תרגיל מס.9

עפיף חלומה 302323001

5 בינואר 2010

1 שאלה 1

$$\begin{aligned}
P(a+x) &= \sum_{i=1}^{n} p_i (a+x)^i \\
&= \sum_{i=0}^{n} p_i \sum_{j=0}^{i} \frac{i!}{j!(i-j)!} x^j a^{i-j} \\
&= \sum_{i=0}^{n} \sum_{j=0}^{i} p_i \frac{i!}{j!(i-j)!} x^j a^{i-j} \\
&= \sum_{j=0}^{n} \sum_{i=0}^{n} p_i \frac{i!}{j!(i-j)!} x^j a^{i-j} \\
&= \sum_{j=0}^{n} \frac{x^j}{j!} \sum_{i=0}^{n} p_i \frac{i!}{(i-j)!} a^{i-j} \\
&= \sum_{j=0}^{n} \frac{x^j}{j!} \sum_{i=0}^{n} p_i \frac{i!}{(i-j)!} a^{i-j}
\end{aligned}$$

נכדיר סדרות חדשות:

$$\begin{aligned}
b_i &= \frac{x_i}{i!} \\
c_i &= p_i i! \\
d_i &= \frac{a^i}{i!}
\end{aligned}$$

אזי

$$P(x+a) = \sum_{j=0}^{n} b_j \sum_{i=j}^{n} c_i d_{i-j} = \sum_{j=0}^{n} b_j (c*d)_j$$

זאת קונבולוציה, למדנו איך לבצע אותה ב $\mathcal{O}(n \log n)$

2 שאלה 2

2.1 א

אם $a=\prod f_i^{\alpha_i}$ ו $b=\prod f_i^{\beta_i}$ אזי $GCD\left(a,b\right)=\prod f_i^{\min(\alpha_i,\beta_i)}$. נסמן $\frac{a}{2}=\prod f_i^{\gamma_i},\frac{b}{2}=\prod f_i^{\delta_i}$ אזי בהנחה שa,b הם זוגיים(נתון) ו $f_k=2$ מקבלים כי $\gamma_i=\begin{cases}\alpha_i & i\neq k\\ \alpha_i-1 & i=k\end{cases}$, $\delta_i=\begin{cases}\beta_i & i\neq k\\ \beta_i-1 & i=k\end{cases}$ אז מקבלים כי $\min\left(\gamma_i,\delta_i\right)=\begin{cases}\min\left(\alpha_i,\beta_i\right) & i\neq k\\ \min\left(\alpha_i,\beta_i\right)-1 & i=k\end{cases}$. אנחנו יודעים כי $f_k=2$ וההבדל היחיד ביצוג של $GCD\left(\frac{a}{2},\frac{b}{2}\right)$ זה שהוא חסר הכפלה ב2, אזי $GCD\left(a,b\right)=2\cdot GCD\left(\frac{a}{2},\frac{b}{2}\right)$

2.2 ב

אם $a=\prod f_i^{\alpha_i}$ ו $b=\prod f_i^{\beta_i}$ אזי $GCD\left(a,b\right)=\prod f_i^{\min(\alpha_i,\beta_i)}$. אנחנו יודעים כי אם $f_k=2$ אזי $\alpha_k=0$ לכן לא משנה אם מחלקים את b ב 2, המינימום של α_k,β_k תמיד יהיה אפס מכיבן ש $\alpha_k=0$.

2.3 ג

נסמן $g=GCD\left(a,b\right)$ אזי $g|a,g|b$ לכן נובע ש $g|\left(a-b\right)$. מכיוון שa הוא אי זוגי ו b אי זוגי ברור שגם g הוא אי זוגי, אזי $g|\left(\frac{a-b}{2}\right)$

2.4 ד

לחזעיפטם 1 $\mathrm{GCD}\left(a,b\right)$

if($a<b$) swap(a,b)
if($b==0$) return a
if($a==1\vee b==1$) return 1
if($a==b$) return a
if($2|a\wedge 2|b$): return $2\cdot\mathrm{GCD}\left(\frac{a}{2},\frac{b}{2}\right)$
if($2\nmid a\wedge 2|b$) : retrun $\mathrm{GCD}\left(a,\frac{b}{2}\right)$
if($2\nmid a\wedge 2\nmid b$) : return $\mathrm{GCD}\left(\frac{a-b}{2},b\right)$

3 שאלה 3

לחןעיפטם 2 Extended-GCD (a,b)

if$(a<b)$ swap(a,b)
if$(b==0)$ return $(a,0,1)$
if$(a==1 \vee b==1)$ return $(1,0,1)$
if$(a==b)$ return $(a,1,0)$
if$(2|a \wedge 2|b)$:
–$d,x',y' \leftarrow$ Extended-GCD $\left(\frac{a}{2},\frac{a}{2}\right)$
–return $(2d,x',y')$
if$(2\nmid a \wedge 2|b)$:
–$d,x',y' \leftarrow$ Extended-GCD $\left(a,\frac{b}{2}\right)$
–if$(2\nmid y)$:
– – return $\left(d,x+\frac{b}{2},\frac{y-a}{2}\right)$
–else
– – return $\left(d,x,\frac{y}{2}\right)$
–return $\left(d,,\frac{y'}{2}\right)$
if$(2\nmid a \wedge 2\nmid b)$:
–$d,x',y' \leftarrow$ Extended-GCD $\left(\frac{a-b}{2},b\right)$
–return $(d,)$

4 שאלה 4

4.1 א

נוכיח באינדוקציה:

בדיקה עבור $n=0$: אם GCD מסיים בצעד 1 אז $a>f_1, b>f_0,$ כלומר $a>1, b>0$. זה נכון כי אם $b=0$ או $a=1, a=0$ היינו מסיימים ב 0 צעדים.

נניח כי זה מתקיים עבור n ונוכיח עבור $n+1$

$$\begin{aligned} a &> f_{n+2} \\ b &> f_{n+1} \\ a &> f_{n+1}+f_n \\ b &> f_n+f_{n-1} \end{aligned}$$

לפי אלג אוקלידס השלב הבא הוא לחסר:

$$\begin{aligned} a_{new} &= a-b \\ &> f_{n+1}+f_n-f_{n+1} \\ a_{new} &> f_n \end{aligned}$$

מכיוון ש $a_{new} < b$ מחליפים ביניהם ומקבלים GCD המתחיל מ a_{new}, b_{new} שעובדים עבור f_{n+1}, f_n אחרי שעשינו צעד אחד. אזי לפי הנחת האינדוקציה נשארו n צעדים. משל.

4.2 ג

יודעים כי $\lim f_i = \varphi^i$ אזי לפי א. זה מתקיים.

5 שאלה 5

נסמן את החבורה:

$$Z = \{1, a_1, a_2 \dots a_n\}$$

נסתכל על האיבר $a_i \in Z, a_i \neq 1$. נתון כי $\operatorname{ord}(a_i) = 3$ אזי $Z_{a_i} = \{1, a_i, a_i^2\}$ אזי רואים כי $Z = \{1\} \dot\cup \{\dot\cup \{a_i, a_i^2\}\}_{i=1}^{n}$ כלומר $|Z| = 1 + n \cdot 2$ כלומר זה אי זוגי.

6 שאלה 6

6.1 א

$GCD(16, 26) = 1 \Leftrightarrow 15x + 26y = 1$

$$\begin{aligned} GCD(15, 26) &= 1 \\ 15x + 26y &= 1 \\ (15x + 26y) \mod 26 &= 1 \mod 26 \\ 15x \mod 26 &= 1 \mod 26 \end{aligned}$$

6.2 ב

נניח $n \in \mathbb{Z}$

$$\begin{aligned} x \mod 5 &= 3 \\ x &= 3 + 5n \\ x \mod 13 &= 1 \\ x &= 1 + 13n \\ x \mod 9 &= 8 \\ x &= 8 + 9n \end{aligned}$$