Криптографија
- четврти део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

24. - 28. фебруар 2025.

Генератор случајног простог броја

- У свим претходним алгоритмима: изабрати кључ = користити генератор случајних бројева

Генератор случајног простог броја

- У свим претходним алгоритмима: изабрати кључ = користити генератор случајних бројева
- Знамо како ради генератор (псеудо)случајних природних бројева

Генератор случајног простог броја

- У свим претходним алгоритмима: изабрати кључ = користити генератор случајних бројева
- Знамо како ради генератор (псеудо)случајних природних бројева
- Али како се генерише случајан прост број?

Генератор случајног простог броја

- У свим претходним алгоритмима: изабрати кључ = користити генератор случајних бројева
- Знамо како ради генератор (псеудо)случајних природних бројева
- Али како се генерише случајан прост број?
- Насумично изабран број вероватно није прост

Генератор случајног простог броја

- У свим претходним алгоритмима: изабрати кључ = користити генератор случајних бројева
- Знамо како ради генератор (псеудо)случајних природних бројева
- Али како се генерише случајан прост број?
- Насумично изабран број вероватно није прост
- Не постоји формула за n-ти прост број $p_n = \ldots$

Генератор случајног простог броја

- У свим претходним алгоритмима: изабрати кључ = користити генератор случајних бројева
- Знамо како ради генератор (псеудо)случајних природних бројева
- Али како се генерише случајан прост број?
- Насумично изабран број вероватно није прост
- Не постоји формула за n-ти прост број $p_n = \ldots$
- $p_n \sim n \log n$, кад $n \to \infty$
  - Зато је неизводљиво: чување простих бројева у листи и бирање насумичног члана листе

Принцип рада генератора:

- Изабере се непаран (велики) псеудослучајан број n
- Затим се прост број тражи у низу n, $n+2$, $n+4$, $n+6$, $\ldots$

Принцип рада генератора:

- Изабере се непаран (велики) псеудослучајан број n
- Затим се прост број тражи у низу n, $n+2$, $n+4$, $n+6$, $\ldots$
- Очекујемо да претх. корак не траје дуго:
  - $p_m \sim n$ тј. $m \sim \frac{n}{\log n}$
  - тада је размак између узастопних простих $p_{m+1} - p_m \sim \log m \sim \log n$

Принцип рада генератора:

- Изабере се непаран (велики) псеудослучајан број n
- Затим се прост број тражи у низу n, $n+2$, $n+4$, $n+6$, $\ldots$
- Очекујемо да претх. корак не траје дуго:
  - $p_m \sim n$ тј. $m \sim \frac{n}{\log n}$
  - тада је размак између узастопних простих $p_{m+1} - p_m \sim \log m \sim \log n$
- Али: треба нам ефикасан начин да проверимо да ли је неки број прост. Елементарно решето је споро - временска сложеност $O(\sqrt{n})$.

Тестови прималности

Направљени тако да

- ако број n падне на тесту онда је n сложен
- ако број n прође тест он може (али не мора) да буде прост

Тестови прималности

Направљени тако да

- ако број n падне на тесту онда је n сложен
- ако број n прође тест он може (али не мора) да буде прост
- $v = \frac{\mathrm{card}\{n \in [1,N] \mid n \text{ је прост}\}}{\mathrm{card}\{n \in [1,N] \mid n \text{ је прошао тест}\}}$ је вероватноћа да је број који прошао тест прост
- веће v - бољи тест.

Тестови прималности

Направљени тако да

- ако број n падне на тесту онда је n сложен
- ако број n прође тест он може (али не мора) да буде прост
- $v = \frac{\text{card}\{n \in [1,N] \mid n \text{ је прост}\}}{\text{card}\{n \in [1,N] \mid n \text{ је прошао тест}\}}$ је вероватноћа да је број који прошао тест прост
- веће v - бољи тест.
- Тест обично зависи од неких параметара. Понављање теста за разне (независне) параметре повећава повећава вероватноћу да је број који је преживео сва тестирања заиста прост

Тестови прималности

Направљени тако да

- ако број n падне на тесту онда је n сложен
- ако број n прође тест он може (али не мора) да буде прост
- $v = \frac{\text{card}\{n \in [1,N] \mid n \text{ је прост}\}}{\text{card}\{n \in [1,N] \mid n \text{ је прошао тест}\}}$ је вероватноћа да је број који прошао тест прост
- веће v - бољи тест.
- Тест обично зависи од неких параметара. Понављање теста за разне (независне) параметре повећава повећава вероватноћу да је број који је преживео сва тестирања заиста прост
- Тест мора да ради брзо

Кармајклови бројеви

- Мала Фермаова теорема: $(\bigstar)$ $a^{n-1} \equiv 1 \pmod{n}$, за n прост и НЗД$(a, n) = 1$

Кармајклови бројеви

- Мала Фермаова теорема: $(\bigstar)$ $a^{n-1} \equiv 1 \pmod{n}$, за n прост и НЗД$(a, n) = 1$
- Али није немогуће да $(\bigstar)$ важи и уколико n није прост

Кармајклови бројеви

- Мала Фермаова теорема: $(\bigstar)$ $a^{n-1} \equiv 1 \pmod{n}$, за n прост и НЗД$(a, n) = 1$
- Али није немогуће да $(\bigstar)$ важи и уколико n није прост

Дефиниција

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

Кармајклови бројеви

- Мала Фермаова теорема: $(\bigstar)$ $a^{n-1} \equiv 1 \pmod{n}$, за n прост и НЗД$(a, n) = 1$
- Али није немогуће да $(\bigstar)$ важи и уколико n није прост

Дефиниција

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

Пример: Број $n = 91 = 7 \cdot 13$ је псеудопрост у бази 3 јер је $3^{90} \equiv 1 \pmod{91}$, али није псеудопрост у бази 2 јер је $2^{90} \equiv 64 \pmod{91}$

Кармајклови бројеви

- Мала Фермаова теорема: $(\bigstar)$ $a^{n-1} \equiv 1 \pmod{n}$, за n прост и НЗД$(a, n) = 1$
- Али није немогуће да $(\bigstar)$ важи и уколико n није прост

Дефиниција

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

Пример: Број $n = 91 = 7 \cdot 13$ је псеудопрост у бази 3 јер је $3^{90} \equiv 1 \pmod{91}$, али није псеудопрост у бази 2 јер је $2^{90} \equiv 64 \pmod{91}$

- Ојлерова теорема: $a^{\varphi(n)} \equiv 1 \pmod{n}$.
  - али $\varphi(n)$ обично не знамо

Кармајклови бројеви

- Мала Фермаова теорема: $(\bigstar)$ $a^{n-1} \equiv 1 \pmod{n}$, за n прост и НЗД$(a, n) = 1$
- Али није немогуће да $(\bigstar)$ важи и уколико n није прост

Дефиниција

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

Пример: Број $n = 91 = 7 \cdot 13$ је псеудопрост у бази 3 јер је $3^{90} \equiv 1 \pmod{91}$, али није псеудопрост у бази 2 јер је $2^{90} \equiv 64 \pmod{91}$

- Ојлерова теорема: $a^{\varphi(n)} \equiv 1 \pmod{n}$.
  - али $\varphi(n)$ обично не знамо
- Ако је n псеудопрост у бази a мора бити $a^{n-\varphi(n)-1} \equiv 1 \pmod{n}$, а $n - \varphi(n) - 1$ је обично много мањи од $n - 1$

Кармајклови бројеви

- Мала Фермаова теорема: $(\bigstar)$ $a^{n-1} \equiv 1 \pmod{n}$, за n прост и НЗД$(a, n) = 1$
- Али није немогуће да $(\bigstar)$ важи и уколико n није прост

Дефиниција

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

Пример: Број $n = 91 = 7 \cdot 13$ је псеудопрост у бази 3 јер је $3^{90} \equiv 1 \pmod{91}$, али није псеудопрост у бази 2 јер је $2^{90} \equiv 64 \pmod{91}$

- Ојлерова теорема: $a^{\varphi(n)} \equiv 1 \pmod{n}$.
  - али $\varphi(n)$ обично не знамо
- Ако је n псеудопрост у бази a мора бити $a^{n-\varphi(n)-1} \equiv 1 \pmod{n}$, а $n - \varphi(n) - 1$ је обично много мањи од $n - 1$
- У нашем примеру $91 - \varphi(91) - 1 = 18$, па базе a у којима је 91 псеудопрост треба тражити међу $a^{18} \equiv 1 \pmod{91}$

Теорема

1. Ако је n псеудопрост и у бази a и у b онда је псеудопрост и у бази ab
2. Ако је n псеудопрост у бази a, али није псеудопрост у b онда није псеудопрост ни у бази ab
3. Ако је n није псеудопрост у бази a онда није псеудопрост ни у бази b, за бар пола b-ова из $\mathbb{Z}_n^* = \{b \in \mathbb{Z}_n \mid \text{НЗД}(b, n) = 1\}$

Теорема

1. Ако је n псеудопрост и у бази a и у b онда је псеудопрост и у бази ab
2. Ако је n псеудопрост у бази a, али није псеудопрост у b онда није псеудопрост ни у бази ab
3. Ако је n није псеудопрост у бази a онда није псеудопрост ни у бази b, за бар пола b-ова из $\mathbb{Z}_n^* = \{b \in \mathbb{Z}_n \mid \text{НЗД}(b, n) = 1\}$

Доказ:

1. $(ab)^{n-1} = a^{n-1}b^{n-1} \equiv 1 \cdot 1 \pmod{n}$
2. $(ab)^{n-1} = a^{n-1}b^{n-1} \equiv b^{n-1} \not\equiv 1 \pmod{n}$
3. За сваки базу c у којој је n псеудопрост постоји база $b = ca$ у којој n није псеудопрост (према 2.)

Дефиниција

Кармајклов број n је сложен број који је псеудопрост у свакој бази $a \in \mathbb{Z}_n^*$

Дефиниција

Кармајклов број n је сложен број који је псеудопрост у свакој бази $a \in \mathbb{Z}_n^*$

- По претх. теореми вероватноћа да број n који није ни прост ни Кармајклов прође тест $(\bigstar)$
  - у једном тестирању са случајно изабраном базом је највише $\frac{1}{2}$

Дефиниција

Кармајклов број n је сложен број који је псеудопрост у свакој бази $a \in \mathbb{Z}_n^*$

- По претх. теореми вероватноћа да број n који није ни прост ни Кармајклов прође тест ($\bigstar$)
  - у једном тестирању са случајно изабраном базом је највише $\frac{1}{2}$
  - у k тестирања са случајно и независно изабраним базама је највише $\frac{1}{2^k}$

Дефиниција

Кармајклов број n је сложен број који је псеудопрост у свакој бази $a \in \mathbb{Z}_n^*$

- По претх. теореми вероватноћа да број n који није ни прост ни Кармајклов прође тест ($\bigstar$)
  - у једном тестирању са случајно изабраном базом је највише $\frac{1}{2}$
  - у k тестирања са случајно и независно изабраним базама је највише $\frac{1}{2^k}$
- Врло ефикасан тест, али не одваја просте од Кармајклових бројева

Дефиниција

Кармајклов број n је сложен број који је псеудопрост у свакој бази $a \in \mathbb{Z}_n^*$

- По претх. теореми вероватноћа да број n који није ни прост ни Кармајклов прође тест ($\bigstar$)
  - у једном тестирању са случајно изабраном базом је највише $\frac{1}{2}$
  - у k тестирања са случајно и независно изабраним базама је највише $\frac{1}{2^k}$
- Врло ефикасан тест, али не одваја просте од Кармајклових бројева
- Користи само степеновање (поновљеним квадрирањем)

Коблиц, глава $V.1$:

- Сваки Кармајклов број је облика $p_1 p_2 \dots p_k$, где је $k \geqslant 3$ и p_i-ови су међусобно различити прости бројеви

Коблиц, глава $V.1$:

- Сваки Кармајклов број је облика $p_1 p_2 \dots p_k$, где је $k \geqslant 3$ и p_i-ови су међусобно различити прости бројеви
- Бесквадратан број n је Кармајклов акко за сваки прост p важи

$$p | n \implies p - 1 | n - 1$$

- Пример:

$$\begin{array}{llll}
1105 = 5 \cdot 13 \cdot 17 & (4 \mid 1104; & 12 \mid 1104; & 16 \mid 1104) \\
1729 = 7 \cdot 13 \cdot 19 & (6 \mid 1728; & 12 \mid 1728; & 18 \mid 1728) \\
2465 = 5 \cdot 17 \cdot 29 & (4 \mid 2464; & 16 \mid 2464; & 28 \mid 2464) \\
2821 = 7 \cdot 13 \cdot 31 & (6 \mid 2820; & 12 \mid 2820; & 30 \mid 2820) \\
6601 = 7 \cdot 23 \cdot 41 & (6 \mid 6600; & 22 \mid 6600; & 40 \mid 6600) \\
8911 = 7 \cdot 19 \cdot 67 & (6 \mid 8910; & 18 \mid 8910; & 66 \mid 8910).
\end{array}$$

Коблиц, глава $V.1$:

- Сваки Кармајклов број је облика $p_1 p_2 \dots p_k$, где је $k \geqslant 3$ и p_i-ови су међусобно различити прости бројеви
- Бесквадратан број n је Кармајклов акко за сваки прост p важи

$$p | n \implies p - 1 | n - 1$$

- Пример:

$$\begin{array}{llll}
1105 = 5 \cdot 13 \cdot 17 & (4 \mid 1104; & 12 \mid 1104; & 16 \mid 1104) \\
1729 = 7 \cdot 13 \cdot 19 & (6 \mid 1728; & 12 \mid 1728; & 18 \mid 1728) \\
2465 = 5 \cdot 17 \cdot 29 & (4 \mid 2464; & 16 \mid 2464; & 28 \mid 2464) \\
2821 = 7 \cdot 13 \cdot 31 & (6 \mid 2820; & 12 \mid 2820; & 30 \mid 2820) \\
6601 = 7 \cdot 23 \cdot 41 & (6 \mid 6600; & 22 \mid 6600; & 40 \mid 6600) \\
8911 = 7 \cdot 19 \cdot 67 & (6 \mid 8910; & 18 \mid 8910; & 66 \mid 8910).
\end{array}$$

- Кармајклови бројеви заиста постоје и морамо да имамо тест који их одваја од простих

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 (тј. a је квадратни остатак) 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 (тј. a је квадратни остатак) 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.

- Од раније: за НЗД$(a, p) = 1$ број решења једначине $x^2 \equiv a \pmod{p}$ је или 0 или 2

- Од раније: за НЗД$(a, p) = 1$ број решења једначине $x^2 \equiv a \pmod{p}$ је или 0 или 2
- $+$ претх. теорема: број решења је $1 + \left(\frac{a}{p}\right)$

- Од раније: за НЗД$(a, p) = 1$ број решења једначине $x^2 \equiv a \pmod{p}$ је или 0 или 2
- $+$ претх. теорема: број решења је $1 + \left(\frac{a}{p}\right)$
- Зато се додефинише $\left(\frac{a}{p}\right) = 0$ кад $p|a$ јер је $a^{\frac{p-1}{2}} \equiv_p 0$ и $x^2 \equiv_p 0$ има тачно једно решење

- Од раније: за НЗД$(a, p) = 1$ број решења једначине $x^2 \equiv a \pmod{p}$ је или 0 или 2
- $+$ претх. теорема: број решења је $1 + \left(\frac{a}{p}\right)$
- Зато се додефинише $\left(\frac{a}{p}\right) = 0$ кад $p|a$ јер је $a^{\frac{p-1}{2}} \equiv_p 0$ и $x^2 \equiv_p 0$ има тачно једно решење

Гаусов закон квадратног реципроцитета

За различите непарне просте p и q важи $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$

- Од раније: за НЗД$(a, p) = 1$ број решења једначине $x^2 \equiv a \pmod{p}$ је или 0 или 2
- $+$ претх. теорема: број решења је $1 + \left(\frac{a}{p}\right)$
- Зато се додефинише $\left(\frac{a}{p}\right) = 0$ кад $p|a$ јер је $a^{\frac{p-1}{2}} \equiv_p 0$ и $x^2 \equiv_p 0$ има тачно једно решење

Гаусов закон квадратног реципроцитета

За различите непарне просте p и q важи $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$

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

Дефиниција

Ако за пародан број a и непаран 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 непаран 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 породан број a и непаран 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 непаран 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 најмање $1 - \frac{1}{2^k}$

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 најмање $1 - \frac{1}{2^k}$
- Како се (брзо) рачуна десна страна $(\bigstar)$?

Имплементација Јакобијевог симбола у python-у:

- улаз: m и n - узајамно прости непарни позитивни
- $\left(\frac{m}{n}\right)$ се рачуна истом стратегијом као $\left(\frac{2013}{2311}\right)$ у примеру

Имплементација Јакобијевог симбола у python-у:

- улаз: m и n - узајамно прости непарни позитивни
- $\left(\frac{m}{n}\right)$ се рачуна истом стратегијом као $\left(\frac{2013}{2311}\right)$ у примеру
- користе се особине ($a, b \in \mathbb{N}$):
  - $\left(\frac{1}{n}\right) = 1$
  - $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
  - $a \equiv b \pmod{n} \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
  - (квадратни реципроцитет) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$
  - $\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{за } n \equiv \pm 1 \pmod{8}, \\ -1, & \text{за } n \equiv \pm 3 \pmod{8}, \end{cases}$

  (ово су Јакобијеви симболи, имају исте особине као Лежандрови)

Имплементација Јакобијевог симбола у python-у:

- улаз: m и n - узајамно прости непарни позитивни
- $\left(\frac{m}{n}\right)$ се рачуна истом стратегијом као $\left(\frac{2013}{2311}\right)$ у примеру
- користе се особине ($a, b \in \mathbb{N}$):
  - $\left(\frac{1}{n}\right) = 1$
  - $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
  - $a \equiv b \pmod{n} \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
  - (квадратни реципроцитет) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$
  - $\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{за } n \equiv \pm 1 \pmod{8}, \\ -1, & \text{за } n \equiv \pm 3 \pmod{8}, \end{cases}$

  (ово су Јакобијеви симболи, имају исте особине као Лежандрови)
- Временска сложеност $O(\log m \log n)$

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.

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

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.

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

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

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.

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

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
- Временска сложеност: a_j-ова има $r < \log_2 n$, и рачунају се поновљеним квадрирањем

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

Доказ: $a^{n-1} \equiv_n a_{r-1}^2 = 1$

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

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

Доказ: $a^{n-1} \equiv_n a_{r-1}^2 = 1$

- 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 $\Longrightarrow$ ПСЕУДОПРОСТ У БАЗИ a

Доказ: $a^{n-1} \equiv_n a_{r-1}^2 = 1$

- 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

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