Криптографија
- седми део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

12. април 2024.

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 $\varphi(n) = (p-1)(q-1)$

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 $d = e^{-1} \mod \varphi(n)$

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 $d = e^{-1} \bmod \varphi(n)$
- 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

RSA криптосистем (Ривест-Шамир-Еjдлман)

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 $d = e^{-1} \mod \varphi(n)$
- 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 $N = M^e \mod n$ и шаље Бобану

RSA криптосистем (Ривест-Шамир-Ејдлман)

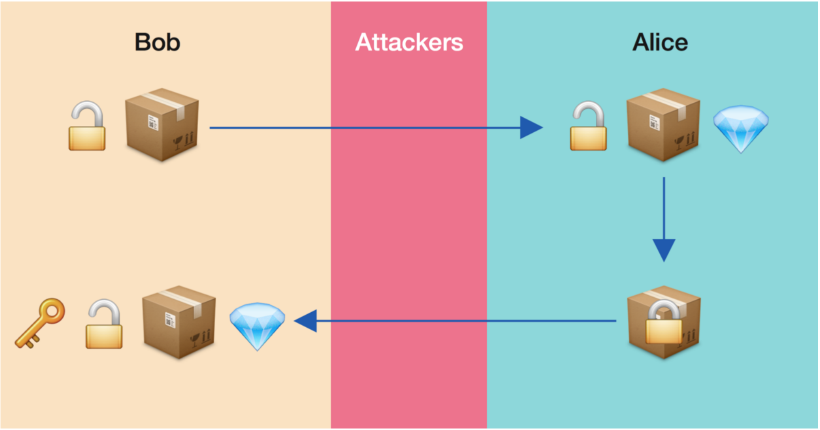
Алиса жели да пошаље поруку или кључ Бобану

- 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 $d = e^{-1} \bmod \varphi(n)$
- 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

RSA криптосистем (Ривест-Шамир-Еjдлман)

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

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.

- $f(M) = M^e \bmod n$ 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 RSA 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 RSA 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 $x^2 - (n - \varphi(n) + 1)x + n$

Дигитални потпис помоћу RSA

Како Алиса може да убеди Бобана у свој идентитет? Тј. како да Бобан буде сигуран да не добија поруке од Цице?

Дигитални потпис помоћу RSA

Како Алиса може да убеди Бобана у свој идентитет? Тј. како да Бобан буде сигуран да не добија поруке од Цице?

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RSA

Дигитални потпис помоћу RSA

Како Алиса може да убеди Бобана у свој идентитет? Тј. како да Бобан буде сигуран да не добија поруке од Цице?

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RSA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$

Дигитални потпис помоћу RSA

Како Алиса може да убеди Бобана у свој идентитет? Тј. како да Бобан буде сигуран да не добија поруке од Цице?

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RSA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$

Дигитални потпис помоћу RSA

Како Алиса може да убеди Бобана у свој идентитет? Тј. како да Бобан буде сигуран да не добија поруке од Цице?

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RSA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$
- Бобан пореди M_2 са оригиналном поруком M

Дигитални потпис помоћу RSA

Како Алиса може да убеди Бобана у свој идентитет? Тј. како да Бобан буде сигуран да не добија поруке од Цице?

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RSA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$
- Бобан пореди M_2 са оригиналном поруком M
- Цица не може (пре Алисе) да одговори Бобану шта је M

Дигитални потпис помоћу RSA

Како Алиса може да убеди Бобана у свој идентитет? Тј. како да Бобан буде сигуран да не добија поруке од Цице?

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RSA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$
- Бобан пореди M_2 са оригиналном поруком M
- Цица не може (пре Алисе) да одговори Бобану шта је M
- Цица ће на крају видети поруку M_2, али не може да је употреби јер Бобан у следећој провери генерише ново M

Дигитални потпис помоћу RSA

Како Алиса може да убеди Бобана у свој идентитет? Тј. како да Бобан буде сигуран да не добија поруке од Цице?

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RSA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$
- Бобан пореди M_2 са оригиналном поруком M
- Цица не може (пре Алисе) да одговори Бобану шта је M
- Цица ће на крају видети поруку M_2, али не може да је употреби јер Бобан у следећој провери генерише ново M

Другачије улоге (у односу на претх.): Алиса $\leftrightarrow$ Бобан

Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у RSA
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у RSA

Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у RSA
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у RSA
- $M < n_A, n_B$ кодирана Алисина порука

Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у RSA
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у RSA
- $M < n_A, n_B$ кодирана Алисина порука
- Алиса рачуна $M_1 = M^{d_A} \bmod n_A$ и $M_2 = M_1^{e_B} \bmod n_B$ и шаље Бобану M_2

Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у RSA
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у RSA
- $M < n_A, n_B$ кодирана Алисина порука
- Алиса рачуна $M_1 = M^{d_A} \bmod n_A$ и $M_2 = M_1^{e_B} \bmod n_B$ и шаље Бобану M_2
- Бобан рачуна $M_3 = M_2^{d_B} \bmod n_B$ и $M_4 = M_3^{e_A} \bmod n_A$, и управо M_4 ће бити Алисина порука

Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у RSA
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у RSA
- $M < n_A, n_B$ кодирана Алисина порука
- Алиса рачуна $M_1 = M^{d_A} \bmod n_A$ и $M_2 = M_1^{e_B} \bmod n_B$ и шаље Бобану M_2
- Бобан рачуна $M_3 = M_2^{d_B} \bmod n_B$ и $M_4 = M_3^{e_A} \bmod n_A$, и управо M_4 ће бити Алисина порука

Битан је редослед операција:

- $M_3 \equiv_{n_B} M_2^{d_B} \equiv_{n_B} M_1^{e_B d_B} \equiv_{n_B} M_1 \implies M_3 = M_1$
- И слично ће бити $M_4 = M$

Криптоанализа RSA

- Одредити тајни кључ $\iff$ наћи инверз за множење $\cdot_{\varphi(n)}$ $\iff$ $\varphi(n) = ?$ $\iff$ раставити n $\iff$ наћи прави делилац од n

Криптоанализа RSA

- Одредити тајни кључ $\iff$ наћи инверз за множење $\cdot_{\varphi(n)}$ $\iff$ $\varphi(n) = ?$ $\iff$ раставити n $\iff$ наћи прави делилац од n
- Елементарно решето (провера да ли $p|n$ за $p \leqslant \sqrt{n}$) је преспоро - време криптовања је $O\left(\log^3 n\right)$

Криптоанализа RSA

- Одредити тајни кључ $\iff$ наћи инверз за множење $\cdot_{\varphi(n)}$ $\iff$ $\varphi(n) = ?$ $\iff$ раставити n $\iff$ наћи прави делилац од n
- Елементарно решето (провера да ли $p|n$ за $p \leqslant \sqrt{n}$) је преспоро - време криптовања је $O\left(\log^3 n\right)$
- Основна претпоставка RSA је да не постоји ефикасан начин да се реши један од претходних проблема (а самим тим и сви)

Криптоанализа RSA

- Одредити тајни кључ $\iff$ наћи инверз за множење $\cdot_{\varphi(n)}$ $\iff$ $\varphi(n) = ?$ $\iff$ раставити n $\iff$ наћи прави делилац од n
- Елементарно решето (провера да ли $p|n$ за $p \leqslant \sqrt{n}$) је преспоро - време криптовања је $O\left(\log^3 n\right)$
- Основна претпоставка RSA је да не постоји ефикасан начин да се реши један од претходних проблема (а самим тим и сви)
- Показаћемо неке алгоритме који раде ефикасно за неке специфичне n, као и неке који за произвољно n могу да смање време израчунавања

Фермаов метод

- Претпоставља да је $n = pq$, где су p и q сличне величине

Фермаов метод

- Претпоставља да је $n = pq$, где су p и q сличне величине
  - Напада случај који делује најоптималније за избор кључа n у RSA - тада би елементарним решетом трагали до $\sqrt{n}$

Фермаов метод

- Претпоставља да је $n = pq$, где су p и q сличне величине
  - Напада случај који делује најоптималније за избор кључа n у RSA - тада би елементарним решетом трагали до $\sqrt{n}$
  - p и q не морају бити прости, али код примене на RSA јесу

Фермаов метод

- Претпоставља да је $n = pq$, где су p и q сличне величине
  - Напада случај који делује најоптималније за избор кључа n у RSA - тада би елементарним решетом трагали до $\sqrt{n}$
  - p и q не морају бити прости, али код примене на RSA јесу
- $n = pq = s^2 - t^2$, где су $s = \frac{p+q}{2}$ и $t = \frac{p-q}{2}$ природни бројеви

Фермаов метод

- Претпоставља да је $n = pq$, где су p и q сличне величине
  - Напада случај који делује најоптималније за избор кључа n у RSA - тада би елементарним решетом трагали до $\sqrt{n}$
  - p и q не морају бити прости, али код примене на RSA јесу
- $n = pq = s^2 - t^2$, где су $s = \frac{p+q}{2}$ и $t = \frac{p-q}{2}$ природни бројеви
- Проблем се своди на налажење s и t, при чему је $s > \sqrt{n}$ и t мало

Фермаов метод

- Претпоставља да је $n = pq$, где су p и q сличне величине
  - Напада случај који делује најоптималније за избор кључа n у RSA - тада би елементарним решетом трагали до $\sqrt{n}$
  - p и q не морају бити прости, али код примене на RSA јесу
- $n = pq = s^2 - t^2$, где су $s = \frac{p+q}{2}$ и $t = \frac{p-q}{2}$ природни бројеви
- Проблем се своди на налажење s и t, при чему је $s > \sqrt{n}$ и t мало
- У низу $s_1 = [\sqrt{n}] + 1$, $s_2 = [\sqrt{n}] + 2$, $\dots$, $s_i = [\sqrt{n}] + i$, $\dots$ тражимо најмањи s_i тд. је $s_i^2 - n$ потпун квадрат тј.
  $t_i = \sqrt{s_i^2 - n}$ цео број
  (где је $[\cdot]$ цео део)

Фермаов метод

- Претпоставља да је $n = pq$, где су p и q сличне величине
  - Напада случај који делује најоптималније за избор кључа n у RSA - тада би елементарним решетом трагали до $\sqrt{n}$
  - p и q не морају бити прости, али код примене на RSA јесу
- $n = pq = s^2 - t^2$, где су $s = \frac{p+q}{2}$ и $t = \frac{p-q}{2}$ природни бројеви
- Проблем се своди на налажење s и t, при чему је $s > \sqrt{n}$ и t мало
- У низу $s_1 = [\sqrt{n}] + 1$, $s_2 = [\sqrt{n}] + 2$, $\ldots$, $s_i = [\sqrt{n}] + i$, $\ldots$ тражимо најмањи s_i тд. је $s_i^2 - n$ потпун квадрат тј.
  $t_i = \sqrt{s_i^2 - n}$ цео број
  (где је $[\cdot]$ цео део)
- Тада је $p = s_i + t_i$ и $q = s_i - t_i$

Пример: раставити 3229799

$$\sqrt{3229799} = 1797,164\ldots$$

$$\sqrt{1798^2 - 3229799} = \sqrt{3232804 - 3229799} = \sqrt{3005} \notin \mathbb{Z}$$

$$\sqrt{1799^2 - 3229799} = \sqrt{3236401 - 3229799} = \sqrt{6602} \notin \mathbb{Z}$$

$$\sqrt{1800^2 - 3229799} = \sqrt{3240000 - 3229799} = \sqrt{10201} = 101$$

$$3229799 = (1800 - 101)(1800 + 101) = 1699 \cdot 1901$$

Пример: раставити 3229799

$$\sqrt{3229799} = 1797,164\ldots$$

$$\sqrt{1798^2 - 3229799} = \sqrt{3232804 - 3229799} = \sqrt{3005} \notin \mathbb{Z}$$

$$\sqrt{1799^2 - 3229799} = \sqrt{3236401 - 3229799} = \sqrt{6602} \notin \mathbb{Z}$$

$$\sqrt{1800^2 - 3229799} = \sqrt{3240000 - 3229799} = \sqrt{10201} = 101$$

$$3229799 = (1800 - 101)(1800 + 101) = 1699 \cdot 1901$$

Пример: раставити 1357

$$\sqrt{1357} = 36,837\ldots$$

$$\sqrt{37^2 - 1357} = \sqrt{12} \notin \mathbb{Z}$$

$$\sqrt{38^2 - 1357} = \sqrt{87} \notin \mathbb{Z}$$

$$\sqrt{39^2 - 1357} = \sqrt{164} \notin \mathbb{Z}$$

$$\sqrt{40^2 - 1357} = \sqrt{243} \notin \mathbb{Z}$$

$$\sqrt{41^2 - 1357} = \sqrt{324} = 18$$

$$1357 = (41 - 18)(41 + 18) = 23 \cdot 59$$

Полардов $(p-1)$-метод

Дефиниција

Нека су $N, B \in \mathbb{N}$. За број $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ кажемо да је B-гладак ако важи $p_i^{\alpha_i} \leqslant B$, за све $1 \leqslant i \leqslant k$

Полардов $(p-1)$-метод

Дефиниција

Нека су $N, B \in \mathbb{N}$. За број $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ кажемо да је B-гладак ако важи $p_i^{\alpha_i} \leqslant B$, за све $1 \leqslant i \leqslant k$

- Пример: $70 = 2 \cdot 5 \cdot 7$ је 7-гладак, али $150 = 2 \cdot 3 \cdot 5^2$ није 7-гладак

Полардов $(p-1)$-метод

Дефиниција

Нека су $N, B \in \mathbb{N}$. За број $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ кажемо да је B-гладак ако важи $p_i^{\alpha_i} \leqslant B$, за све $1 \leqslant i \leqslant k$

- Пример: $70 = 2 \cdot 5 \cdot 7$ је 7-гладак, али $150 = 2 \cdot 3 \cdot 5^2$ није 7-гладак
- Полардов метод омогућава да (брзо) факторишемо природан број n. Претпоставке
  - $B \ll n$ нпр. $B \sim \log n$
  - n има прост чинилац p тд. $p-1$ је B-гладак

(не знамо p, само претпостављамо да постоји)

Полардов $(p-1)$-метод

Дефиниција

Нека су $N, B \in \mathbb{N}$. За број $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ кажемо да је B-гладак ако важи $p_i^{\alpha_i} \leqslant B$, за све $1 \leqslant i \leqslant k$

- Пример: $70 = 2 \cdot 5 \cdot 7$ је 7-гладак, али $150 = 2 \cdot 3 \cdot 5^2$ није 7-гладак
- Полардов метод омогућава да (брзо) факторишемо природан број n. Претпоставке
  - $B \ll n$ нпр. $B \sim \log n$
  - n има прост чинилац p тд. $p-1$ је B-гладак

  (не знамо p, само претпостављамо да постоји)
- Пре примене Полардовог алгоритма треба израчунати $m = \text{НЗС}(1, 2, \dots, B)$

Полардов $(p-1)$-метод

Дефиниција

Нека су $N, B \in \mathbb{N}$. За број $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ кажемо да је B-гладак ако важи $p_i^{\alpha_i} \leqslant B$, за све $1 \leqslant i \leqslant k$

- Пример: $70 = 2 \cdot 5 \cdot 7$ је 7-гладак, али $150 = 2 \cdot 3 \cdot 5^2$ није 7-гладак
- Полардов метод омогућава да (брзо) факторишемо природан број n. Претпоставке
  - $B \ll n$ нпр. $B \sim \log n$
  - n има прост чинилац p тд. $p-1$ је B-гладак

  (не знамо p, само претпостављамо да постоји)
- Пре примене Полардовог алгоритма треба израчунати $m = \text{НЗС}(1, 2, \dots, B)$
  - Уместо m може се користити и B!

Како се рачуна $m = \text{НЗС}(1, 2, \ldots, B)$?

$$m = \prod_{\substack{p \text{ прост} \\ p \leqslant B}} p^{[\log_p B]}$$

У канонској факторизацији m учествују само прости бројеви p који деле неки од $1, 2, \ldots, B$, па је $p \leqslant B$. Ако је $\alpha = \alpha_P$ највећи степен тд. $p^\alpha | m$ онда p^α дели неки од $1, 2, \ldots, B$. Зато је $p^\alpha \leqslant B$ тј. $\alpha \leqslant \log_p B$.

Како се рачуна $m = \text{НЗС}(1, 2, \ldots, B)$?

$$m = \prod_{\substack{p \text{ прост} \\ p \leqslant B}} p^{[\log_p B]}$$

У канонској факторизацији m учествују само прости бројеви p који деле неки од $1, 2, \ldots, B$, па је $p \leqslant B$. Ако је $\alpha = \alpha_P$ највећи степен тд. $p^\alpha | m$ онда p^α дели неки од $1, 2, \ldots, B$. Зато је $p^\alpha \leqslant B$ тј. $\alpha \leqslant \log_p B$.

Овде проналажење простих чинилаца p захтева $O(B)$ операција, остало се брзо извршава

Како се рачуна $m = \text{НЗС}(1, 2, \dots, B)$?

$$m = \prod_{\substack{p \text{ прост} \\ p \leqslant B}} p^{[\log_p B]}$$

У канонској факторизацији m учествују само прости бројеви p који деле неки од $1, 2, \dots, B$, па је $p \leqslant B$. Ако је $\alpha = \alpha_P$ највећи степен тд. $p^\alpha | m$ онда p^α дели неки од $1, 2, \dots, B$. Зато је $p^\alpha \leqslant B$ тј. $\alpha \leqslant \log_p B$.

Овде проналажење простих чинилаца p захтева $O(B)$ операција, остало се брзо извршава

Сви B-глатки бројеви деле m

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m = \text{НЗС}(1,2,\ldots,B)$)

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m =$ НЗС$(1, 2, \dots, B)$)
- $p-1|m$ и МФТ $a^{p-1} \equiv 1 \pmod{p}$ повлаче $a^m \equiv 1 \pmod{p}$

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m = \text{НЗС}(1,2,\ldots,B)$)
- $p-1|m$ и МФТ $a^{p-1} \equiv 1 \pmod{p}$ повлаче $a^m \equiv 1 \pmod{p}$
- $g = \text{НЗД}\,(n, a^m - 1)$ је дељив са p, па g не може бити један

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m =$ НЗС$(1, 2, \ldots, B)$)
- $p-1|m$ и МФТ $a^{p-1} \equiv 1 \pmod p$ повлаче $a^m \equiv 1 \pmod p$
- $g =$ НЗД$\,(n, a^m - 1)$ је дељив са p, па g не може бити један
- Ако $g \neq n$ онда ће g бити прави делилац од n који тражимо.

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m = \text{НЗС}(1, 2, \ldots, B)$)
- $p-1|m$ и МФТ $a^{p-1} \equiv 1 \pmod{p}$ повлаче $a^m \equiv 1 \pmod{p}$
- $g = \text{НЗД}\,(n, a^m - 1)$ је дељив са p, па g не може бити један
- Ако $g \neq n$ онда ће g бити прави делилац од n који тражимо.
- важно: g не зависи од p, зависи само од n и a (које можемо изабрати произвољно)

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m = \text{НЗС}(1, 2, \ldots, B)$)
- $p-1|m$ и МФТ $a^{p-1} \equiv 1 \pmod{p}$ повлаче $a^m \equiv 1 \pmod{p}$
- $g = \text{НЗД}\,(n, a^m - 1)$ је дељив са p, па g не може бити један
- Ако $g \neq n$ онда ће g бити прави делилац од n који тражимо.
- важно: g не зависи од p, зависи само од n и a (које можемо изабрати произвољно)
- Ако је $g = n$ треба пробати са другим a

Полардов алгоритам

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ je B-гладак (па дели $m = \text{НЗС}(1, 2, \ldots, B)$)

Полардов алгоритам

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m = \text{НЗС}(1, 2, \ldots, B)$)
  - Одабрати $2 \leqslant a \leqslant n-1$ тд. $\text{НЗД}(a, n) = 1$ нпр. $a = 2$

Полардов алгоритам

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m = \text{НЗС}(1, 2, \ldots, B)$)
  - Одабрати $2 \leqslant a \leqslant n-1$ тд. $\text{НЗД}(a, n) = 1$ нпр. $a = 2$
  - Израчунати $x = a^m - 1 \bmod n$

Полардов алгоритам

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m = \text{НЗС}(1, 2, \ldots, B)$)
  - Одабрати $2 \leqslant a \leqslant n-1$ тд. НЗД$(a, n) = 1$ нпр. $a = 2$
  - Израчунати $x = a^m - 1 \bmod n$
  - Ако је $x = 0$ променити a (нпр. $a + 1$) и вратити се на први корак

Полардов алгоритам

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m=$ НЗС$(1,2,\ldots,B)$)
  - Одабрати $2 \leqslant a \leqslant n-1$ тд. НЗД$(a,n)=1$ нпр. $a=2$
  - Израчунати $x = a^m - 1 \bmod n$
  - Ако је $x=0$ променити a (нпр. $a+1$) и вратити се на први корак
  - Ако је $x \neq 0$ израчунати $g =$ НЗД (n,x)

Полардов алгоритам

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m =$ НЗС$(1, 2, \ldots, B)$)
  - Одабрати $2 \leqslant a \leqslant n-1$ тд. НЗД$(a, n) = 1$ нпр. $a = 2$
  - Израчунати $x = a^m - 1 \bmod n$
  - Ако је $x = 0$ променити a (нпр. $a+1$) и вратити се на први корак
  - Ако је $x \neq 0$ израчунати $g =$ НЗД(n, x)
- Ако је претпоставка о B-глаткости испуњена, знамо да ће алгоритам дати $g \in \{2, 3, \ldots, n-1\}$, $g|n$

Полардов алгоритам

- Претпоставке: $B \ll n$ и n има прост чинилац p тд. $p-1$ је B-гладак (па дели $m = \text{НЗС}(1,2,\ldots,B)$)
  - Одабрати $2 \leqslant a \leqslant n-1$ тд. $\text{НЗД}(a,n)=1$ нпр. $a=2$
  - Израчунати $x = a^m - 1 \bmod n$
  - Ако је $x=0$ променити a (нпр. $a+1$) и вратити се на први корак
  - Ако је $x \neq 0$ израчунати $g = \text{НЗД}\,(n,x)$
- Ако је претпоставка о B-глаткости испуњена, знамо да ће алгоритам дати $g \in \{2,3,\ldots,n-1\}$, $g|n$
- Уколико се појави $x=1$ то значи да претпоставка о B-глаткости није испуњена. Тада евентуално може да се покуша са већим B

Одредити делилац броја 5197

Нека je $B = 5$ и $m = \text{НЗС}(1, 2, 3, 4, 5) = 60$.

$$2^{60} - 1 \equiv 3416 \pmod{5197} \qquad \text{и} \qquad \text{НЗД}(3416, 5197) = 61$$

па je 61 делилац 5197

Одредити делилац броја 5197

Нека је $B = 5$ и $m = \text{НЗС}(1,2,3,4,5) = 60$.

$$2^{60} - 1 \equiv 3416 \pmod{5197} \qquad \text{и} \qquad \text{НЗД}(3416, 5197) = 61$$

па је 61 делилац 5197

Одредити делилац броја 187

Нека је $B = 15$ и $m = \text{НЗС}(1,2,\ldots,15) = 360360$.

$$2^{360360} - 1 \equiv 0 \pmod{187}$$

$$3^{360360} - 1 \equiv 66 \pmod{187} \qquad \text{и} \qquad \text{НЗД}(66, 187) = 11$$

па је 11 делилац 187

- RSA je рањив ако je $n = pq$ тд. један од $p - 1$ или $q - 1$ je B-гладак

- RSA је рањив ако је $n = pq$ тд. један од $p - 1$ или $q - 1$ је B-гладак
- Можемо да проверимо B-глаткост $p - 1$ за неко фиксирано B (а самим тим и за све $B' \leqslant B$), али и даље постоји опасност од $(B + 1)$-глаткости
  - А не можемо ни тражити најмање B које испуњава претх. услов јер бисмо се опет вратили на факторизацију

- RSA је рањив ако је $n = pq$ тд. један од $p - 1$ или $q - 1$ је B-гладак
- Можемо да проверимо B-глаткост $p - 1$ за неко фиксирано B (а самим тим и за све $B' \leqslant B$), али и даље постоји опасност од $(B + 1)$-глаткости
  - А не можемо ни тражити најмање B које испуњава претх. услов јер бисмо се опет вратили на факторизацију
- Слично, алгоритми засновани на проблему дискретног логаритма могу бити рањиви Полиг-Хелмановим алгоритмом

Полардов метод примењен на $n = 5959$, са $B = 20$

$n = 5959 = 59 \cdot 101$, а ни $58 = 2 \cdot 29$ ни $100 = 2^2 \cdot 5^2$ нису 20-глатки.
Са друге стране, $59 - 2 = 57 = 3 \cdot 19$ јесте 20-гладак

Полардов метод примењен на $n = 5959$, са $B = 20$

$n = 5959 = 59 \cdot 101$, а ни $58 = 2 \cdot 29$ ни $100 = 2^2 \cdot 5^2$ нису 20-глатки.
Са друге стране, $59 - 2 = 57 = 3 \cdot 19$ јесте 20-гладак

- Да ли можемо да радимо нешто слично Полардовом методу са $p - 2$ или генерално са $p + s$, где је $s \ll p$

Полардов метод примењен на $n = 5959$, са $B = 20$

$n = 5959 = 59 \cdot 101$, а ни $58 = 2 \cdot 29$ ни $100 = 2^2 \cdot 5^2$ нису 20-глатки.
Са друге стране, $59 - 2 = 57 = 3 \cdot 19$ јесте 20-гладак

- Да ли можемо да радимо нешто слично Полардовом методу са $p - 2$ или генерално са $p + s$, где је $s \ll p$
- Како се појавило $p - 1$ у нашој причи?

Полардов метод примењен на $n = 5959$, са $B = 20$

$n = 5959 = 59 \cdot 101$, а ни $58 = 2 \cdot 29$ ни $100 = 2^2 \cdot 5^2$ нису 20-глатки.
Са друге стране, $59 - 2 = 57 = 3 \cdot 19$ јесте 20-гладак

- Да ли можемо да радимо нешто слично Полардовом методу са $p - 2$ или генерално са $p + s$, где је $s \ll p$
- Како се појавило $p - 1$ у нашој причи?
- $p - 1$ је кардиналност групе $\left(\mathbb{Z}_p^*, \cdot_p\right)$ и зато се појављује у експоненту у МФТ. Зато је тајни кључ d за RSA прављен по модулу $p - 1$

Полардов метод примењен на $n = 5959$, са $B = 20$

$n = 5959 = 59 \cdot 101$, а ни $58 = 2 \cdot 29$ ни $100 = 2^2 \cdot 5^2$ нису 20-глатки.
Са друге стране, $59 - 2 = 57 = 3 \cdot 19$ јесте 20-гладак

- Да ли можемо да радимо нешто слично Полардовом методу са $p - 2$ или генерално са $p + s$, где је $s \ll p$
- Како се појавило $p - 1$ у нашој причи?
- $p - 1$ је кардиналност групе $(\mathbb{Z}_p^*, \cdot_p)$ и зато се појављује у експоненту у МФТ. Зато је тајни кључ d за RSA прављен по модулу $p - 1$
- Било би добро кад бисмо имали групу кардиналности $p + s$

Полардов метод примењен на $n = 5959$, са $B = 20$

$n = 5959 = 59 \cdot 101$, а ни $58 = 2 \cdot 29$ ни $100 = 2^2 \cdot 5^2$ нису 20-глатки.
Са друге стране, $59 - 2 = 57 = 3 \cdot 19$ јесте 20-гладак

- Да ли можемо да радимо нешто слично Полардовом методу са $p - 2$ или генерално са $p + s$, где је $s \ll p$
- Како се појавило $p - 1$ у нашој причи?
- $p - 1$ је кардиналност групе $\left(\mathbb{Z}_p^*, \cdot_p\right)$ и зато се појављује у експоненту у МФТ. Зато је тајни кључ d за RSA прављен по модулу $p - 1$
- Било би добро кад бисмо имали групу кардиналности $p + s$
- Такве групе ће се појавити на елиптичким кривама

Диксонов метод случајних квадрата

- Користи B-глатке бројеве
  - довољна је и слабија верзија глаткости: N је B-гладак ако $p|N$ прост повлачи $p \leqslant B$

Диксонов метод случајних квадрата

- Користи B-глатке бројеве
  - довољна је и слабија верзија глаткости: N је B-гладак ако $p|N$ прост повлачи $p \leqslant B$
- За изабрану границу глаткости B база чинилаца је $\mathcal{B} = \{p \leqslant B \,|\, p \text{ прост}\} \cup \{-1\}$

Диксонов метод случајних квадрата

- Користи B-глатке бројеве
  - довољна је и слабија верзија глаткости: N је B-гладак ако $p|N$ прост повлачи $p \leqslant B$
- За изабрану границу глаткости B база чинилаца је $\mathcal{B} = \{p \leqslant B \,|\, p \text{ прост}\} \cup \{-1\}$
- Нека је n број који треба раставити

Диксонов метод случајних квадрата

- Користи B-глатке бројеве
  - довољна је и слабија верзија глаткости: N је B-гладак ако $p|N$ прост повлачи $p \leqslant B$
- За изабрану границу глаткости B база чинилаца је $\mathcal{B} = \{p \leqslant B \,|\, p \text{ прост}\} \cup \{-1\}$
- Нека је n број који треба раставити
- 1. корак: проналазе се бројеви x тд. $r_n\left(x^2\right)$ је B-гладак број
  - $r_n(\cdot)$ је ,,означени" остатак по модулу n из интервала $\left(-\frac{n}{2}, \frac{n}{2}\right]$

Диксонов метод случајних квадрата

- Користи B-глатке бројеве
  - довољна је и слабија верзија глаткости: N је B-гладак ако $p|N$ прост повлачи $p \leqslant B$
- За изабрану границу глаткости B база чинилаца је $\mathcal{B} = \{p \leqslant B \,|\, p \text{ прост}\} \cup \{-1\}$
- Нека је n број који треба раставити
- 1. корак: проналазе се бројеви x тд. $r_n\left(x^2\right)$ је B-гладак број
  - $r_n(\cdot)$ је ,,означени" остатак по модулу n из интервала $\left(-\frac{n}{2}, \frac{n}{2}\right]$
  - најлакше их је наћи као $x \approx \sqrt{n}$, а ако их нема довољно може и $x \approx \sqrt{2n}$, $x \approx \sqrt{3n}$, ...

Диксонов метод случајних квадрата

- Користи B-глатке бројеве
  - довољна је и слабија верзија глаткости: N је B-гладак ако $p|N$ прост повлачи $p \leqslant B$
- За изабрану границу глаткости B база чинилаца је $\mathcal{B} = \{p \leqslant B \,|\, p \text{ прост}\} \cup \{-1\}$
- Нека је n број који треба раставити
- 1. корак: проналазе се бројеви x тд. $r_n\left(x^2\right)$ је B-гладак број
  - $r_n(\cdot)$ је ,,означени" остатак по модулу n из интервала $\left(-\frac{n}{2}, \frac{n}{2}\right]$
  - најлакше их је наћи као $x \approx \sqrt{n}$, а ако их нема довољно може и $x \approx \sqrt{2n}$, $x \approx \sqrt{3n}$, ...
  - све $r_n\left(x^2\right)$ смо морали да раставимо на $b_1^{\alpha_1} b_2^{\alpha_2} \dots b_k^{\alpha_k}$ због провере B-глаткости ($b_i \in \mathcal{B}$, $\alpha_i \geqslant 0$, $k = |\mathcal{B}|$) и та растављања се чувају као вектори $v(x) = (\alpha_1, \alpha_2, \dots, \alpha_k)$

- 1. корак се понавља све док не дођемо неколико x-ева тд. је производ њихових означених остатака потпун квадрат (производ бројева из $\mathcal{B}$ са парним експонентима)
  - Ово би требало „брзо“ да се деси ако је кардиналност $\mathcal{B}$ мала

- 1. корак се понавља све док не дођемо неколико x-ева тд. је производ њихових означених остатака потпун квадрат (производ бројева из $\mathcal{B}$ са парним експонентима)
  - Ово би требало „брзо“ да се деси ако је кардиналност $\mathcal{B}$ мала
  - Прецизније: редукција $v(x) \bmod 2$ је вектор из $\mathbb{Z}_2^k$, где има највише k линеарно независних вектора

- 1. корак се понавља све док не дођемо неколико x-ева тд. је производ њихових означених остатака потпун квадрат (производ бројева из $\mathcal{B}$ са парним експонентима)
  - Ово би требало „брзо“ да се деси ако је кардиналност $\mathcal{B}$ мала
  - Прецизније: редукција $v(x) \bmod 2$ је вектор из $\mathbb{Z}_2^k$, где има највише k линеарно независних вектора
- 2. корак: када смо добили $r_n\left(x_1^2\right) r_n\left(x_2^2\right) \dots r_n\left(x_n^2\right) = b_1^{2\beta_1} b_2^{2\beta_2} \dots b_k^{2\beta_k}$

- 1. корак се понавља све док не дођемо неколико x-ева тд. је производ њихових означених остатака потпун квадрат (производ бројева из $\mathcal{B}$ са парним експонентима)
  - Ово би требало „брзо“ да се деси ако је кардиналност $\mathcal{B}$ мала
  - Прецизније: редукција $v(x) \bmod 2$ је вектор из $\mathbb{Z}_2^k$, где има највише k линеарно независних вектора
- 2. корак: када смо добили $r_n\left(x_1^2\right) r_n\left(x_2^2\right) \ldots r_n\left(x_n^2\right) = b_1^{2\beta_1} b_2^{2\beta_2} \ldots b_k^{2\beta_k}$
  - Нека је $x = x_1 x_2 \ldots x_n$ и $y = b_1^{\beta_1} b_2^{\beta_2} \ldots b_k^{\beta_k}$, тада је $x^2 \equiv y^2 \pmod{n}$

- 1. корак се понавља све док не дођемо неколико x-ева тд. је производ њихових означених остатака потпун квадрат (производ бројева из $\mathcal{B}$ са парним експонентима)
  - Ово би требало „брзо“ да се деси ако је кардиналност $\mathcal{B}$ мала
  - Прецизније: редукција $v(x) \bmod 2$ је вектор из $\mathbb{Z}_2^k$, где има највише k линеарно независних вектора
- 2. корак: када смо добили $r_n\left(x_1^2\right) r_n\left(x_2^2\right) \ldots r_n\left(x_n^2\right) = b_1^{2\beta_1} b_2^{2\beta_2} \ldots b_k^{2\beta_k}$
  - Нека је $x = x_1 x_2 \ldots x_n$ и $y = b_1^{\beta_1} b_2^{\beta_2} \ldots b_k^{\beta_k}$, тада је $x^2 \equiv y^2 \pmod{n}$
  - Напомена: последње не повлачи $x \equiv \pm y \pmod{n}$ нпр. $1^2 \equiv 3^2 \pmod{8}$, а $1 \not\equiv \pm 3 \pmod{8}$

- 1. корак се понавља све док не дођемо неколико x-ева тд. је производ њихових означених остатака потпун квадрат (производ бројева из $\mathcal{B}$ са парним експонентима)
  - Ово би требало „брзо“ да се деси ако је кардиналност $\mathcal{B}$ мала
  - Прецизније: редукција $v(x) \bmod 2$ је вектор из $\mathbb{Z}_2^k$, где има највише k линеарно независних вектора
- 2. корак: када смо добили $r_n\left(x_1^2\right) r_n\left(x_2^2\right) \ldots r_n\left(x_n^2\right) = b_1^{2\beta_1} b_2^{2\beta_2} \ldots b_k^{2\beta_k}$
  - Нека је $x = x_1 x_2 \ldots x_n$ и $y = b_1^{\beta_1} b_2^{\beta_2} \ldots b_k^{\beta_k}$, тада је $x^2 \equiv y^2 \pmod{n}$
  - Напомена: последње не повлачи $x \equiv \pm y \pmod{n}$ нпр. $1^2 \equiv 3^2 \pmod{8}$, а $1 \not\equiv \pm 3 \pmod{8}$
  - Проверити да ли је $x \not\equiv \pm y \pmod{n}$
    - Ако јесте: из $n \mid x^2 - y^2 = (x+y)(x-y)$ следи НЗД$(n, x+y)$ је прави делилац n
    - Ако није: потражити друге x, y

- 1. корак се понавља све док не дођемо неколико x-ева тд. је производ њихових означених остатака потпун квадрат (производ бројева из $\mathcal{B}$ са парним експонентима)
  - Ово би требало „брзо“ да се деси ако је кардиналност $\mathcal{B}$ мала
  - Прецизније: редукција $v(x) \bmod 2$ је вектор из $\mathbb{Z}_2^k$, где има највише k линеарно независних вектора
- 2. корак: када смо добили $r_n\left(x_1^2\right) r_n\left(x_2^2\right) \ldots r_n\left(x_n^2\right) = b_1^{2\beta_1} b_2^{2\beta_2} \ldots b_k^{2\beta_k}$
  - Нека је $x = x_1 x_2 \ldots x_n$ и $y = b_1^{\beta_1} b_2^{\beta_2} \ldots b_k^{\beta_k}$, тада је $x^2 \equiv y^2 \pmod{n}$
  - Напомена: последње не повлачи $x \equiv \pm y \pmod{n}$ нпр. $1^2 \equiv 3^2 \pmod{8}$, а $1 \not\equiv \pm 3 \pmod{8}$
  - Проверити да ли је $x \not\equiv \pm y \pmod{n}$
    - Ако јесте: из $n \mid x^2 - y^2 = (x+y)(x-y)$ следи НЗД$(n, x+y)$ је прави делилац n
    - Ако није: потражити друге x, y
  - Временску сложеност није лако објаснити, уз најоптималнији избор параметара је $O\left(e^{2\sqrt{2\log n \log\log n}}\right)$ (што је много мање од $O(\sqrt{n})$), али ради за произвољно n

Пример: Раставити $n = 89893$, користећи границу глаткости $B = 20$

$\sqrt{n} \approx 299.8$

		−1	2	3	5	7	11	13	17	19
$299^2 \equiv -492$	није гладак									
$300^2 \equiv 107$	није гладак									
$298^2 \equiv -1089$	$-1 \cdot 3^2 \cdot 11^2$	1	0	2	0	0	2	0	0	0
$301^2 \equiv 708$	није гладак									
$\sqrt{2n} \approx 424.01$										
$424^2 \equiv -10$	$-1 \cdot 2 \cdot 5$	1	1	0	1	0	0	0	0	0
$425^2 \equiv 839$	није гладак									
$423^2 \equiv -857$	није гладак									
$426^2 \equiv 1690$	$= 2 \cdot 5 \cdot 13^2$	0	1	0	1	0	0	2	0	0

$$298^2 \cdot 424^2 \cdot 426^2 \equiv (-1) \cdot 3^2 \cdot 11^2 \cdot (-1) \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 13^2 \pmod{n}$$
$$(298 \cdot 424 \cdot 426)^2 \equiv ((-1) \cdot 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13)^2 \pmod{n}$$

$298 \cdot 424 \cdot 426 \equiv 69938 \pmod{n}$ и $(-1) \cdot 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \equiv 85603 \pmod{n}$
Примећујемо да је $\mathrm{nzd}(69938 + 85603, n) = 373$ и $n/373 = 241$.