(תרגול הקדמה
תרגיל בית # 14)

אלגוריתם אוקלידס - אלגוריתם אקראי + RSA

Do: Euclidean w/ x,y.

Proof of running time from back.

Finding inverses via euclidean.

$\phi(a,b) = \phi(a)\phi(b)$ when $\gcd(a,b)=1$

Example when it fails

$a,b \in \mathbb{Z},\ a,b \geq 1,\qquad \gcd(a,b) = \min\{d \in \mathbb{Z} : d \geq 1,\ d \mid a,\ d \mid b\}$ הגדרה

```
EUCLID(a,b)
if b=0
    return a
else return EUCLID(b, a mod b)
```

צעד רגיל נניח לגבי $a > b \geq 0$.

- אם $a=b$ אז הגבול אחד EUCLID(b,0) פלט

- אם $a<b$ אז הגבול הראשון EUCLID(b,a) קטן פחות מהראשון.

למה 33.1 אם $a>b\geq 0$ – Euclid(a,b)

אזי $k\geq 1$ הריצה הקרסיבית

אז $a\geq F_{k+2}$, $b\geq F_{k+1}$

מספר פיבונצ'י

$(F_0=0, F_1=1, F_i=F_{i-1}+F_{i-2})$

הוכחה: באינדוקציה על k.

בסיס $k=1$ אז $b>0$ ולכן $b\geq 1=F_2$

– $a>b \Leftarrow a\geq b+1\geq 2=F_3$

ולכן נכון.

הנחה: בריצות הקרסיביות $b>a(\bmod b)$

ולכן בקריאה ל Euclid(a',b') עבור $a'>b'\geq 0$,

הנחת האינדוקציה נכון ל $k-1$ קריאות.

$k>0 \Leftarrow b>0$ ∴

קריאה הקרסיבית כשנכנס ל Euclid(b, a(mod b))

שאז יש $k-1$ קריאות רקורסיביות,

לפי הנחת האינדוקציה $b\geq F_{(k-1)+2}=F_{k+1}$ ✓

$a(\bmod b)\geq F_{(k-1)+1}=F_k$

$$a>b>0 \Rightarrow \lfloor a/b\rfloor\geq 1 \Rightarrow a = a-\lfloor\tfrac{a}{b}\rfloor b+\lfloor\tfrac{a}{b}\rfloor b \geq b+\underbrace{\left(a-\lfloor\tfrac{a}{b}\rfloor b\right)}_{=a(\bmod b)}$$

$$= b+a(\bmod b)\geq F_{k+1}+F_k=F_{k+2}$$

$\square$ $\Rightarrow a\geq F$

משפט: (מקסימום) Lamé 33.11

לכל $k \geq 1$ אם $a > b \geq 0$ ו- $F_{k+1} > b$ אזי EUCLID(a,b) אינו מחזיר יותר מ- k קריאות רקורסיביות.

הערה: $F_k \approx \frac{\phi^k}{\sqrt{5}}$ $\left(\phi = \frac{1+\sqrt{5}}{2}\right)$

מסקנה $\Leftarrow$ מספר הקריאות הרקורסיביות הוא $O(\log b)$.

טענה: יהיו $a, b \geq 1$. אזי לכל $d|a$, $d|b$ והיימים $x, y \in \mathbb{Z}$ כך ש- $d = ax + by$

אם $d = \gcd(a,b)$

הוכחה: $\Delta = \gcd(a,b) \Leftarrow \Delta|a$ ו- $\Delta|b \Leftarrow \Delta|(ax+by) \Leftarrow \Delta|d$

$\therefore \Delta \leq d \Leftarrow \Delta = d$.

(מהגדרת gcd)

טענה: יש מספר x, y כאלו אלגוריתם המוצא את x, y.

```
EXTENDED-EUCLID (a,b)
if b=0
    then return (a,1,0)
(d', x', y') ← EXTENDED-EUCLID (b, a mod b)
(d, x, y) ← (d', y', x' - ⌊a/b⌋ y')
return (d,x,y)
```

[See explanation on next page - do first]

בכר

הלגוריתם איטרטיבי ל Extended GCD

באמצעות הרעיון יצרנו

$$d = a'x' + b'y'$$

ובאן יש לנו בדיוק אותה קלט כ,ב

$$a' = b$$

$$b' = a - \left\lfloor \frac{a}{b} \right\rfloor b$$

ולכן

$$d = a'x' + b'y'$$

$$= bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor b\right) y'$$

$$= a\underset{\parallel}{y'} + b\underbrace{\left(x' - \left\lfloor \frac{a}{b} \right\rfloor y'\right)}_{y''}$$

$$= ax + by$$

בס"ד

שאר ⑤ שאר ⑥

בדוגמא הקודמת ל euclid-ל extended.

gcd(374, 85)

a	b	$\lfloor a/b \rfloor$	r	d	x	y
85	374	0	85	17	9	-2
374	85	4	34	17	-2	9
85	34	2	17	17	1	-2
34	17	2	0	17	0	1
17	0	—	—	17	1	0

$y = x' - \lfloor \frac{a}{b} \rfloor y'$

α $1-(2)(0) = 1$

β $0-(2)(1) = -2$

γ $1-(4)(-2) = 9$

δ $(-2)-(0)(9) = -2$

בדיקה: $ax + by = (374)(-2) + (85)(9)$

$= -748 + 765 = 17 = d$

נמצאת בטבלה בהתאם

(6)

בסך

דוגמה נוספת לחישוב GCD ע"י שלב extended

(נשמרים רק בחישובים אלו)

a	b	$\lfloor \frac{a}{b} \rfloor$	r	d	x	y	
77	65	1	12	1	-27	32	(ε)
65	12	5	5	1	5	-27	(δ)
12	5	2	2	1	-2	5	(γ)
5	2	2	1	1	1	-2	(β)
2	1	2	0	1	0	1	(α)
1	0	—	—	1	1	0	

$x = x' - \lfloor \frac{a}{b} \rfloor y'$

(α) $(1) - (2)(0) = 1$

(β) $(0) - (2)(1) = -2$

(γ) $(1) - (2)(-2) = 5$

(δ) $(-2) - (5)(5) = -27$

(ε) $(5) - (1)(-27) = 32$

בדיקה

$ax + by = (77)(-27) + (65)(32)$

$= -2079 + 2080 = 1 = d.$

(7)

ב כה

נבדוק מקרה m:

טענה: יהי a, m מספרים טבעיים כך ש $\gcd(a,m)=1$.

אז קיים b כך ש $ab \equiv 1 \pmod m$

הוכחה (+ אלגוריתם)

$\exists\, x,y : xa + ym = 1$ (by Euclidean algo)

$1 = xa + ym \equiv xa \pmod m$

לכן $b = x$ אבל!!! ($m+1$ זו יוצא!!!)

דוגמא: $m = 293$ $a = 374$ $\in$ $b = 123$

$a = 293$ $m = 374$ $\in$ $b = -157$

$= 374 - 157 = 217$

OLD

$(217)(293) - 1 = 63580 = (374)(170)$

לנה תיאור $\gcd(77,65)$ עבור **הקיום**

דוגמה $m = 77$, $a = 65$

$(77)(-27) + (65)(32) = 1$

אז $a^{-1} \equiv 32 \pmod{77}$

כי $(65)(32) = 2080 \equiv 1 \pmod{77}$

בכל

דוגמה

$2X = 10 \pmod{100}$

$X \equiv 5$

$X \equiv 55$

$25X \equiv 30 \pmod{100}$

modular-equation-solver

① רוצים לפתור $ax \equiv b \pmod{n}$

② לא תמיד יש פתרון – אף יש – אולי יכול כמה !!! ($\gcd(a,n)$ מעל n)

③ אלגו

```
MLES(a, b, n)
(d, x', y') ← EXTENDED-EUCLID(a, n)
if d | b
    then x_0 ← x'(b/d) (mod n)
        for i ← 0 to d-1
            do print (x_0 + i(n/d)) (mod n)
    else "no solution" print
```

④ דוגמה:

Ex $n = 374$, $a = 85$ (2.11.17) (17.5)

$b = 68$

$x = 36$

$(36)(85) = 8(374) + 68$

$x \quad a \quad n \quad b$

a	b	$\lfloor a/b \rfloor$	r	d	x	y	$= x' - \lfloor a/b \rfloor y'$
374	85	4	34	17	-2	9	$1 - 4(-2) = 9$
85	34	2	17	17	1	-2	$0 - 2(1) = -2$
34	17	2	0	17	0	1	$1 - (2)(0)$
17	0	—	—	17	1	0	

$x_0 \leftarrow \left(\frac{68}{17}\right)$

$\frac{n}{d} = 22$

9 corrected

[illegible]

במקרה שלנו:

$a = 85$ (5.17) $\quad n = 374$ (2.11.17)

$b = 68 =$

$$X_0 = \underset{9}{x'} \left(\frac{b}{d}\right)^{(n,d)} = 9 \cdot 4 = 36$$

($\frac{b}{d} = 17$, $(n,d) = 374$)

בתחילה:

$$\left\{ X_0 + i\left(\frac{n}{d}\right) : i = 0, \dots, d-1 \right\}$$

$n/d = 22$

$$\left\{ 36 + 22i : i = 0, \dots, d-1 \right\}$$

מתי

$$= \{36, 58, \dots, 344, 366, 388\} \quad (n = 374)$$

$366 = -8$, $388 = \underline{14}$

בדיקה:

$$\underset{a}{85}(\underbrace{36 + 22i}_{x}) = 3060 + 1870i$$

$$\equiv 68 + 0i \equiv 68$$

($3060 \equiv 68$, $1870 \equiv 0$, $68 = b$)

$3060 = 8(374) + 68 = 2992 + 68$

$1870 = 5(374)$

לאחר שראינו שאפשר:

לפי מ"ש $x'a + y'n = d$

נכפיל ב $\frac{b}{d}$ שהוא שלם:

$$x'a\left(\frac{b}{d}\right) + y'n\left(\frac{b}{d}\right) = d\cdot\left(\frac{b}{d}\right)$$

$$\|$$

$$\left(x'\frac{b}{d}\right)\cdot a + \underbrace{y'\left(\frac{b}{d}\right)\cdot n}_{\equiv 0 \pmod n} = b$$

ובנוסף

$$a\cdot\frac{n}{d} = \left(\frac{a}{d}\right)\cdot n \equiv 0 \pmod n$$

$(d|a)$

אזהרה:

שים לב: לא לקחתי את האיבר בשני שאתה Extended Euclid

כי זה באופן כללי אין לשים לב בדוגמה.

---

* אין בהכרח שזה $y'\left(\frac{b}{d}\right) = (2)(4) = 8$

הוא כן פעמים ולכן זה יכול גם הכל

בכל

למה: $\gcd(ab, m)=1$ אמ"ט $\gcd(a,m)=1 \wedge \gcd(b,m)=1$

הוכחה: $\Leftarrow$:

$\exists x,y: xab+ym=1$

$\Rightarrow (xa)b+ym=1$

$\& \ 1|b, \ 1|m \Rightarrow \gcd(b,m)=1$

$\Rightarrow (xb)a+ym=1 \Rightarrow \gcd(a,m)=1$

smallest gcd is set $\{ax+by\}$ of all integers

$\exists x,y: xa+ym=1 \Rightarrow xab+ymb=b \Rightarrow$

$\exists \tilde{x},\tilde{y}: \tilde{x}b+\tilde{y}m=1$

$\Rightarrow \tilde{x}(xab+ymb)+\tilde{y}m=1$

$\Rightarrow (\tilde{x}x)ab+(\tilde{x}yb+\tilde{y})m=1$

$\Rightarrow \gcd(ab,m)=1$

$\square$

לעבר: נניח $\gcd(a,b)=1$

$\gcd(\alpha,a)=1$

$\gcd(\beta,b)=1$

אזי בפתרון הייחס (מיגולו ab) γ לשרר

$x\equiv\alpha \pmod a$

$x\equiv\beta \pmod b$

מקיים $\gcd(\gamma,ab)=1$.

הערה: יש y כנ"ל. נמצא לו מאד בעזרת הכלל:

$$\gcd(a,b)=1 \Rightarrow \exists A = b^{-1} \pmod a \quad \Big| \quad A\cdot b \equiv 1 \pmod a$$
$$\exists B = a^{-1} \pmod b \quad \Big| \quad B\cdot a \equiv 1 \pmod b$$

$$y = A\cdot b\cdot \alpha + B a \beta$$

$$\text{mod } a \Rightarrow y \equiv \cancel{A\cdot b}\cdot \alpha + 0 \equiv \alpha$$
$$\text{mod } b \Rightarrow y \equiv 0 + \cancel{B\cdot a}\cdot \beta \equiv \beta$$

הוכחה נוספת:

$$\gcd(y,a) \equiv \gcd(\alpha,a) = 1$$
$$\gcd(y,b) = \gcd(\beta,b) = 1$$
$$\xRightarrow{\text{(לפי קודם)}} \gcd(y, ab) = 1$$

$\square$

מסקנה: יש התאמה חח"ע בין זוגות α,β לבין y - $\gcd(a,b)=1$ כאלו

$$\gcd(a,b)=1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$$

דוגמה נגדית כאשר $\gcd(a,b)>1$

$2\cdot 3$
$2\cdot 5$

$\gcd(a,b)=2 \quad a=6,\ b=10$

$\alpha=5,\ \beta=4$

$\varphi(6)=2 \longrightarrow$ 5 ~~4~~ ~~3~~ ~~2~~ ~~1~~

$\varphi(10)=4 \longrightarrow$ ~~9~~ ~~8~~ ~~7~~ ~~6~~ ~~5~~ ~~4~~ ~~3~~ ~~2~~ ~~1~~

~~$\varphi(1)$~~ 9 8 7 6 5 4 3 2 1