Algorytm szybkiego potęgowania

$1 // 2 = 0$

IN: $x \in \mathbb{R}$, $n \in \mathbb{N}_0$

OUT: x^n

```
y ← x
m ← n
z ← 1
while m > 0
    if m jest nieparzyste
        z ← z·y
    y ← y·y
    m ← m // 2
return z
```

S

$$3^{21} = 3^{(10101)_2} = 3^{16}\cdot 3^{4}\cdot 3^{1}$$

$$3^1 \to 3^2 \to 3^4 \to 3^8 \to 3^{16}$$

1 0 1 0 1

1) Czy pętla się kończy?

$m_{nowe} = m//2$ $\quad \lfloor m/2 \rfloor \in \mathbb{N}_0$

$m_{nowe} < m \Rightarrow$ po skończonej liczbie kroków $m = 0$

2) NIEZMIENNIK

$\boxed{P:\ z\cdot y^m = x^n}$ i $m \geq 0$

(I) Czy P jest prawdziwe przed wejściem do pętli?

TAK: $z\cdot y^m = 1\cdot x^n = x^n$ ✓

(II) (Z) $z\cdot y^m = x^n$

(T) $z_{nowe}\cdot y_{nowe}^{m_{nowe}} = x^n$

a) m jest parzyste

$z_{nowe} = z$

$y_{nowe} = y^2$

$m_{nowe} = \frac{m}{2}$

$$z_{nowe}\cdot y_{nowe}^{m_{nowe}} = z\cdot (y^2)^{m/2} = z\cdot y^m \overset{(Z)}{=} x^n$$

b) m jest nieparzyste

$z_{nowe} = z\cdot y$ $\quad y_{nowe} = y^2$

$m_{nowe} = \frac{m-1}{2}$

$$z_{nowe}\cdot y_{nowe}^{m_{nowe}} = (z\cdot y)\cdot(y^2)^{\frac{m-1}{2}} = z\cdot y\cdot y^{m-1} = z\cdot y^m \overset{(Z)}{=} x^n.$$

Tw. o niezmiennikach: po zakończeniu programu mamy:

$$\underbrace{m \leq 0}_{} \quad i \quad z \cdot y^m = x^n.$$

$$m = 0 \quad i \quad z \cdot y^m = x^n$$

$$z \cdot y^0 = x^n$$

$$\boxed{z = x^n}$$

---

1) $0^0 \to \underline{1}$

$\uparrow$ niezdefiniowane

$\lim_{x \to 0} x^x = \underline{1}$. $\quad 0^0 = \underline{1}$

---

2) – $x^n = \underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{n} = x^n$

$n - 1$.

$x^{2^{1000}}$, 2^{1000}.

0

$\#$

– ASP $\quad n = (b_k b_{k-1} \ldots b_1 b_0)_2$

$k+1$ bitów $\to$ $k+1$ obrotów pętli

$$\downarrow$$

$$2^k \leq n \leq 2^k + 2^{k-1} + \ldots + 2^1 + 2^0 =$$

$$= 1 \cdot \frac{1 - 2^{k+1}}{1 - 2} = 2^{k+1} - 1$$

$$2^k \leq n \leq 2^{k+1} - 1 < 2^{k+1} \quad | \log_2()$$

$$k = \log_2(2^k) \leq \log_2 n < \log_2(2^{k+1}) = k+1$$

$$k \leq \log_2 n$$

$$\boxed{k+1 \leq \log_2 n + 1}$$

liaba obvotso

$2(\log_2 n + 1)$ – ogvaniuenie liaby

$x^{2^{1000}}$

$$2(\log_2(2^{1000}) + 1) = 2(1000 + 1) =$$

$$= 2002$$

Kryptografie

x^{5} ← wielkie

LOGIKA MATEMATYCZNA

Jeśli liczba n jest liczbą pierwszą, to $n = 2$ lub n jest liczbą nieparzystą.

spójniki

$p, q, r, \ldots$ – zdania

$\wedge$	i	koniunkcja
$\vee$	lub	alternatywa
$\Rightarrow$	jeśli ..., to ...	implikacja
$\Leftrightarrow$	wtedy i tylko wtedy, gdy	równoważność
$\neg$	nieprawda, że	negacja $(\sim)$

$\boxed{1/0}$ – symbole „prawdy" i „fałszu" T/F jaki funktor

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \circ q$	
1	1	1	1	1	1	1/0	?
1	0	0	1	0	0	1/0	?
0	1	0	1	1	0	1/0	?
0	0	0	0	1	1	1/0	?

Jeśli $1=0$ to $3=8$

0 $\qquad$ 0

$p \Rightarrow (q \vee r) \qquad (p \Rightarrow q) \vee r$

---

p	$\neg p$	op	
1	0	1/0	2
0	1	1/0	2
			4

		XOR	NAND	NOR
p	q	$p \oplus q$	$p \mid q$	$p \downarrow q$
1	1	0	0	0
1	0	1	1	0
0	1	1	1	0
0	0	0	1	1
		alternatywa wykluczająca	kreska Sheffera	strzałka Pierce'a