Szybkie potęgowanie

W naiwnym potęgowaniu by obliczyć wartość x^b musieliśmy wykonać b mnożeń. Jednak liczbę tą można zredukować do O(log b)

Przykład:
$x^5 = x^4 * x$
$x^{11} = x^8 * x^2 * x$

Pytanie: co decyduje o tym, które z czynników znajdują się w mnożeniu (dla danego wykładnika), a innych nie ma?
Odpowiedź: Rozwinięcie binarne wykładnika!

Zauważmy, że na przykład:

$5=(101)_2$
$x^5 = x^4 * x$ (nie ma x^2,bo na drugim od prawej bicie jest 0)

$11=(1011)_2$
$x^{11} = x^8 * x^2 * x$ (nie ma x^4,bo na trzecim od prawej bicie jest 0)

Zatem aby szybko podnieść liczbę x do potęgi o wykładniku naturalnym możemy postępować według poniższego schematu:
Zmienna w będzie przechowywała aktualny wynik. Na początek w=1.
Czynnik, który w mnożeniu się pojawi lub nie oznaczony zostaje przez c. Na początek c=x.
Zamieniamy wykładnik na system binarny i rozpatrujemy powstające bity w kolejności od najmniej znaczącego:

- **Jeśli jest jeden to w=w*c, $c=c^2$**
- **Jeśli jest zero to jedynie $c=c^2$**

Zauważmy, że przy zamianie wykładnika na system binarny nie musimy przechowywać w pamięci wszystkich bitów. Potrzebujemy tylko jeden bit w danym obiegu pętli, w kolejności takiej w jakiej powstają, czyli od najmniej znaczącego. Stąd nazwa algorytmu „od prawej do lewej".

Wskazówki (wykorzystanie operatorów bitowych):

- **If (b&1) jest równoważne zapisowi if(b%2==1) ale jest bardziej efektywne**
- **b>>=1 jest równoważne zapisowi: b=b/2 ale jest bardziej efektywne**