# Криптографија
## - трећи део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

5. март 2024.

# Кармајклови бројеви

## Дефиниција

За сложен број $n$ кажемо да је Кармајклов ако важи $a^{n-1} \equiv 1 \pmod{n}$, за све $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$.

# Кармајклови бројеви

## Дефиниција

За сложен број $n$ кажемо да је Кармајклов ако важи $a^{n-1} \equiv 1 \pmod{n}$, за све $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$.

- Вероватноћа да број $n$ који није ни прост ни Кармајклов прође тест $a^{n-1} \equiv 1 \pmod{n}$
  - у једном тестирању (за једно конкретно $a$) је највише $\frac{1}{2}$
  - у $k$ тестирања са случајно (за $k$ независно изабраних $a$-ова) је највише $\frac{1}{2^k}$

# Кармајклови бројеви

## Дефиниција

За сложен број $n$ кажемо да је Кармајклов ако важи $a^{n-1} \equiv 1 \pmod{n}$, за све $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$.

- Вероватноћа да број $n$ који није ни прост ни Кармајклов прође тест $a^{n-1} \equiv 1 \pmod{n}$
  - у једном тестирању (за једно конкретно $a$) је највише $\frac{1}{2}$
  - у $k$ тестирања са случајно (за $k$ независно изабраних $a$-ова) је највише $\frac{1}{2^k}$
- Хоћемо тест који одваја просте од Кармајклових бројева

## Последица Мале Фермаове теореме

$p$ - непаран прост и $a \in \mathbb{Z}$ тд. НЗД$(a, p) = 1$. Тада је

$$(*) \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

## Последица Мале Фермаове теореме

$p$ - непаран прост и $a \in \mathbb{Z}$ тд. НЗД$(a, p) = 1$. Тада је

$$(*) \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

Доказ:

$a^{p-1} \equiv 1 \pmod{p} \quad \Longrightarrow \quad p \,\big|\, a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right),$

па $p$ дели бар једну заграду јер јер прост.

## Последица Мале Фермаове теореме

$p$ - непаран прост и $a \in \mathbb{Z}$ тд. НЗД$(a, p) = 1$. Тада је

$$(*) \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

Доказ:

$$a^{p-1} \equiv 1 \pmod{p} \quad \Longrightarrow \quad p \,\Big|\, a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right),$$

па $p$ дели бар једну заграду јер јер прост.

- Број на десној страни $(*)$ зовемо Лежандров симбол и означавамо са $\left(\frac{a}{p}\right)$

## Последица Мале Фермаове теореме

$p$ - непаран прост и $a \in \mathbb{Z}$ тд. НЗД$(a, p) = 1$. Тада је

$$(*) \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

Доказ:

$a^{p-1} \equiv 1 \pmod{p} \quad \Longrightarrow \quad p \,|\, a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right),$

па $p$ дели бар једну заграду јер јер прост.

- Број на десној страни $(*)$ зовемо Лежандров симбол и означавамо са $\left(\frac{a}{p}\right)$
- Детаљније о Лежандровим симболима: Мићић, Каделбург, Ђукић: Увод у теорију бројева, ДМС, 2021. - Глава 5

(Очигледне) особине:

- $\left(\frac{1}{p}\right) = 1$

(Очигледне) особине:

- $\left(\frac{1}{p}\right) = 1$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (баш $=$, не $\equiv$)

(Очигледне) особине:

- $\left(\frac{1}{p}\right) = 1$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (баш $=$, не $\equiv$)
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(Очигледне) особине:

- $\left(\frac{1}{p}\right) = 1$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (баш $=$, не $\equiv$)
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

## Веза са квадратним конгруенцијама

$p$ - непаран прост и $a \in \mathbb{Z}$ тд. НЗД$(a, p) = 1$. Тада конгруенцијска једначина

$$x^2 \equiv a \pmod{p}$$

има решења акко је $\left(\frac{a}{p}\right) = 1$.

## Веза са квадратним конгруенцијама

$p$ - непаран прост и $a \in \mathbb{Z}$ тд. НЗД$(a, p) = 1$. Тада конгруенцијска једначина

$$x^2 \equiv a \pmod{p}$$

има решења акко је $\left(\frac{a}{p}\right) = 1$.

Доказ: $(\Longrightarrow)$ ако има решења онда је
$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}} \equiv_p \left(x^2\right)^{\frac{p-1}{2}} = x^{p-1} \equiv_p 1$
$(\Longleftarrow)$ $a = g^k$, $g$ генератор $\mathbb{Z}_p^*$ и $k \in \mathbb{N}$,
$1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}}$, тада $p - 1 \left| \frac{k(p-1)}{2} \right.$, тј. $2|k$ и $x = g^{\frac{k}{2}}$ је решење конгруенције.

- Број решења једначине $x^2 \equiv a \pmod{p}$ је $1 + \left(\frac{a}{p}\right) \in \{0, 2\}$ јер по претх. теореми
  - ако је $\left(\frac{a}{p}\right) = -1$: једначина нема решења
  - ако је $\left(\frac{a}{p}\right) = 1$: једначина има једно решење $x_0$, али онда ће имати и друго решење $p - x_0$

- Број решења једначине $x^2 \equiv a \pmod{p}$ је $1 + \left(\frac{a}{p}\right) \in \{0, 2\}$ јер по претх. теореми
  - ако је $\left(\frac{a}{p}\right) = -1$: једначина нема решења
  - ако је $\left(\frac{a}{p}\right) = 1$: једначина има једно решење $x_0$, али онда ће имати и друго решење $p - x_0$
- Има $\frac{p-1}{2}$ $a$-ова за које је $\left(\frac{a}{p}\right) = 1$ и $\frac{p-1}{2}$ $a$-ова за које је $\left(\frac{a}{p}\right) = -1$ јер ако и $a$ гледамо као непознату $x^2 \equiv a \pmod{p}$ има $p - 1$ решење по $(x, a)$

- Број решења једначине $x^2 \equiv a \pmod{p}$ је $1 + \left(\frac{a}{p}\right) \in \{0, 2\}$ јер по претх. теореми
  - ако је $\left(\frac{a}{p}\right) = -1$: једначина нема решења
  - ако је $\left(\frac{a}{p}\right) = 1$: једначина има једно решење $x_0$, али онда ће имати и друго решење $p - x_0$
- Има $\frac{p-1}{2}$ $a$-ова за које је $\left(\frac{a}{p}\right) = 1$ и $\frac{p-1}{2}$ $a$-ова за које је $\left(\frac{a}{p}\right) = -1$ јер ако и $a$ гледамо као непознату $x^2 \equiv a \pmod{p}$ има $p - 1$ решење по $(x, a)$
- Занимљивост: За различите непарне просте $p$ и $q$ важи $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ (Гаусов закон квадратног реципроцитета)

- Број решења једначине $x^2 \equiv a \pmod{p}$ је $1 + \left(\frac{a}{p}\right) \in \{0, 2\}$ јер по претх. теореми
  - ако је $\left(\frac{a}{p}\right) = -1$: једначина нема решења
  - ако је $\left(\frac{a}{p}\right) = 1$: једначина има једно решење $x_0$, али онда ће имати и друго решење $p - x_0$
- Има $\frac{p-1}{2}$ $a$-ова за које је $\left(\frac{a}{p}\right) = 1$ и $\frac{p-1}{2}$ $a$-ова за које је $\left(\frac{a}{p}\right) = -1$ јер ако и $a$ гледамо као непознату
  $x^2 \equiv a \pmod{p}$ има $p - 1$ решење по $(x, a)$
- Занимљивост: За различите непарне просте $p$ и $q$ важи $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ (Гаусов закон квадратног реципроцитета)
- Повезује решавање $x^2 \equiv p \pmod{q}$ и $x^2 \equiv q \pmod{p}$

Пример: Да ли конгруенција $x^2 \equiv 2013 \pmod{2311}$ има решења?

$2013 = 3 \cdot 11 \cdot 61$ 2311 - прост

$\left(\frac{2013}{2311}\right) = \left(\frac{3}{2311}\right)\left(\frac{11}{2311}\right)\left(\frac{61}{2311}\right) = (*)$

$(-1)^{\frac{3-1}{2}\frac{2311-1}{2}} = -1 \Rightarrow \left(\frac{3}{2311}\right) = -\left(\frac{2311}{3}\right) = -\left(\frac{3\cdot 770+1}{3}\right) = -\left(\frac{1}{3}\right) = -1$

$(-1)^{\frac{11-1}{2}\frac{2311-1}{2}} = -1 \Rightarrow \left(\frac{11}{2311}\right) = -\left(\frac{2311}{11}\right) = -\left(\frac{21\cdot 11+1}{11}\right) = -\left(\frac{1}{11}\right) = -1$

$(-1)^{\frac{61-1}{2}\frac{2311-1}{2}} = 1 \Rightarrow \left(\frac{61}{2311}\right) = \left(\frac{2311}{61}\right) = \left(\frac{61\cdot 37+54}{61}\right) = \left(\frac{54}{61}\right) = \left(\frac{-7}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{7}{61}\right)$

$\left(\frac{-1}{61}\right) = (-1)^{\frac{61-1}{2}} = 1$

$(-1)^{\frac{7-1}{2}\frac{61-1}{2}} = 1 \Rightarrow \left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$ јер $x^2 \equiv 2 \pmod 5$ нема решења

$(-1)^{\frac{5-1}{2}\frac{7-1}{2}} = 1$

$(*) = (-1)(-1)\cdot 1\cdot(-1) = -1$

$\Rightarrow x^2 \equiv 2013 \pmod{2311}$ нема решење

Како се уопштава $\left(\frac{\cdot}{n}\right)$ на непаран сложен природан број $n$?

Како се уопштава $\left(\frac{\cdot}{n}\right)$ на непаран сложен природан број $n$?

- Запишемо $n$ као $n = p_1 p_2 \dots p_k$, где су $p_i$ прости, не обавезно различити бројеви
- За НЗД$(a, n) = 1$ дефинишемо Јакобијев симбол $\left(\frac{a}{n}\right)$ као $\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_k}\right)$

Како се уопштава $\left(\frac{\cdot}{n}\right)$ на непаран сложен природан број $n$?

- Запишемо $n$ као $n = p_1 p_2 \dots p_k$, где су $p_i$ прости, не обавезно различити бројеви
- За НЗД$(a, n) = 1$ дефинишемо Јакобијев симбол $\left(\frac{a}{n}\right)$ као $\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_k}\right)$
- Веза са квадратним конгруенцијама
  - Ако $x^2 \equiv a \pmod{n}$ има решење онда је $\left(\frac{a}{n}\right) = 1$
  - Обрнуто не важи: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, али $x^2 \equiv 2 \pmod{15}$ нема решење

Како се уопштава $\left(\frac{\cdot}{n}\right)$ на непаран сложен природан број $n$?

- Запишемо $n$ као $n = p_1 p_2 \dots p_k$, где су $p_i$ прости, не обавезно различити бројеви
- За НЗД$(a, n) = 1$ дефинишемо Јакобијев симбол $\left(\frac{a}{n}\right)$ као $\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_k}\right)$
- Веза са квадратним конгруенцијама
  - Ако $x^2 \equiv a \pmod{n}$ има решење онда је $\left(\frac{a}{n}\right) = 1$
  - Обрнуто не важи: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, али $x^2 \equiv 2 \pmod{15}$ нема решење
- Да ли и даље важи

$$(\bigstar) \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

Како се уопштава $\left(\frac{\cdot}{n}\right)$ на непаран сложен природан број $n$?

- Запишемо $n$ као $n = p_1 p_2 \dots p_k$, где су $p_i$ прости, не обавезно различити бројеви
- За НЗД$(a, n) = 1$ дефинишемо Јакобијев симбол $\left(\frac{a}{n}\right)$ као $\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_k}\right)$
- Веза са квадратним конгруенцијама
  - Ако $x^2 \equiv a \pmod{n}$ има решење онда је $\left(\frac{a}{n}\right) = 1$
  - Обрнуто не важи: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, али $x^2 \equiv 2 \pmod{15}$ нема решење
- Да ли и даље важи

$$(\bigstar) \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

- ! лева страна не мора бити $\equiv_n \pm 1$

## Дефиниција

Ако за пародан број $a$ и сложен број $n$ тд. НЗД$(a, n) = 1$ важи ($\bigstar$) кажемо да је $n$ Ојлеров псеудопрост број у бази $a$.

## Дефиниција

Ако за природан број $a$ и сложен број $n$ тд. НЗД$(a, n) = 1$ важи $(\bigstar)$ кажемо да је $n$ Ојлеров псеудопрост број у бази $a$.

Пример: Видели смо да је $91$ псеудопрост у бази $3$, али неће бити Ојлеров псеудопрост у истој бази јер је $3^{45} \equiv_{91} 27$. Али, $91$ је Ојлеров псеудопрост у бази $10$ јер је $10^{45} \equiv_{91} -1 = \left(\frac{10}{91}\right)$

## Дефиниција

Ако за пародан број $a$ и сложен број $n$ тд. НЗД$(a, n) = 1$ важи ($\bigstar$) кажемо да је $n$ Ојлеров псеудопрост број у бази $a$.

Пример: Видели смо да је $91$ псеудопрост у бази $3$, али неће бити Ојлеров псеудопрост у истој бази јер је $3^{45} \equiv_{91} 27$. Али, $91$ је Ојлеров псеудопрост у бази $10$ јер је $10^{45} \equiv_{91} -1 = \left(\frac{10}{91}\right)$

- Немамо аналог Кармајклових бројева - Не постоји сложен број $n$ који је Ојлеров псеудопрост у свакој бази! (видети Коблиц, Глава V.1)

## Дефиниција

Ако за природан број $a$ и сложен број $n$ тд. НЗД$(a, n) = 1$ важи ($\bigstar$) кажемо да је $n$ Ојлеров псеудопрост број у бази $a$.

Пример: Видели смо да је $91$ псеудопрост у бази $3$, али неће бити Ојлеров псеудопрост у истој бази јер је $3^{45} \equiv_{91} 27$. Али, $91$ је Ојлеров псеудопрост у бази $10$ јер је $10^{45} \equiv_{91} -1 = \left(\frac{10}{91}\right)$

- Немамо аналог Кармајклових бројева - Не постоји сложен број $n$ који је Ојлеров псеудопрост у свакој бази! (видети Коблиц, Глава V.1)

## Ојлеров псеудопрост у бази $a$ $\Longrightarrow$ псеудопрост у бази $a$

Доказ: $a^{n-1} = \left(a^{\frac{n-1}{2}}\right)^2 \equiv_n (\pm 1)^2 = 1$

## Дефиниција

Ако за пародан број $a$ и сложен број $n$ тд. НЗД$(a, n) = 1$ важи ($\bigstar$) кажемо да је $n$ Ојлеров псеудопрост број у бази $a$.

Пример: Видели смо да је $91$ псеудопрост у бази $3$, али неће бити Ојлеров псеудопрост у истој бази јер је $3^{45} \equiv_{91} 27$. Али, $91$ је Ојлеров псеудопрост у бази $10$ јер је $10^{45} \equiv_{91} -1 = \left(\frac{10}{91}\right)$

- Немамо аналог Кармајклових бројева - Не постоји сложен број $n$ који је Ојлеров псеудопрост у свакој бази! (видети Коблиц, Глава V.1)

## Ојлеров псеудопрост у бази $a$ $\Longrightarrow$ псеудопрост у бази $a$

Доказ: $a^{n-1} = \left(a^{\frac{n-1}{2}}\right)^2 \equiv_n (\pm 1)^2 = 1$

- Све заједно: добићемо тест који има исту или бољу ефикасност од Кармајкловог, а филтрира само просте бројеве.

## Соловеј-Штрасенов тест

Нека је $n \in \mathbb{N}$ непаран број и $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$. Број $n$ пролази тест у бази $a$ ако је

$$(\bigstar) \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

## Соловеј-Штрасенов тест

Нека је $n \in \mathbb{N}$ непаран број и $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$. Број $n$ пролази тест у бази $a$ ако је

$$(\bigstar) \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

- Ако број $n$ прође тест за $k$ независно изабраних база, вероватноћа да је $n$ прост је $1 - \frac{1}{2^k}$

## Соловеј-Штрасенов тест

Нека је $n \in \mathbb{N}$ непаран број и $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$. Број $n$ пролази тест у бази $a$ ако је

$$(\bigstar) \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

- Ако број $n$ прође тест за $k$ независно изабраних база, вероватноћа да је $n$ прост је $1 - \frac{1}{2^k}$
- Како се рачуна десна страна $(\bigstar)$?

Имплементација Јакобијевог симбола у python-у:

- улаз: $m$ и $n$ - узајамно прости непарни позитивни
- користи особине
  - $\left(\frac{1}{n}\right) = 1$
  - $\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{за } n \equiv \pm 1 \pmod 8, \\ -1, & \text{за } n \equiv \pm 3 \pmod 8, \end{cases}$
  - $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
  - $a \equiv b \pmod p \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
  - (реципроцитет) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$

  за $a, b \in \mathbb{N}$

Имплементација Јакобијевог симбола у python-у:

- улаз: $m$ и $n$ - узајамно прости непарни позитивни
- користи особине
  - $\left(\frac{1}{n}\right) = 1$
  - $\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{за } n \equiv \pm 1 \pmod 8, \\ -1, & \text{за } n \equiv \pm 3 \pmod 8, \end{cases}$
  - $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
  - $a \equiv b \pmod p \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
  - (реципроцитет) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$

  за $a, b \in \mathbb{N}$
- Иста стратегија као у примеру $x^2 \equiv 2013 \pmod{2311}$

Рекурзивна функција рачуна вредност $\left(\frac{m}{n}\right)$, за $m, n \in \mathbb{N}$, $2 \nmid n$:

```
def jacobi(m, n):
    if m == 1:
        return 1

    if (m >= n):
        return jacobi(m%n, n)

    if m % 2 == 0:
        if (n%8 == 3 or n%8 == 5):
            return -jacobi(m/2, n)
        else:
            return +jacobi(m/2, n)

    if m % 4 == 3 and n % 4 == 3:
        return -jacobi(n, m)
    else:
        return jacobi(n, m)
```

# Милер-Рабинов тест прималности

- Показали смо
$$a^{p-1} \equiv 1 \pmod{p} \quad \Longrightarrow \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

# Милер-Рабинов тест прималности

- Показали смо
  $a^{p-1} \equiv 1 \pmod{p} \quad \Longrightarrow \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$
- Али ако је $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ и $\frac{p-1}{2}$ парно ово можемо поновити и добити $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$

# Милер-Рабинов тест прималности

- Показали смо
  $a^{p-1} \equiv 1 \pmod{p} \quad \Longrightarrow \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$
- Али ако је $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ и $\frac{p-1}{2}$ парно ово можемо поновити и добити $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$
- Поступак понављамо све док је $a^{\frac{p-1}{2^i}} \equiv 1 \pmod{p}$ и $\frac{p-1}{2^i}$ парно и добијамо $a^{\frac{p-1}{2^{i+1}}} \equiv \pm 1 \pmod{p}$

# Милер-Рабинов тест прималности

- Показали смо
  $a^{p-1} \equiv 1 \pmod{p} \quad \Longrightarrow \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$
- Али ако је $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ и $\frac{p-1}{2}$ парно ово можемо поновити и добити $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$
- Поступак понављамо све док је $a^{\frac{p-1}{2^i}} \equiv 1 \pmod{p}$ и $\frac{p-1}{2^i}$ парно и добијамо $a^{\frac{p-1}{2^{i+1}}} \equiv \pm 1 \pmod{p}$
- Низ $a^{\frac{p-1}{2}}, a^{\frac{p-1}{2^2}}, a^{\frac{p-1}{2^3}}, \ldots$ је конгруентан $\underbrace{1, \ldots, 1}_{k \text{ пута}}, -1, \underbrace{\ldots}_{\text{било шта}}$, за $k \geqslant 0$

## Милер-Рабинов тест прималности

Нека је $n$ непаран и $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$. Запишемо $n - 1 = 2^r d$, где је $d$ непаран.

$$a_j = a^{2^j d} \bmod p, \qquad \text{за } j = 0, 1, \ldots, r-1$$

Број $n$ пролази Милер-Рабинов тест у бази $a$ ако је испуњен један од услова

1. $a_0 = 1$
2. постоји $0 \leqslant s \leqslant r - 1$ тд. $a_s = -1$

- Приметимо да је $a_{j+1} \equiv a_j^2 \pmod p$ и
  1. $\Longrightarrow$ сви $a_j = 1$
  2. $\Longrightarrow a_j = 1$ за $j > s$

## Милер-Рабинов тест прималности

Нека је $n$ непаран и $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$. Запишемо $n - 1 = 2^r d$, где је $d$ непаран.

$$a_j = a^{2^j d} \bmod p, \qquad \text{за } j = 0, 1, \ldots, r-1$$

Број $n$ пролази Милер-Рабинов тест у бази $a$ ако је испуњен један од услова

1. $a_0 = 1$
2. постоји $0 \leqslant s \leqslant r - 1$ тд. $a_s = -1$

- Приметимо да је $a_{j+1} \equiv a_j^2 \pmod p$ и
  1. $\Longrightarrow$ сви $a_j = 1$
  2. $\Longrightarrow a_j = 1$ за $j > s$
- За сложен $n$ број који пролази Милер-Рабинов тест у бази $a$ кажемо да је јако псеудопрост у бази $a$

**ЈАКО ПСЕУДОПРОСТ У БАЗИ $a$ $\Longrightarrow$ ПСЕУДОПРОСТ У БАЗИ $a$**

Доказ: $a^{n-1} \equiv a_{r-1}^2 \pmod{n}$

- Последица: Ефикасност Милер-Рабиновог теста $\geqslant$ ефикасност Кармајкловог теста

## ЈАКО ПСЕУДОПРОСТ У БАЗИ $a$ $\Longrightarrow$ ПСЕУДОПРОСТ У БАЗИ $a$

Доказ: $a^{n-1} \equiv a_{r-1}^2 \pmod{n}$

- Последица: Ефикасност Милер-Рабиновог теста $\geqslant$ ефикасност Кармајкловог теста
- али имамо и више

## Теорема

1. Не постоји сложен број $n$ који је јако псеудопрост у свакој бази $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$
2. Ако је $n$ непаран сложен, онда он може бити јако псеудопрост за највише четвртину база $a \in \mathbb{Z}_n^*$.

Комплетан доказ у Коблиц, глава V.1

## ЈАКО ПСЕУДОПРОСТ У БАЗИ $a \implies$ ПСЕУДОПРОСТ У БАЗИ $a$

Доказ: $a^{n-1} \equiv a_{r-1}^2 \pmod{n}$

- Последица: Ефикасност Милер-Рабиновог теста $\geqslant$ ефикасност Кармајкловог теста
- али имамо и више

## Теорема

1. Не постоји сложен број $n$ који је јако псеудопрост у свакој бази $a \in \mathbb{Z}$ тд. НЗД$(a, n) = 1$
2. Ако је $n$ непаран сложен, онда он може бити јако псеудопрост за највише четвртину база $a \in \mathbb{Z}_n^*$.

Комплетан доказ у Коблиц, глава V.1

- Ефикасност Милер-Рабиновог теста је најмање $1 - \frac{1}{4^k}$, где је $k$ број тестирања

| | |
|---|---|
| $\boldsymbol{n = 104717}$, $n-1 = 2^2 \cdot 26179$.<br>Choose $a = 96152$.<br>$a^{26179} \equiv 1 \pmod{n}$<br>*Conclusion:* $n$ is ***probably prime***. | $\boldsymbol{n = 577757}$, $n-1 = 2^2 \cdot 144439$.<br>Choose $a = 314997 \pmod{n}$.<br>$a^{144439} \equiv 373220 \pmod{n}$<br>$a^{2 \cdot 144439} \equiv 577756 \equiv -1 \pmod{n}$<br>*Conclusion:* $n$ is ***probably prime***. |
| $\boldsymbol{n = 101089}$, $n-1 = 2^5 \cdot 3159$.<br>Choose $a = 5$.<br>$a^{3159} \equiv 101088 \equiv -1 \pmod{n}$<br>*Conclusion:* $n$ is ***probably prime***. | $\boldsymbol{n = 280001}$, $n-1 = 2^6 \cdot 4375$.<br>Choose $a = 105532$.<br>$a^{4375} \equiv 236926 \pmod{n}$<br>$a^{2 \cdot 4375} \equiv 168999 \pmod{n}$<br>$a^{2^2 \cdot 4375} \equiv 280000 \equiv -1 \pmod{n}$<br>*Conclusion:* $n$ is ***probably prime***. |

probably prime = прост са вероватноћом најмање $\frac{3}{4}$

**$n = 252601$**, $n-1 = 2^3 \cdot 31575$.
Choose $a = 85132$.

$$a^{31575} \equiv 191102 \pmod{n}$$
$$a^{2 \cdot 31575} \equiv 184829 \pmod{n}$$
$$a^{2^2 \cdot 31575} \equiv 1 \pmod{n}$$

*Conclusion:* $n$ is ***composite***.
(184829 is a square root of 1, mod $n$, different from $\pm 1$.)

**$n = 3057601$**, $n-1 = 2^6 \cdot 47775$.
Choose $a = 99908 \pmod{n}$.

$$a^{47775} \equiv 1193206 \pmod{n}$$
$$a^{2 \cdot 47775} \equiv 2286397 \pmod{n}$$
$$a^{2^2 \cdot 47775} \equiv 235899 \pmod{n}$$
$$a^{2^3 \cdot 47775} \equiv 1 \pmod{n}$$

*Conclusion:* $n$ is ***composite***.
(235899 is a square root of 1, mod $n$, different from $\pm 1$.)

```python
def miller_rabin(n, k):
    if n <= 3:
        if n == 1:
            return False
        return True

    # n prost => n neparan => n = (2 ^ r) * d + 1
    d = n - 1
    r = 0
    while d % 2 == 0:
        r = r + 1
        d = d // 2

    for i in range(k):
        a = random.randrange(2, n - 1)

        x = mod_pow(a, d, n)

        if x == 1 or x == n - 1:  # n - 1 = -1 (mod n)
            continue

        witness = True

        for j in range(r - 1):
            x = mod_pow(x, 2, n)
            if x == 1:
                return False
            if x == n - 1:
                witness = False
                break

        if witness:
            return False

    return True
```

Функција која користи Милер-Рабинов тест да генерише случајан број који је прост са вероватноћом барем $1 - \frac{1}{4^k}$

```
def get_prime(limit, k = 20):
    is_prime = False
    n = 2*random.randrange(limit)+1
    while not is_prime:
        is_prime = miller_rabin(n, k)
        n = n+2
    return n
```

# RCA криптосистем (Ривест-Шамир-Ејдлман)

Алиса жели да пошаље поруку или кључ Бобану

- Бобан тајно бира два велика проста броја $p$ и $q$, множи их $n = pq$ и рачуна $\varphi(n) = (p-1)(q-1)$

# RSA криптосистем (Ривест-Шамир-Ејдлман)

Алиса жели да пошаље поруку или кључ Бобану

- Бобан тајно бира два велика проста броја $p$ и $q$, множи их $n = pq$ и рачуна $\varphi(n) = (p-1)(q-1)$
- Затим Бобан бира број $1 \leqslant e \leqslant \varphi(n)$ тд. НЗД$(e, \varphi(n)) = 1$ и рачуна $d = e^{-1} \bmod \varphi(n)$

# РСА криптосистем (Ривест-Шамир-Ејдлман)

Алиса жели да пошаље поруку или кључ Бобану

- Бобан тајно бира два велика проста броја $p$ и $q$, множи их $n = pq$ и рачуна $\varphi(n) = (p-1)(q-1)$
- Затим Бобан бира број $1 \leqslant e \leqslant \varphi(n)$ тд. НЗД$(e, \varphi(n)) = 1$ и рачуна $d = e^{-1} \bmod \varphi(n)$
- Бобан шаље Алиси јавни кључ $(n, e)$, а $d$ чува као свој тајни кључ. У овом тренутку Бобан може да заборави $p$ и $q$, али је битно да их не објављује

# RCA криптосистем (Ривест-Шамир-Ејдлман)

Алиса жели да пошаље поруку или кључ Бобану

- Бобан тајно бира два велика проста броја $p$ и $q$, множи их $n = pq$ и рачуна $\varphi(n) = (p-1)(q-1)$
- Затим Бобан бира број $1 \leqslant e \leqslant \varphi(n)$ тд. НЗД$(e, \varphi(n)) = 1$ и рачуна $d = e^{-1} \bmod \varphi(n)$
- Бобан шаље Алиси јавни кључ $(n, e)$, а $d$ чува као свој тајни кључ. У овом тренутку Бобан може да заборави $p$ и $q$, али је битно да их не објављује
- Ако је $M < n$ кодирана порука, Алиса рачуна $N = M^e \bmod n$ и шаље Бобану

# РСА криптосистем (Ривест-Шамир-Ејдлман)

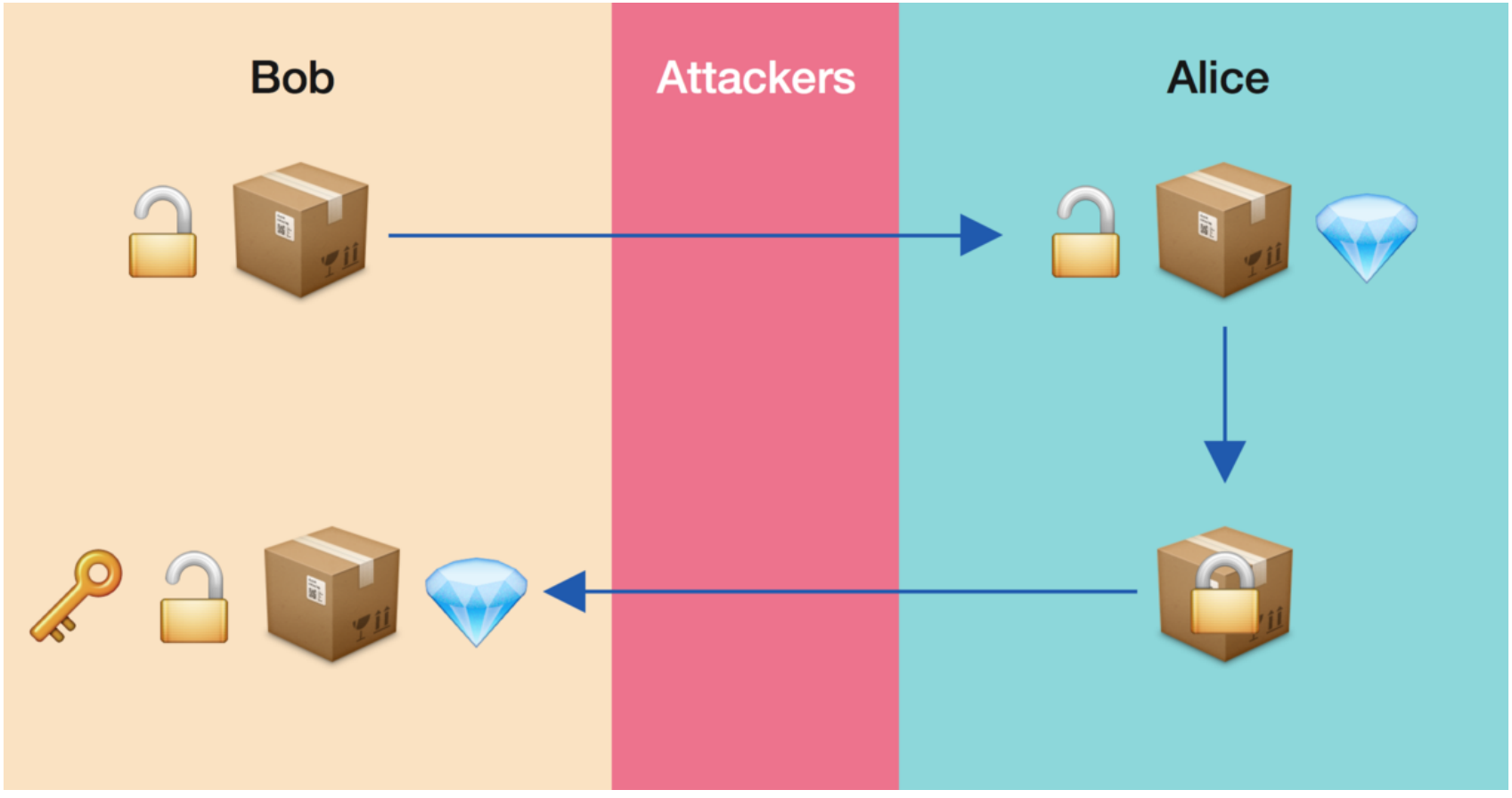
Алиса жели да пошаље поруку или кључ Бобану

- Бобан тајно бира два велика проста броја $p$ и $q$, множи их $n = pq$ и рачуна $\varphi(n) = (p-1)(q-1)$
- Затим Бобан бира број $1 \leqslant e \leqslant \varphi(n)$ тд. НЗД$(e, \varphi(n)) = 1$ и рачуна $d = e^{-1} \bmod \varphi(n)$
- Бобан шаље Алиси јавни кључ $(n, e)$, а $d$ чува као свој тајни кључ. У овом тренутку Бобан може да заборави $p$ и $q$, али је битно да их не објављује
- Ако је $M < n$ кодирана порука, Алиса рачуна $N = M^e \bmod n$ и шаље Бобану
- Бобан има тајни кључ $d$ помоћу кога лако рачуна $N^d \equiv M^{ed} \equiv M \pmod{n}$. Овде се користи $ed \equiv 1 \pmod{\varphi(n)}$ и Ојлерова теорема

# РСА криптосистем (Ривест-Шамир-Ејдлман)

Алиса жели да пошаље поруку или кључ Бобану

- Бобан тајно бира два велика проста броја $p$ и $q$, множи их $n = pq$ и рачуна $\varphi(n) = (p-1)(q-1)$
- Затим Бобан бира број $1 \leqslant e \leqslant \varphi(n)$ тд. НЗД$(e, \varphi(n)) = 1$ и рачуна $d = e^{-1} \bmod \varphi(n)$
- Бобан шаље Алиси јавни кључ $(n, e)$, а $d$ чува као свој тајни кључ. У овом тренутку Бобан може да заборави $p$ и $q$, али је битно да их не објављује
- Ако је $M < n$ кодирана порука, Алиса рачуна $N = M^e \bmod n$ и шаље Бобану
- Бобан има тајни кључ $d$ помоћу кога лако рачуна $N^d \equiv M^{ed} \equiv M \pmod{n}$. Овде се користи $ed \equiv 1 \pmod{\varphi(n)}$ и Ојлерова теорема
- Цица види $n$, $e$ и $N$, али не може да дође до поруке $M$ све док не одреди $d$ тј. $\varphi(n)$


Bob
Attackers
Alice

- $f(M) = M^e \bmod n$ је пример привидно једносмерне функције, то значи да
  - $f$ је једносмерна за Алису и Цицу: оне не могу да одреде $f^{-1}$ у реалном времену
  - $f$ није једносмерна за Бобана: он је могао да одреди $f^{-1}$ јер је имао податак више (факторизацију $n$)

- $f(M) = M^e \bmod n$ је пример привидно једносмерне функције, то значи да
  - $f$ је једносмерна за Алису и Цицу: оне не могу да одреде $f^{-1}$ у реалном времену
  - $f$ није једносмерна за Бобана: он је могао да одреди $f^{-1}$ јер је имао податак више (факторизацију $n$)
- Основна претпоставка PCA криптосистема: Не може се ефикасно израчунати Ојлерова функција!

- $f(M) = M^e \bmod n$ је пример привидно једносмерне функције, то значи да
  - $f$ је једносмерна за Алису и Цицу: оне не могу да одреде $f^{-1}$ у реалном времену
  - $f$ није једносмерна за Бобана: он је могао да одреди $f^{-1}$ јер је имао податак више (факторизацију $n$)
- Основна претпоставка PCA криптосистема: Не може се ефикасно израчунати Ојлерова функција!

**Нека је $n = pq$ и нека је $n$ познато. Тада је $\varphi(n)$ познато акко су познати $p$ и $q$**

Доказ: ($\Longleftarrow$) $\varphi(n) = (p-1)(q-1)$
($\Longrightarrow$) Тада је познато и $pq = n$ и $p + q = n - \varphi(n) + 1$.
Вијетова правила: $p$ и $q$ могу одредити као корени квадратне једначине $x^2 - (n - \varphi(n) + 1)x + n$

Пример: Бобан бира $p = 17$, $q = 41$. Он затим израчунава $n = pq = 17 \cdot 41 = 697$ и $\varphi(n) = (17-1)(41-1) = 640$. Он бира $e = 33$, што је узајамно просто са 640. Он затим израчунава $d \equiv 33^{-1} \pmod{640} = 97$. Бобан на свој сајт ставља пар $n = 697$, $e = 33$.

Алиса жели да користи афину шифру $C = aP + b \pmod{26}$ са кључем, $C \equiv 7P + 25 \pmod{26}$ да би Бобану могла да пошаље дугачку поруку. Она кодира кључ бројем $7 \cdot 26 + 25 = 207$, па израчунава шифрат $207^e \pmod{n} = 207^{33} \pmod{697}$. За то она користи свој рачунар и алгоритам степеновање квадрирањем: $33 = 32 + 1$, $207^2 \equiv 332$, $207^4 \equiv 332^2 \equiv 98$, $207^8 \equiv 98^2 \equiv 543$, $207^{16} \equiv 543^2 \equiv 18$, $207^{32} \equiv 18^2 \equiv 324$. Према томе, $207^{33} \equiv 207^{32}207^1 \equiv 324 \cdot 207 \equiv 156 \pmod{697}$.

Алиса шаље Бобану број 156. Полазећи од броја 156 Цици је теже да израчуна 207.

Бобан добија поруку 156, па израчунава $156^d \pmod{n} = 156^{97} \pmod{697} = 207$. Затим он декодира поруку (то није део алгоритма RSA ) $207 = 7 \cdot 26 + 25$. Затим (то такође није део RSA ) Алиса шаље Бобану дугачку поруку користећи $C \equiv 7P + 25 \pmod{26}$. Крај примера.

Сваки корисник има свој пар бројева: Алиса има пар $n$, $e$. Бобан пар