

КРИПТОГРАФИЈА

- ДЕСЕТИ ДЕО -

ДОЦ. ДР ДРАГАН ЂОКИЋ

Математички факултет, Универзитет у Београду

`dragan.djokic@matf.bg.ac.rs`

10. мај 2024.

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 $p_n = \dots$

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 $p_n = \dots$
- ▶ $p_n \sim n \log n$, кад $n \rightarrow \infty$
 - ▶ 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 $n, n + 2, n + 4, n + 6, \dots$

Принцип рада генератора:

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

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.

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

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: (★) $a^{n-1} \equiv 1 \pmod{n}$, за n прост и $\text{НЗД}(a, n) = 1$

КАРМАЈКЛОВИ БРОЈЕВИ

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

КАРМАЈКЛОВИ БРОЈЕВИ

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

ДЕФИНИЦИЈА

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

КАРМАЈКЛОВИ БРОЈЕВИ

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

ДЕФИНИЦИЈА

Ако за прородан број a и сложен број n тд. $\text{НЗД}(a, n) = 1$ важи (★) 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: (★) $a^{n-1} \equiv 1 \pmod{n}$, за n прост и $\text{НЗД}(a, n) = 1$
- ▶ Али није немогуће да (★) важи и уколико n није прост

ДЕФИНИЦИЈА

Ако за прородан број a и сложен број n тд. $\text{НЗД}(a, n) = 1$ важи (★) 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: (★) $a^{n-1} \equiv 1 \pmod{n}$, за n прост и $\text{НЗД}(a, n) = 1$
- ▶ Али није немогуће да (★) важи и уколико n није прост

ДЕФИНИЦИЈА

Ако за прородан број a и сложен број n тд. $\text{НЗД}(a, n) = 1$ важи (★) 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: (★) $a^{n-1} \equiv 1 \pmod{n}$, за n прост и $\text{НЗД}(a, n) = 1$
- ▶ Али није немогуће да (★) важи и уколико n није прост

ДЕФИНИЦИЈА

Ако за прородан број a и сложен број n тд. $\text{НЗД}(a, n) = 1$ важи (★) 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. теореме вероватноћа да број n који није ни прост ни Кармајклов прође тест (★)
 - ▶ 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. теореме вероватноћа да број n који није ни прост ни Кармајклов прође тест (★)
 - ▶ 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. теореме вероватноћа да број n који није ни прост ни Кармајклов прође тест (★)
 - ▶ 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. теореме вероватноћа да број n који није ни прост ни Кармајклов прође тест (★)
 - ▶ 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 $k \geq 3$ 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 $k \geq 3$ и p_i -ови су међусобно различити прости бројеви
- ▶ Бесквдратан број n је Кармајклов ако за сваки прост p важи

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

- ▶ Пример:

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

Коблиц, глава V.1:

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

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

- ▶ Пример:

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

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

ПОСЛЕДИЦА МАЛЕ ФЕРМАНОВЕ 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:

$a^{p-1} \equiv 1 \pmod{p} \implies p \mid a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right)$,
па p дели бар једну заграду јер p 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:

$a^{p-1} \equiv 1 \pmod{p} \implies p \mid a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right)$,
па p дели бар једну заграду јер p 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:

$a^{p-1} \equiv 1 \pmod{p} \implies p \mid a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right)$,
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:

$$\blacktriangleright \binom{1}{p} = 1$$

(Очигледне) особине:

▶ $\left(\frac{1}{p}\right) = 1$

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

(Очигледне) особине:

▶ $\left(\frac{1}{p}\right) = 1$

▶ $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (баш \equiv , 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) ако је $\left(\frac{a}{p}\right) = 1$.

Доказ: (\implies) ако има решења онда је

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}} \equiv_p (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv_p 1$$

(\impliedby) $a = g^k$, 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 $p-1 \mid \frac{k(p-1)}{2}$, тј. $2 \mid k$ и $x = g^{\frac{k}{2}}$ је решење конгруенције.

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

- ▶ Од раније: за $\text{НЗД}(a, p) = 1$ 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 $\text{НЗД}(a, p) = 1$ 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 $\text{НЗД}(a, p) = 1$ 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 $\text{НЗД}(a, p) = 1$ 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?

$$2013 = 3 \cdot 11 \cdot 61 \quad 2311 - \text{ппрост}$$

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

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

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

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

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

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

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

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

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

Како се уопштава $\binom{\cdot}{n}$ 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

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

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 $\text{НЗД}(a, n) = 1$:
 - ▶ 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

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

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

ДЕФИНИЦИЈА

Ако за природан број a и непаран сложен број n тд.

$\text{НЗД}(a, n) = 1$ важи (★) кажемо да је n Ојлеров псеудопрост број у бази a .

ДЕФИНИЦИЈА

Ако за прородан број a и непаран сложен број n тд.

$\text{НЗД}(a, n) = 1$ важи (★) 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 прородан број a и непаран сложен број n тд.

$\text{НЗД}(a, n) = 1$ важи (★) 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 прородан број a и непаран сложен број n тд.

$\text{НЗД}(a, n) = 1$ важи (★) 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 $a \implies$ ПСЕУДОПРОСТ У БАЗИ a

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

ДЕФИНИЦИЈА

Ако за прородан број a и непаран сложен број n тд.

$\text{НЗД}(a, n) = 1$ важи (★) 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 $a \implies$ 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. $\text{НЗД}(a, n) = 1$. Број n пролази тест у бази a ако је

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

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

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

- ▶ 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. $\text{НЗД}(a, n) = 1$. Број n пролази тест у бази a ако је

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

- ▶ 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 (\star) ?

- ▶ улаз: m и n - узајамно прости непарни позитивни
- ▶ $\binom{m}{n}$ се рачуна истом стратегијом као $\binom{2013}{2311}$ у примеру

- ▶ 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)

- ▶ 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 $O(\log m \log n)$

Подсећање: Код кодирања података помоћу елиптичких кривих:

- ▶ требало је проверити да ли на ЕК $y^2 = x^3 + ax + b$ над пољем \mathbb{Z}_p постоји тачка (x_0, y_0) , где је x_0 задато
- ▶ није било неопходно одредити y_0 , већ само проверити да ли постоји

Подсећање: Код кодирања података помоћу елиптичких кривих:

- ▶ требало је проверити да ли на ЕК $y^2 = x^3 + ax + b$ над пољем \mathbb{Z}_p постоји тачка (x_0, y_0) , где је x_0 задато
- ▶ није било неопходно одредити y_0 , већ само проверити да ли постоји
- ▶ рађено је претраживање табеле (преспоро!), брже је помоћу Лежандрових симбола

Пример: 4-битну поруку $m = 6 = 0110_2$ треба кодирати тачком $P = (x_0, y_0)$ са ЕК $y^2 = x^3 + x + 3$ над пољем \mathbb{Z}_{307}

- ▶ Можемо користити $k = 16$ покушаја јер је $307 > 2^4 \cdot 16$

Пример: 4-битну поруку $m = 6 = 0110_2$ треба кодирати тачком $P = (x_0, y_0)$ са ЕК $y^2 = x^3 + x + 3$ над пољем \mathbb{Z}_{307}

- ▶ Можемо користити $k = 16$ покушаја јер је $307 > 2^4 \cdot 16$
- ▶ Покушамо са $x_0 = mk = 96 = 0110|0000_2$

$$\left(\frac{96^3 + 96 + 3}{307} \right) = \left(\frac{61}{307} \right) = + \left(\frac{307}{61} \right) = \left(\frac{2}{61} \right) = -1$$

Пример: 4-битну поруку $m = 6 = 0110_2$ треба кодирати тачком $P = (x_0, y_0)$ са ЕК $y^2 = x^3 + x + 3$ над пољем \mathbb{Z}_{307}

- ▶ Можемо користити $k = 16$ покушаја јер је $307 > 2^4 \cdot 16$
- ▶ Покушамо са $x_0 = mk = 96 = 0110|0000_2$

$$\left(\frac{96^3 + 96 + 3}{307}\right) = \left(\frac{61}{307}\right) = + \left(\frac{307}{61}\right) = \left(\frac{2}{61}\right) = -1$$

- ▶ Покушамо са $x_0 = mk + 1 = 97 = 0110|0001_2$

$$\begin{aligned} \left(\frac{97^3 + 97 + 3}{307}\right) &= \left(\frac{62}{307}\right) = \left(\frac{31}{307}\right) \underbrace{\left(\frac{2}{307}\right)}_{-1} = + \left(\frac{307}{31}\right) \\ &= \left(\frac{28}{31}\right) = \underbrace{\left(\frac{2}{31}\right)^2}_1 \left(\frac{7}{31}\right) = - \left(\frac{31}{7}\right) \\ &= - \left(\frac{3}{7}\right) = + \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1 \end{aligned}$$

- ▶ Порука се кодира тачком $P = (97, \dots)$

МИЛЕР-РАБИНОВ ТЕСТ ПРИМАЛНОСТИ

► Показали смо

$$a^{p-1} \equiv 1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

МИЛЕР-РАБИНОВ ТЕСТ ПРИМАЛНОСТИ

- ▶ Показали смо
$$a^{p-1} \equiv 1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$
- ▶ 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
$$a^{p-1} \equiv 1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$
- ▶ 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
$$a^{p-1} \equiv 1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$
- ▶ 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 $a^{\frac{p-1}{2}}, a^{\frac{p-1}{2^2}}, a^{\frac{p-1}{2^3}}, \dots$ је конгруентан $\underbrace{1, \dots, 1}_{k \text{ пута}}, -1, \underbrace{\dots}_{\text{било шта}}$, за $k \geq 0$

МИЛЕР-РАВИНОВ ТЕСТ ПРИМАЛНОСТИ

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

$$a_j = a^{2^j d} \pmod{n}, \quad \text{за } j = 0, 1, \dots, r - 1$$

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

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

► Приметимо да је $a_{j+1} \equiv a_j^2 \pmod{p}$ и

1. \implies сви $a_j = 1$
2. $\implies a_j = 1$ за $j > s$

МИЛЕР-РАВИНОВ ТЕСТ ПРИМАЛНОСТИ

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

$$a_j = a^{2^j d} \pmod{n}, \quad \text{за } j = 0, 1, \dots, r - 1$$

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

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

▶ Приметимо да је $a_{j+1} \equiv a_j^2 \pmod{p}$ и

1. \implies сви $a_j = 1$
2. $\implies a_j = 1$ за $j > s$

▶ За сложен n број који пролази Милер-Рабинов тест у бази a кажемо да је јако псеудопрост у бази a

МИЛЕР-РАВИНОВ ТЕСТ ПРИМАЛНОСТИ

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

$$a_j = a^{2^j d} \pmod{n}, \quad \text{за } j = 0, 1, \dots, r - 1$$

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

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

- ▶ Приметимо да је $a_{j+1} \equiv a_j^2 \pmod{p}$ и
 1. \implies сви $a_j = 1$
 2. $\implies a_j = 1$ 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 $a \implies$ ПСЕУДОПРОСТ У
БАЗИ a

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

- ▶ Последица: Ефикасност Милер-Рабиновог теста \geq
ефикасност Кармајкловог теста

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

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

- ▶ Последица: Ефикасност Милер-Рабиновог теста \geq 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. $\text{НЗД}(a, n) = 1$
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: $a^{n-1} \equiv_n a_{r-1}^2 = 1$

- ▶ Последица: Ефикасност Милер-Рабиновог теста \geq 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

$n = 104717$, $n-1 = 2^2 \cdot 26179$.
Choose $a = 96152$.

$$a^{26179} \equiv 1 \pmod{n}$$

*Conclusion: n is **probably prime**.*

$n = 577757$, $n-1 = 2^2 \cdot 144439$.
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**.*

$n = 101089$, $n-1 = 2^5 \cdot 3159$.
Choose $a = 5$.

$$a^{3159} \equiv 101088 \equiv -1 \pmod{n}$$

*Conclusion: n is **probably prime**.*

$n = 280001$, $n-1 = 2^6 \cdot 4375$.
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 .)