ASSIGNMENT 1.3

```
1 def Pow(x, k) :
2     y ⟵ x, i ⟵ k, a ⟵ 1
3     while i > 0 :
4         if i is odd
5             a ⟵ a × y
6         y ⟵ y × y
7         i ⟵ ⌊i/2⌋
8     return expression
```

۱. به جای عبارت *expression* چه عبارتی باشد تا الگوریتم به درستی کار کند؟ شیوه کارکرد الگوریتم را به طور کامل توضیح دهید. (۴۰ نمره)

پاسخ: الگوریتم توان مورد نظر را به صورت دودویی در نظر گرفته و در هر گام (تکرار حلقه)، x را به نمای یکی از بیت های توان می‌رساند و به مقدار فعلی اضافه می‌کند. مثال زیر نمایشی کلی از کارکرد الگوریتم است:

$$7^{13} = 7^{(1101)_2} = 7^{(0001)_2} \times 7^{(0100)_2} \times 7^{(1000)_2} = 7^1 \times 7^4 \times 7^8$$

بنابراین *expression* باید برابر a باشد.

۲. پیچیدگی زمانی الگوریتم را با تحلیل کد محاسبه کنید. (۲۰ نمره)

پاسخ: پیچیدگی زمانی الگوریتم به حلقه‌ی موجود در خط‌های 3–7 وابسته است. در هر تکرار حلقه i بر 2 تقسیم می‌شود و تا زمانی که i مثبت باشد ادامه دارد. بنابراین پیچیدگی زمانی برابر $O(log\, k)$ است زیرا مقدار اولیه i برابر k است.

۳. درستی الگوریتم را به کمک Loop invariant اثبات کنید. (۴۰ نمره)

پاسخ: با توجه به توضیحات بخش اول:

Loop Invariant:

به منظور ساده سازی اثبات، متغیر فرضی j را در نظر بگیرید که در ابتدای کار مقدار آن صفر بوده و در ابتدای هر تکرار حلقه به مقدار آن یکی اضافه می‌شود. در این صورت، فرض ناوردا در ابتدای تکرار jــام به صورت زیر است:

$$a = x^{k \,\%\, 2^j}$$

$$y = x^{2^j}$$

$$i = [\frac{k}{2^j}]$$

نماد $a \,\%\, b$ نشان‌دهنده باقی‌مانده تقسیم a بر b است. عبارت $k \,\%\, 2^j$ به بیانی دیگر به معنی j **بیت اول عدد** k است.

Initialization:

در ابتدا j برابر صفر است پس خواهیم داشت:

$$a = x^{k \,\%\, 2^0} = x^0 = 1$$
$$y = x^{2^0} = 1$$
$$i = [\frac{k}{2^0}] = k$$

Maintenance:

فرض کنید که حلقه در شروع تکرار jــام باشد و فرض ناوردا برای $j - 1$ برقرار باشد. در خط ۴ام زوجیت i بررسی می‌شود. زوجیت به این خاطر بررسی می‌شود که تشخیص دهیم که بیت اول i، صفر است یا یک (زیرا زوجیت تنها به بیت اول وابسته است). به این نکته توجه کنید که **بیت اول** i**، در واقع بیت** j**ــام** k **است**. چرا؟ دقت کنید که i برابر با $[\frac{k}{2^j}]$ است. این یعنی عدد i از حذف j بیت اول k بدست آمده است. در ابتدای حلقه jــام داریم $i = [\frac{k}{2^{j-1}}]$.
بنابراین بیت اول i، بیت jــام k است. اگر i زوج باشد، بیت اول آن صفر است در نتیجه تاثیری در جواب در ندارد.
اگر فرد باشد: مقدار مورد نظر به a اضافه خواهد شد (به کمک ضرب؛ به مثال بخش اول توجه کنید).

$$a_j = x^{k \,\%\, 2^j} = x^{k \,\%\, 2^{j-1}} = a_{j-1} \qquad i \text{ is even}$$
$$a_j = a_{j-1} \times y_{j-1} = x^{k \,\%\, 2^{j-1}} \times x^{2^{j-1}} = x^{k \,\%\, 2^j} \qquad o.w$$

$$y_j = y_{j-1} \times y_{j-1} = \left(x^{2^{j-1}}\right)^2 = x^{2^j}$$

$$i_j = \lfloor \frac{i_{j-1}}{2} \rfloor = \lfloor \frac{\lfloor \frac{k}{2^{j-1}} \rfloor}{2} \rfloor = \lfloor \frac{k}{2^j} \rfloor$$

Termination:

پس از پایان حلقه، j برابر با تعداد بیت های k خواهد بود (چرا؟). در نتیجه خواهیم داشت $k < 2^j$ (چرا؟). پس:

$$k \,\%\, 2^j = k \implies a_j = x^k$$