

جلسه ششم

قضیه: اگر T یک درخت دودویی پر باشد ، ثابت کنید $n^T \leq 2^{h(T)+1}$

اثبات: با مراجعه به تعریف بازگشتی درخت دودویی پر ، اثبات استقرایی به صورت زیر به دست می آید:

مقدمه استقرا: اگر یک راس تنها باشد داریم:

$$n(T) = 1, h(T) = 0 \rightarrow h(T) = 1 \leq 2^1 - 1 = 2^{h(T)+1}$$

مرحله استقرایی: فرض کنیم حکم مورد نظر برای T_1, T_2 برقرار باشد، درستی آن را برای $T = T_1.T_2$ به صورت زیر نتیجه میگیریم :

$$\begin{aligned} n(T) &= 1 + n(T_1) + n(T_2) \leq 1 + (2^{h(T_1)+1} - 1) + (2^{h(T_2)+1} - 1) \\ &\leq 2 \max(2^{h(T_1)+1}, 2^{h(T_2)+1}) - 1 = 2 \cdot 2^{\max(h(T_1), h(T_2))+1} - 1 \\ &= 2 \cdot 2^{h(T)} - 1 = 2^{h(T)+1} - 1 \rightarrow P(T) \end{aligned}$$

*اصل استقرا معادل خوشترتیبی اعداد صحیح مثبت است که طبق آن هر زیر مجموعه از اعداد صحیح مثبت با ترتیب عادی اعداد دارای کوچکترین عضو (عضو ابتدا) است .

*برای اثبات برخی احکام میتوان مستقیماً از خاصیت خوشترتیبی مجموعه اعداد صحیح مثبت (نامنفی) استفاده کرد.

مثال. ثابت کنید a عددی صحیح و d عددی صحیح و مثبت باشد آنگاه عدد های صحیح و یکتای عدد های صحیح و یکتای r, q موجودند بطوریکه $a = pq + r, 0 \leq r \leq q$

اثبات: فرض کنید $S = \{a - dq \geq 0, q \in \mathbb{Z}\}$ با توجه به اینکه به ازای $q = -|a|$ داریم :

$$a - dq = d|a| + a = |a|(d + \text{sgn}(a)) \geq 0$$

لذا $S \neq \emptyset$

جلسه ششم

طبق خاصیت خوشترتیبی مجموعه اعداد صحیح نامنفی، S دارای کوچکترین عضو است آن را V می نامیم:

از سوی دیگر به برهان خلف، به صورت زیر می توان ثابت کرد
 $r - d \geq 0$ یعنی $r - d \geq 0$ یعنی $r - d = a - dq = a - d(q + 1) \geq 0$
 یعنی $r - d \in S$ و $r - d < r$ و این با عضو ابتدا بودن r در تناقض است.

الگوریتم های بازگشتی:

مثال محاسبه $b^n \bmod m$

Procedure $m \text{ power } (b, n, m: \text{integer with } m \geq 2, n \geq 0)$

1) if $n=0$ then:

2) $m \text{ power } (b, n, m) = 1$

3) else if n is even then:

4) $m \text{ power } (b, n, m) = (m \text{ power } (b, \frac{n}{2}, m))^2 \bmod m$

5) else

6) $m \text{ power } (b, n, m) = ((m \text{ power } (b, \frac{n}{2}, m))^2 \bmod m) \cdot b \bmod m$

ثابت کنید الگوریتم فوق به ازای هر عدد صحیح $n \geq 0$ مقدار $(b^n \bmod m)$ را محاسبه می کند.

اثبات: استقرا نسبت به n به ازای $n=0$ با توجه به اولین if برنامه، خروجی برنامه 1 است و میدانیم

$$1 = b^0 \bmod m$$

مرحله استقرایی: فرض کنید حکم مطلوب به ازای هر عدد صحیح K' که $0 \leq K \leq K'$ برقرار باشد. حال درستی حکم را به ازای K نتیجه میگیریم. این نتیجه گیری در دو حالت بیان می شود:

الف) اگر K زوج باشد؛ $\frac{K}{2}$ عددی صحیح است، در این حالت با توجه به خط 4 برنامه داریم:

$$m \text{ power } (b, k, m) = m \text{ power } (b, \frac{k}{2}, m) = (m \text{ power } (b, \frac{k}{2}, m))^2 \bmod m$$

$$m \text{ power } (b, \frac{k}{2}, m) = (b^{\frac{k}{2}} \bmod m) \text{ داریم}$$

جلسه ششم

در نتیجه:

$$m \text{ power}(b, k, m) = (b^{\frac{k}{2}} \bmod m) = b^k \bmod m$$

ب) حالتی که k به صورت مشابه اثبات قابل تکمیل است.

*اثبات یکی از مثال های جلسات قبل بدون استفاده از قضیه دو جمله ای

$$2 \leq \left(1 + \frac{1}{n}\right)^n < 3$$

n, k اعداد صحیح و مثبت :

$$1 + \frac{k}{n} \leq \left(1 + \frac{1}{n}\right)^n < 3$$

$$1 \leq k \leq n \rightarrow \left(1 + \frac{1}{n}\right)^k < 1 + \frac{k}{n} + \frac{k^2}{n^2}$$

(استقرای کراندار)

$$P(1): \left(1 + \frac{1}{n}\right)^1 < 1 + \frac{1}{n} + \frac{1}{n^2}$$

$$k < n, P(k): \left(1 + \frac{1}{n}\right)^k < 1 + \frac{k}{n} + \frac{k^2}{n^2} \rightarrow \left(1 + \frac{1}{n}\right)^{k+1} < \left(1 + \frac{k}{n} + \frac{k^2}{n^2}\right) \left(1 + \frac{1}{n}\right)$$

$$\begin{aligned} &= 1 + \frac{k}{n} + \frac{k^2}{n^2} + \frac{1}{n} + \frac{k}{n^2} + \frac{k^2}{n^3} = 1 + \frac{k+1}{n} + \frac{k^2 + k + \frac{k^2}{n}}{n^2} \\ &\leq 1 + \frac{k+1}{n} + \frac{(k+1)^2}{n^2} \rightarrow P(k+1) \end{aligned}$$

مثال.

$$m \& n \in \mathbb{Z}, m \& n \geq 0 \rightarrow \exists p \in \mathbb{Z}, p \geq 0 \text{ s.t. } (\sqrt{m} + \sqrt{m+1})^n = \sqrt{p} \cdot \sqrt{p-1}$$

جلسه ششم

برای n زوج:

$$P(n): \exists an, bn \in Z + s.t. (\sqrt{m} \pm \sqrt{m-1})^n \\ = an \pm bn\sqrt{m(m-1)} \& an^2 - bn^2 m(n-1) = 1$$

برای n فرد:

$$Q(n): \exists Cn, dn \in Z + s.t. (\sqrt{m} \pm \sqrt{m-1})^n \\ = cn\sqrt{m} \pm dn\sqrt{m-1} \& cn^2 m - dn^2 (m-1) = 1$$

$$Q(n) \rightarrow P(n+1)$$

$$P(n) \rightarrow Q(n+1)$$

پس $Q(n)$ به ازای n های فرد و $P(n)$ به ازای n های زوج برقرار است. در نتیجه به ازای هر n دلخواه، یکی از $P(n)$ یا $Q(n)$ برقرار خواهد بود. حال اگر n زوج باشد قرار دهید $P = an^2$ و اگر n فرد باشد قرار دهید $P = Cn^2 m$ دیده می شود که:

$$(\sqrt{m} \pm \sqrt{m-1})^n = \sqrt{P} \pm \sqrt{p-1}$$

چند جمله ای های متقارن مقدماتی:

برای $C_{n,k}(x_1, x_2, \dots, x_n)$ داریم:

$$x_n C_{n,k-1}(x_1, \dots, x_n) + C_{n-1,k}(x_1, \dots, x_n), n > 0$$

$$[k = 0], \quad n = 0$$

$$[k \leq 0], \quad n \leq 0$$

	$K=-1$	$K=0$	$K=1$	$K=2$	$K=3$	$K=4$
$n=0$	0	1	0	0	0	0
$n=1$	0	1	X_1	0
$n=2$	0	1	X_2+X_1	0
$n=3$	0	1	$X_3+X_2+X_1$	$X_1X_2+X_2X_3+X_3X_1$