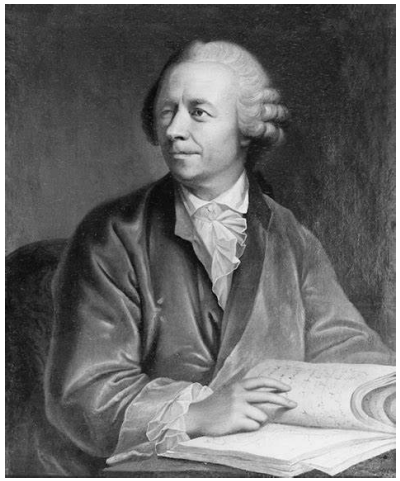
Theorem: Euler's Totient Theorem

If n and a are coprime positive integers, then

$67 = 8 \cdot 8 + 3$

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Euler's totient



From Wikipedia

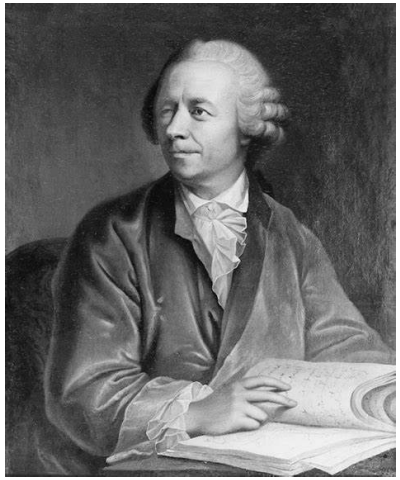
Theorem: Euler's Totient Theorem

If n and a are coprime positive integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

If $p \in \mathbb{P}$ then $\varphi(p) = p - 1$ thus Fermat's Little Theorem follows from Euler's Totient Theorem.

Euler's totient



From Wikipedia

Theorem: Euler's Totient Theorem

If n and a are coprime positive integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Example:

$(34)^{67} \pmod{15} =$

Definition:

Let A be a set. A binary operation on A is a function that assigns each ordered pair of elements of A an element of A.

$$\begin{array}{ccccc} a & + & b & = & c \\ \cap & & \cap & & \cap \\ R & & R & & R \end{array}$$

"$-$" is not a binary operation on $\mathbb{N}$.

Definition:

Let A be a set. A binary operation on A is a function that assigns each ordered pair of elements of A an element of A.

Let A be a non-empty set and $\circ$ be a binary operation $\circ : A \times A \to A$ (**Closure**). The structure $(A, \circ)$ is called a group, if the following conditions hold:

Definition:

Let A be a set. A binary operation on A is a function that assigns each ordered pair of elements of A an element of A.

Let A be a non-empty set and $\circ$ be a binary operation $\circ : A \times A \to A$ (**Closure**). The structure $(A, \circ)$ is called a group, if the following conditions hold:

- $\forall a, b, c \in A \ (a \circ b) \circ c = a \circ (b \circ c)$ – **associativity**

Definition:

Let A be a set. A binary operation on A is a function that assigns each ordered pair of elements of A an element of A.

Let A be a non-empty set and $\circ$ be a binary operation $\circ : A \times A \to A$ (**Closure**). The structure $(A, \circ)$ is called a group, if the following conditions hold:

- $\forall a, b, c \in A \ (a \circ b) \circ c = a \circ (b \circ c)$ – **associativity**
- $\exists e \in A, \ \forall a \in A \ a \circ e = e \circ a = a$ – **identity element** e

Definition:

Let A be a set. A binary operation on A is a function that assigns each ordered pair of elements of A an element of A.

Let A be a non-empty set and $\circ$ be a binary operation $\circ : A \times A \to A$ (**Closure**). The structure $(A, \circ)$ is called a group, if the following conditions hold:

- $\forall a, b, c \in A \ (a \circ b) \circ c = a \circ (b \circ c)$ – **associativity**
- $\exists e \in A, \ \forall a \in A \ a \circ e = e \circ a = a$ – **identity element**
- $\forall a \in A \ \exists a^{-1} \in A \ a \circ a^{-1} = a^{-1} \circ a = e$ – **inverse element**

Definition:

Let A be a set. A binary operation on A is a function that assigns each ordered pair of elements of A an element of A.

Let A be a non-empty set and $\circ$ be a binary operation $\circ : A \times A \to A$ (**Closure**). The structure $(A, \circ)$ is called a group, if the following conditions hold:

- $\forall a, b, c \in A \ (a \circ b) \circ c = a \circ (b \circ c)$ – **associativity**
- $\exists e \in A, \ \forall a \in A \ a \circ e = e \circ a = a$ – **identity element**
- $\forall a \in A \ \exists a^{-1} \in A \ a \circ a^{-1} = a^{-1} \circ a = e$ – **inverse element**

If $\forall a, b \in A \ a \circ b = b \circ a$ (**commutativity**), then group $(A, \circ)$ is called Abelian.

The structure $(\mathbb{Z}_m, +_m)$ where $\mathbb{Z}_m$ is the set of integers modulo m, is an Abelian group. Called Additive Group of Integers Modulo m.

Ex:

$(\mathbb{Z}_8, +_8)$ $\quad \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 6, 7\}$

$e = 0$

$3 + 7 = 2 \mod 8$

$2^{-1} = 6$, $6^{-1} = 2$

$7^{-1} = 1$, $1^{-1} = 7$

$3^{-1} = 5$, $5^{-1} = 3$

$4^{-1} = 4$

The structure $(\mathbb{Z}_m, +_m)$ where $\mathbb{Z}_m$ is the set of integers modulo m, is an Abelian group. Called Additive Group of Integers Modulo m.

Example:

$(\mathbb{Z}_8, +)$

The structure $(\mathbb{Z}_m^*, \cdot_m)$ where $\mathbb{Z}_m^*$ is the set of integers modulo m relatively prime to m, is an Abelian group. Called multiplicative Group of Integers Modulo m.

$(\mathbb{Z}_8^*, *)$ $\quad \mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$(\mathbb{Z}_{15}^*, *)$ $\quad \mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$|\mathbb{Z}_{15}^*| = \phi(15)$

The structure $(\mathbb{Z}_m^*, \cdot_m)$ where $\mathbb{Z}_m^*$ is the set of integers modulo m relatively prime to m, is an Abelian group. Called multiplicative Group of Integers Modulo m.

Example:

$(\mathbb{Z}_8^*, \cdot)$

Example:

Find the inverse of $114 \in \mathbb{Z}_{121}^*$.

$114^{-1} \equiv -52 \pmod{121} = 69 \bmod 121$

$114^{-1} = 69$

Step 1. $\gcd(114, 121) = 1$

Step 2. find $\alpha, \beta : 1 = \alpha \cdot 114 + \beta \cdot 121$

$-52 \cdot 114 + 49 \cdot 121 = 1 \pmod{121}$

$\alpha = -52$

$(-52 \cdot 114 + 49 \cdot 121) \pmod{121} = 1 \pmod{121}$

$-52 \cdot 114 = 1 \pmod{121}$

Definition:

The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ to denote the order of group G.

Definition:

The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ to denote the order of group G.

Definition:

The order of an element g of a group $(G, \circ)$ is the smallest positive integer (exponent) n such that $\underbrace{g \circ g \circ \ldots \circ g}_{n} = g^n = e$. If no such integer exists then we say that G has infinite order. The order of an element g is denoted by $|g|$.

Example:

Find all elements in the group $\mathbb{Z}_6$.

Example:

Find all elements in the group $\mathbb{Z}_8^*$.

Application of algebra – cryptography

Application of algebra – cryptography

$$M \xrightarrow{E} E(M) \xrightarrow{D} D(E(M)) = M$$

Application of algebra – cryptography

$$M \xrightarrow{E} E(M) \xrightarrow{D} D(E(M)) = M$$

Example:

Application of algebra – cryptography

$$M \xrightarrow{E} E(M) \xrightarrow{D} D(E(M)) = M$$

Example:

a) **Rabin method**:
$E(M) = M^2 \pmod{n}$, where $n > M$ and $n = p \cdot q$, $p, q \in \mathbb{P}$ – large, $p, q \equiv 3 \pmod{4}$

Application of algebra – cryptography

$$M \xrightarrow{E} E(M) \xrightarrow{D} D(E(M)) = M$$

Example:

a) **Rabin method**:
$E(M) = M^2 \pmod{n}$, where $n > M$ and $n = p \cdot q$, $p, q \in \mathbb{P}$ – large, $p, q \equiv 3 \pmod 4$

b) **RSA**:
$E(M) = M^k \pmod{n}$, where $n > M$ and $k \in \mathbb{Z}^*_{\varphi(n)}$,
$\varphi(n) = (p-1) \cdot (q-1)$

Application of algebra – cryptography

$$M \xrightarrow{E} E(M) \xrightarrow{D} D(E(M)) = M$$

Example:

a) **Rabin method**:
$E(M) = M^2 \pmod{n}$, where $n > M$ and $n = p \cdot q$, $p, q \in \mathbb{P}$ – large, $p, q \equiv 3 \pmod 4$

b) **RSA**:
$E(M) = M^k \pmod{n}$, where $n > M$ and $k \in \mathbb{Z}^*_{\varphi(n)}$,
$\varphi(n) = (p-1) \cdot (q-1)$

- Publish n

Application of algebra – cryptography

$$M \xrightarrow{E} E(M) \xrightarrow{D} D(E(M)) = M$$

Example:

a) **Rabin method**:
$E(M) = M^2 \pmod{n}$, where $n > M$ and $n = p \cdot q$, $p, q \in \mathbb{P}$ – large, $p, q \equiv 3 \pmod 4$

b) **RSA**:
$E(M) = M^k \pmod{n}$, where $n > M$ and $k \in \mathbb{Z}^*_{\varphi(n)}$,
$\varphi(n) = (p-1) \cdot (q-1)$

- Publish n
- Keep p and q private

Rabin method

$\sqrt{10} = 3, \ldots$

$\sqrt{10}$ in $\mathbb{Z}_{13}$ =

$\sqrt{c} = a$

$a^2 = c$

$\sqrt{10} = \{6, 7\}$

$b^2 = 10 \mod 13.$

$6^2 = 36 \mod 13 = 10 \mod 13$

$(-6)^2 = 36 \mod 13 = 10 \mod 13$

Rabin method

In Rabin method to calculate M we have to find proper root in $\mathbb{Z}_n$.

Rabin method

In Rabin method to calculate M we have to find proper root in $\mathbb{Z}_n$.
It is not easy!!

Rabin method

In Rabin method to calculate M we have to find proper root in $\mathbb{Z}_n$.
It is not easy!!

Theorem:

If $b^2 \equiv a \pmod{n}$, then $(n-b)^2 \equiv a \pmod{n}$.

Rabin method

In Rabin method to calculate M we have to find proper root in $\mathbb{Z}_n$.
It is not easy!!

Theorem:

If $b^2 \equiv a \pmod{n}$, then $(n-b)^2 \equiv a \pmod{n}$.

Definition:

Let $p \in \mathbb{P} \setminus \{2\}$ and $a \in \mathbb{Z}_p$. If there exists $b \in \mathbb{Z}_p$ such that $b^2 \equiv a \pmod{n}$, then a is called **quatradic residue modulo** n.

Rabin method

In Rabin method to calculate M we have to find proper root in $\mathbb{Z}_n$.
It is not easy!!

Theorem:

If $b^2 \equiv a \pmod{n}$, then $(n-b)^2 \equiv a \pmod{n}$.

Definition:

Let $p \in \mathbb{P} \setminus \{2\}$ and $a \in \mathbb{Z}_p$. If there exists $b \in \mathbb{Z}_p$ such that $b^2 \equiv a \pmod{n}$, then a is called **quatradic residue modulo** n.

Theorem:

Let $p \in \mathbb{P} \setminus \{2\}$ and $a \in \mathbb{Z}_p$. If there exists $b \in \mathbb{Z}_p$ such that $b^2 \equiv a \pmod{n}$, then a has exactly two square roots.

Rabin method

Example:

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$1, 2, 4$

$1^2 = 6^2 \equiv 1 \mod 7$

$2^2 \equiv 4 \mod 7 = 5^2$

$3^2 \equiv 2 \equiv 4^2 \mod 7$

Rabin method

Example:

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$1^2 = 6^2 \equiv 1 \pmod 7$, $2^2 = 5^2 \equiv 4 \pmod 7$, $3^2 = 4^2 \equiv 2 \pmod 7$.

Theorem:

Let $p \in \mathbb{P}$, $p \equiv 3 \pmod 4$, a – quadratic residue modulo p ($\exists b \in \mathbb{Z}_p : b^2 = a$), then the square roots with a in $\mathbb{Z}_p$ are

$$a^{\frac{p+1}{4}} \pmod p \text{ and } -a^{\frac{p+1}{4}}.$$

Ex : $p = 19$, $a = 9$

$$9^{\frac{19+1}{4}} = 9^{\frac{19+1}{4}} \bmod (19) = -9^5 \bmod (19)$$

$$9^5 = 9^2 \cdot 9^2 \cdot 9 = 81 \cdot 81 \cdot 9$$

$$= 5 \cdot 5 \cdot 9 \bmod 19 = 25 \cdot 9 \bmod 19$$

$$= 54 = 16$$

$$= (10)^5 \bmod 19$$

$$= 10^2 \cdot 10^2 \cdot 10 \bmod 19$$

$$= 100 \cdot 100 \cdot 10 \bmod 19$$

$$= 5 \cdot 5 \cdot 10 \bmod 19$$

$$= 250 \bmod 19 = 3 \bmod 19$$

Rabin method

Theorem:

Let $p \in \mathbb{P}$, $p \equiv 3 \pmod 4$, a – quadratic residue modulo p ($\exists b \in \mathbb{Z}_p : b^2 = a$), then the square roots with a in $\mathbb{Z}_p$ are

$$a^{\frac{p+1}{4}} \pmod p \text{ and } -a^{\frac{p+1}{4}}.$$

Example:

$a = 4$, $p = 7$

RSA method

RSA (Rivest-Shamir-Adleman) is one of the first (published in 1977) public-key cryptosystems and is widely used for secure data transmission.

$E(M) = M^k \pmod{n} \equiv a \pmod{n}$, where $n > M$ and $n = p \cdot q$, $p, q \in \mathbb{P}$ – large, $k \in \mathbb{Z}^*_{\varphi(n)}$, $\varphi(n) = (p-1)(q-1)$

$D(a) = a^m \equiv M \pmod{n}$, where $m = k^{-1}$ in $\mathbb{Z}^*_{\varphi(n)}$