Тестови прималности: Фермаов и Милер – Рабинов тест

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Колико су чести прости бројеви?

- Већина криптографских система је везана за коришћење великих простих бројева.
- Колика је вјероватноћа да ће случајно изабранни број бити прост?

Теорема

Нека је са $\pi(X)$ означен број простих бројева који се налазе у интервалу $[2, X]$. Тада вриједи

$$\lim_{X\to\infty} \frac{\pi(X)}{X/\ln(X)} = 1$$

- Колико има простих бројева који се могу представити са 1024 бита?

Како одабрати параметре за RSA

- Да би успоставили RSA систем, потребни су велики прости бројеви.
- Дакле, потребан је ефикасан алгоритам који ће тестирати да ли је одабрани број прост или не.

Коришћење Фермаове теореме

Претпоставимо да Боб тестира прималност броја

$$n = 319879377374793553326200686437131014909523353 01.$$

Најприје трага за малим факторима али схвата да n нема простих фактора мањих од 1000000. Зато изводи следећи тест

$$2^{n-1} \equiv 128126595355135906413360121624715183605316007 4 \pmod{n}$$

Претходна конгруенција му потврђује да n није прост број.

Свједоци и варварски бројеви

Дефиниција

За фиксирани број n кажемо да је број a Фермаов свједок његове сложености уколико је

$$a^n \not\equiv a \pmod{n}$$

- Потребно је за дати број n наћи бар једног његовог свједока чиме се потврђује да није прост.
- Међутим, идилу нарушавају нестишљиви, варварски бројеви попут броја 561. Наиме, овај број $561 = 3 \cdot 11 \cdot 17$ нема свједока. Другим ријечима

$$a^{561} \equiv a \pmod{561} \text{ за сваки цио број } a.$$

Фермаов тест прималности

ferma(n)
Испитује да ли је n прост број користећи Фермаов тест.

- for $i = 1, 2, \ldots, s$
  - Изабери $a \in \{2, 3, \ldots, n-2\}$.
  - Ako je $a^n \not\equiv a \pmod{n}$ врати "n је сложен".
- Врати n **је вјероватно прост.**

- Као што знамо, 561 нема свједока, па би тиме "прошао" претходни тест.

Кармајкл vs. Ферма

- Сложен број n је **Кармајклов** ако за сваки број a такав да **нзд**$(a, n) = 1$ вриједи

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

- Име су добили по Мајклу Кармајклу који их је открио 1910. године.
- Ако је n Кармајклов број, онда нема Фермаових свједока.
- Иако релативно ријетки међу природним бројевима, доказано је да Кармајклових бројева има бесконачно много.
- Стога је Бобу потребан бољи алгоритам од **ferma**(a, n) за тестирање сложености бројева.

Основа за Милер-Рабинов тест

Следећа теорема је теоријски основ за Милер-Рабинов тест прималности.

Теорема

Нека је p непаран прост број такав да

$$p - 1 = 2^k q \text{ гдје је } q \text{ непаран број.}$$

Тада вриједи један од следећа два услова. Нека је a било који број који није дјељив са p. Тада вриједи један од два следећа услова

(а) $a^q \equiv 1 \pmod{p}$.

(б) *Један од $a^q, a^{2q}, \ldots, a^{2^{k-1}q}$ је конгруентан са -1 модуло p.*

Добри свједоци или убједљиви лажови?

Дефиниција

Нека је n непаран прост тако да $n-1=2^k q$ гдје је q непаран број. Цио број који задовољава **нзд**$(a,n)=1$ *се назива Милер-Рабинов свједок (сложености броја n) ако су задовољена оба од следећих услова*

a. $a^q \not\equiv 1 \pmod{n}$.

б. $a^{2^i q} \not\equiv -1 \pmod{n}$ *за све* $i=0,1,2,\ldots,k-1$.

- Слиједи из претходне Теореме да ако постоји неки Милер-Рабинов свједок a за број n, онда је дефинитивно да је n сложен број.

Да ли је a Милер-Рабинов свједок?

wit(a, n)
Испитује да ли је a свједок броја n.

- Ако је n паран или $1 < (a, n) < n$, врати n **је сложен.**
- Представи $n - 1 = 2^k q$ гдје је q непаран.
- Постави $a = a^q \pmod{n}$.
- Ако је $a \equiv 1 \pmod{n}$ врати **није свједок**.
- for $i = 0, 1, \ldots, k - 1$
  - Ако је $a \equiv -1 \pmod{n}$ врати **није свједок**.
  - Постави $a = a^2 \pmod{n}$.
- Врати n **је сложен (a је свједок).**

Како наћи свједока?

- Претпоставимо да Боб жели да провјери да ли је n прост број.
- Бира произвољан a у опсегу $\{2, 3, \ldots, n-2\}$.
- Користи програм $\mathbf{wit}(a, n)$.
- Зашто је ово боље од теста помоћу мале Фермаове теореме?
- Сваки сложен број има пуно Милер-Рабинових свједока.
- Следећа лема прецизније дефинише колико често имамо свједоке за сложен број.

Ефикасност Милер-Рабиновог метода

Лема

Нека је n непаран сложен број. Тада су најмање 75% бројева између 2 и $n-1$ Милер-Рабинови свједоци за број n.

- Рачун ефикасности вјероватносног приступа.
- Претпоставимо да је n сложен и да смо имали 10 Милер-Рабинових тестирања.
- Вјероватноћа да је n сложен а да није нађен ниједан **свједок** у 10 тестирања је

$$0.25^{10} \approx 10^{-6}.$$

- Уколико ово није довољно увјерљиво, може се извршити више тестирања.

Хвала на пажњи :)