

סיבוכיות

© ארזים

21 במרץ 2017

הגדרה 0.1 יהיו m, n שני מספרים טבעיים. המחלק המשותף המקסימלי של m, n , שמסומן $\gcd(m, n)$, הוא המקסימלי המחלק גם את m וגם את n .

דוגמאות

$$\gcd(18, 12) = 6$$

נניח כי p ראשוני, $a \in (\mathbb{Z}/p\mathbb{Z})^*$, אזי $\gcd(a, p) = 1$.

נראה אלגוריתם יעיל לחישוב \gcd , שנקרא אלגוריתם אוקלידס.

טענה 0.2 יהיו m, n טבעיים, כאשר $n \geq m$. אזי

$$\gcd(n, m) = \gcd(n \bmod m, m)$$

הוכחה: נראה אי שוויונים בשני הכיוונים.

נסמן $d = \gcd(m, n)$, ונרשום

$$n = mx + y$$

כאשר $0 \leq y < m$. אם נראה $d \mid y$, נקבל $d \leq \gcd(n \bmod m, m) = \gcd(y, m)$, כעת,

$$y = n - mx$$

$d \mid m, d \mid n$, ולכן $d \mid y$. לכן קיבלנו אי שוויון אחד. נסמן $d = \gcd(m \bmod n, m)$, ונרשום

$$n = mx + y$$

כאשר $0 \leq y < m$. מההגדרה, $d \mid m, d \mid n \bmod m = y$, כלומר $d \mid n$, ולכן $d \leq \gcd(n, m)$, וסיימנו. ■

נתאר כעת את אלגוריתם אוקלידס (אלגוריתם 1).

Euclid(n, m):
 If $m = 0$, output n
 If $n = 0$, output m
 If $n \geq m$, output Euclid($m, n \bmod m$)
 Else, output Euclid($n, m \bmod n$)

דוגמא קריאה על 18, 12 תקרא לאלגוריתם על 12, 6, שתקרא לאלגוריתם על 6, 0, שתחזיר 6.

טענה 0.3 לכל n, m טבעיים, Euclid(m, n) מוציא את $\gcd(m, n)$.
הוכחה: נוכיח באינדוקציה על מספר האיטרציות i שהאלגוריתם מבצע.
בסיס: $i = 0$ - ברור שמחזירים תשובה נכונה.

צעד: נניח נכונות עבור i איטרציות ונוכיח עבור $i + 1$. נסמן $d = \gcd(m, n)$. אזי בשלב הראשון תתבצע קריאה Euclid($n \bmod m, m$), ואז ייקח עוד i איטרציות. מהנחת האינדוקציה, זה יוציא את

$$\gcd(n \bmod m, m) = d$$

■

טענה 0.4 זמן הריצה של אלגוריתם אוקלידס הוא $O(\log(n + m))$ פעולות אריתמטיות.
הוכחה: נוכיח ששכום המספרים קטן פי פקטור קבוע בכל איטרציה. נניח $n \geq m$ ונכתוב $n = mx + y$, כאשר $0 \leq y < m$. האיטרציה הבאה היא על (m, y) . נוכיח כי

$$\begin{aligned} m + y \leq \frac{2}{3}(m + n) &\iff m + n - mx \leq \frac{2}{3}n + \frac{2}{3}m \iff \\ &\iff \frac{1}{3}n \leq \left(x - \frac{1}{3}\right)m \iff n \leq (3x - 1)m \end{aligned}$$

היות ומתקיים $n \geq m$, מתקיים $x \geq 1$, וכמוכן $y < m$, כלומר $n \leq (x + 1)m$.
 ■ ההוכחה מסתיימת מכך, היות ומתקיים $x + 1 \leq 3x - 1$ לכל $x \geq 1$.

משפט 0.5 יהיו n, m טבעיים, ויהי $d = \gcd(m, n)$. אזי קיימים שלמים a, b המקיימים $an + mb = d$. כמו כן, קיים אלגוריתם שזמן ריצתו $O(\log(n + m))$ פעולות אריתמטיות שבהינתן m, n מוצא a, b כאלה.

הוכחה: באינדוקציה על $m + n$.

```

Extended-Euclid(n, m):
If m = 0 output (n, 1, 0)
If n = 0 output (m, 0, 1)
If n ≥ m
    write n = mx + y where 0 ≤ y < m
    (d, a, b) = Extended-Euclid(m,y)
    output (d, b, a-bx)
Else
    write m = nx + y where 0 ≤ y < m
    (d, a, b) = Extended-Euclid(n,y)
    output (d, a-bx, y)

```

בסיס: אם $m + n = 1$, אזי בלי הגבלת הכלליות $n = 1, m = 0$ ואז

$$1 \cdot n + 0 \cdot m = 1 = \gcd(n, m)$$

צעד: נניח כי הטענה נכונה לכל n, m המקיימים $n + m \leq N$, ונוכיח עבור n, m עבורם $n + m \leq N + 1$. בלי הגבלת הכלליות, $n \geq m$, ונסמן $d = \gcd(m, n)$. נכתוב

$$n = mx + y$$

כאשר $0 \leq y < m$. מהטענה הראשונה שראינו, $\gcd(m, y) = d$. כמו כן, $m + y < 2m \leq m + n \leq N + 1$, כלומר $m + y \leq N$. לכן לפי הנחת האינדוקציה קיימים a, b שלמים המקיימים

$$am + by = d$$

נציב כעת $y = n - mx$ ונקבל

$$d = am + b(n - mx) = (a - bx)m + bn$$

ואלה כמובן שלמים.

■

ההוכחה הזו נותנת אלגוריתם רקורסיבי שמוצא את המקדמים a, b . הנכונות דומה לקודם, ולכן לא נוכיח אותה. נתאר את האלגוריתם כעת (אלגוריתם 2).

משפט 0.6 קיים אלגוריתם שבהינתן p ראשוני, $x \in (\mathbb{Z}/p\mathbb{Z})^*$, מוצא תוך $O(\log(x + p))$ פעולות אריתמטיות את x^{-1} (הופכי מודולו p).

הוכחה: ראשית, $\gcd(x, p) = 1$. לכן, נשתמש באלגוריתם אוקלידס המורחב כדי למצוא a, b שלמים המקיימים

$$ax + bp = 1$$

כעת, מודולו p , מתקיים

$$ax = 1$$

כלומר $a = x^{-1}$.

■