

توان‌های

Expression = a هر عدد را می‌توان به صورت یکی از توان‌های ۲

نویشت (با بهیمنای ۲ بردن) . . . k را با تقسیم‌های متوالی به ۲

در هر مرحله اگر فرد بود که یعنی در بهیمنای ۲ هم آن رقم

۱ است پس در a ذخیره می‌شود و در غیر این صورت

10

k

a ثابت می‌ماند و به توان زوجی برسد

چون $\log k$ بار در مرحله برای شش و نور در مرحله و نیز به همین سادگی است $O(\log k)$

15 Init : قبل از این که مرحله بار اول اجرا شود $a = x^0$ $y = x$

Main : قبل از اجرای مرحله نام اگر k در بهیمنای دو به این صورت

$$m = \log k$$

20 باشد $k = (d_m d_{m-1} \dots d_1)_2$ باشد $a = d_1 \times x^{r^0} \times d_2 \times x^{r^1} \times \dots \times d_{m-1} \times x^{r^{m-2}} \times d_m \times x^{r^{m-1}}$

$$y = x^{r^{i-1}}$$

و پس از اجرای مرحله نام اگر نا فرد باشد پس $a = d_1 \times x^{r^0} \times d_2 \times x^{r^1} \times \dots \times d_{m-1} \times x^{r^{m-2}} \times d_m \times x^{r^{m-1}}$

25 و $d_i = 1$ و $y = x^{r^i}$ و بهیمنای Main برقراره

و اگر $d_i = 0$ و a همان می‌شود چون d_i مضرب فرد
همان a مرحله قبل می‌ماند و $y = x^{r^i}$

Ter : وقتی به شش می‌رسد یعنی مرحله $\log k$ رسید و

$$a = d_1 \times x^{r^0} \times d_2 \times x^{r^1} \times \dots \times d_{m-1} \times x^{r^{m-2}} \times d_m \times x^{r^{m-1}} = k$$