אלגוריתמים 2

11 בנובמבר 2015

סיבוכיות של פעולות אריתמטיות

תזכורת: חיבור וחיסור ניתנים לביצוע בזמן $\mathcal{O}(n)$ כאשר n הוא מספר הביטים (ולא גודל המספר). כפל וחילוק ניתנים לחישוב בזמן $\mathcal{O}(n^2)$

חשבון מודולרי

חיבור: $a+b\,(mod\,m)$ כאשר $a,b\in\mathbb{Z}_m$ ו m באורך $n\geq$ ביטים
$0\leq a+b<2m$ ולכן נקבל זמן ריצה

$$\mathcal{O}(n) \quad \ni \quad \begin{cases} a+b & \Leftarrow a+b<m \\ a+b-m & \Leftarrow a+b\geq m \end{cases}$$

כפל: $ab\,(mod\,m)$ אשר $a,b\in\mathbb{Z}_m$ ו m באורך $n\geq$ ביטים
החישוב דורש פעולת כפל + פעולת חילוק עם שארית ובסה"כ זמן ריצה $\mathcal{O}\left(n^2\right)$

חילוק: למעשה חילוק מעל הממשיים משמעותו הכפלה באיבר ההופכי כלומר $a/b\Rightarrow ab^{-1}$
כאשר $b^{-1}b=1$
ב$\mathbb{Z}_m$ לא תמיד קיים הופכי אבל אם m ראשוני ו$0\neq a\in\mathbb{Z}_m$ אזי קיים $a'\in\mathbb{Z}_m$ כך ש $aa'=1(mod\,m)$
במקרה כזה נאמר ש$\mathbb{Z}_m$ הוא לא רק חוג אלא שדה

האלגוריתם של אוקלידס למציאת GCD

נעבור לדון כעת באלגוריתם $gcd(a,b)$ כאשר במהלך היון בה"כ $a\leq b$

טענה: אם $b=0\,mod\,m$ כלומר $a\mid b$ אזי - $gcd(a,b)=a$
אחרת - $gcd(a,b)=gcd(a,a-b)$

נימוק: $c|a\wedge c|a\Rightarrow c|ab$ ומנגד $c|a\wedge c|b-a\Rightarrow c|a+b-a=b$
נחסר אם כך את aמbשוב ושוב עד שנרד מתחת ל-aונקבל את בצד ימין $b\,mod\,a$

מסקנה: $gcd(a,b)=gcd(a,b-ka)=gcd(a,b\;mod\;a)$ עבור k כלשהו ומכאן נקבל אלגוריתם רקורסיבי:

$GCD-Euclid(a,b)$:

- $c = b \, mod \, a$
- אם $c = 0$ - נחזיר a
- אחרת - נחזיר $GCD - Euclid(c, a)$

זמן ריצה - a, b באורך $n \geq$ ביטים
בהתבוננות ראשונית נוכל לשים לב שבכל צעד אחד המספרים קטן ולכן נוכל להסיק שעומק הרקורסיה $\geq max(a, b) \geq 2^n$

טענה: $b \, mod \, a \leq \frac{b}{a}$

הוכחה: נחלק למקרים -

1. $a \leq \frac{b}{2}$ - $b \, mod \, a < a \leq \frac{b}{a}$
2. $a > \frac{b}{2}$ - נקבל כי $b \, mod \, a = b - a < b - \frac{b}{2} = \frac{b}{2}$

אם כך בכל צעד <u>אחד</u> הפרמטרים קטן לפחות בחצי $\Leftarrow$מספר האיטרציות הוא לכל היותר $2log_2 min(a, b)$ ומאחר ו$a, b \leq 2^n$ נקבל $\mathcal{O}(n)$ איטרציות $\Leftarrow$נבצע $\mathcal{O}(n)$ פעמים חילוק עם שארית ולכן סה"כ זמן ריצה $\mathcal{O}(n^3)$

משפט: אם ראשוני ו $0 \neq a \in \mathbb{Z}_m$ אזי קיים $a' \in \mathbb{Z}_m$ כך ש $aa' = 1 \in \mathbb{Z}_m$

למה: הלמה של בזו $(Bézout)$
לכל $a, b \in \mathbb{N}$ קיים $x, y \in \mathbb{Z}$ כך ש:
$xa + yb = GCD(a, b)$

הוכחת המשפט: יהי $0 \neq a \in \mathbb{Z}_m$ כאשר m ראשוני
$GCD(a, m) = 1 \Rightarrow \exists x, y : \; xa + ym = 1 \Rightarrow xa = 1 + (-y)bm \Rightarrow xa = 1(mod \, m)$

הערה: גם אם mפריק אבל $GCD(a, m) = 1$ קיים הופכי לa ב$\mathbb{Z}_m$

הוכחת הלמה: נשנה מעט את הלגוריתם של אוקלידס כך שיחזיר גם x, yשעבורם $xa + yb = GCD(a, b)$
$GCD - Euclid(a, b)$:
$c = b \, mod \, a$ ונשמור את d שעבורו $b = da + c$
אם $c = 0$: נחזיר את צש וגם $x = 1$ $y = 0$
אחרת: נחזיר את $GCD(c, a)$ וגם את $x = y' - dx$ $y = x'$ אותם קיבלנו מהרקורסיה

הסבר: נניח שהקריאה הרקורסיבית החזירה x, y כך ש $x'c + y'a = GCD(c, a) = GCD(a, b$
בפעולה $b \, mod \, a$ קיבלנו c, d כך ש $b = da + c$
כלומר $x'c + y'a = x'(b - da) + y'a = x'b + (y' - dx')a$ כנדרש

סבוכיות: $\mathcal{O}\left(n^3\right)$

בדיקת ראשוניות