KRAKOWSKIE MŁODZIEŻOWE TOWARZYSTWO PRZYJACIÓŁ NAUK I SZTUK
KONKURS PRAC MATEMATYCZNYCH
Kraków, 11 kwietnia 2013 r.

LICZBY PIERWSZE

Jan Ciurej i Radosław Żak

Katolicka Szkoła Podstawowa im. Świętej Rodziny z Nazaretu w Krakowie

Co to jest liczba pierwsza?

Liczba pierwsza

to liczba naturalna, która ma dokładnie dwa dzielniki - 1 i samą siebie.

Liczby naturalne, a liczby pierwsze

Liczby naturalne większe od 1, które nie są liczbami pierwszymi, można przedstawić w postaci iloczynu liczb pierwszych, np.:

$$130 = 2 \cdot 5 \cdot 13$$

$$231 = 3 \cdot 7 \cdot 11$$

$$11042013 = 3 \cdot 43 \cdot 85597$$

W IV w. p. n. e. Euklides zastanawiał się, ile jest liczb pierwszych

Jest nieskończenie wiele liczb pierwszych

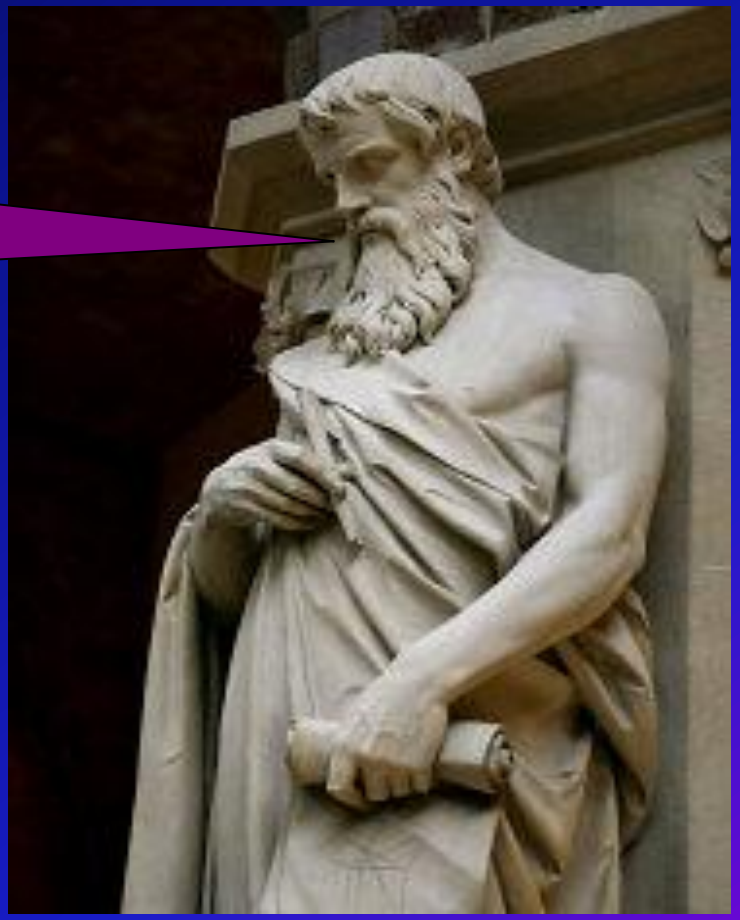


Figura Euklidesa na dziedzińcu Muzeum Historii Naturalnej w Oxfordzie
źródło: http://www.matematyka.wroc.pl/matematykawsztuce/matematycy-na-cokoly

Jak dowodził Euklides?

Ilość kolejnych liczb pierwszych	Wynik	Liczba pierwsza lub iloczyn liczb pierwszych
1	$2 + 1 = 3$	3
2	$2 \cdot 3 + 1 = 7$	7
3	$2 \cdot 3 \cdot 5 + 1 = 31$	31
4	$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$	211
5	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$	2311
6	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$	$59 \cdot 509$

Poszukiwania liczb pierwszych

- Euler $Lp = n^2 + n + 41$
  $n = 40 \quad \rightarrow \quad 1681 = 41^2$

- Legendre $Lp = 2n^2 + 29$
  $n = 29 \quad \rightarrow \quad 1711 = 29 \cdot 59$

- Esscot $Lp = n^2 - 79n + 1601$
  $n = 80 \quad \rightarrow \quad 1681 = 41^2$

Największa znana liczba pierwsza

$$2^{57885161}-1$$

ma 17 425 170 cyfr

Zastosowania liczb pierwszych

- w teorii – podstawowe pojęcie w matematyce
- w praktyce – szyfrowanie (kryptografia)

Arytmetyka modularna

- stosowana powszechnie w obliczeniach zegarowych
- np. jeśli jest godzina 10.00 to za 17 godzin nie będzie 27.00, tylko 3.00, ponieważ: (10 + 17) : 24 = 1 reszty 3

Kod RSA

- Oparty na liczbach pierwszych
- Moduł (N) jest iloczynem dwóch liczb pierwszych (p i q), kod szyfrujący to inna liczba (E)
- Karta kredytowa biorąca udział w transakcji to liczba C

Szyfrowanie kodem RSA

- Zaszyfrowana wiadomość: $C^E \pmod N = F$
- np. dla liczb:

$$p = 17,\ q = 11,\ N = 17 \cdot 11 = 187,$$
$$E = 9,\ C = 7$$

$$F = 7^9 \pmod{187} = 129$$

Złamanie kodu

- Aby złamać kod trzeba poznać liczbę D, która spełnia warunek:

$$D \cdot E \pmod{(p-1)(q-1)} = 1$$

- Stąd można wyliczyć: $C = F^D \pmod{N}$

Program w języku PYTHON

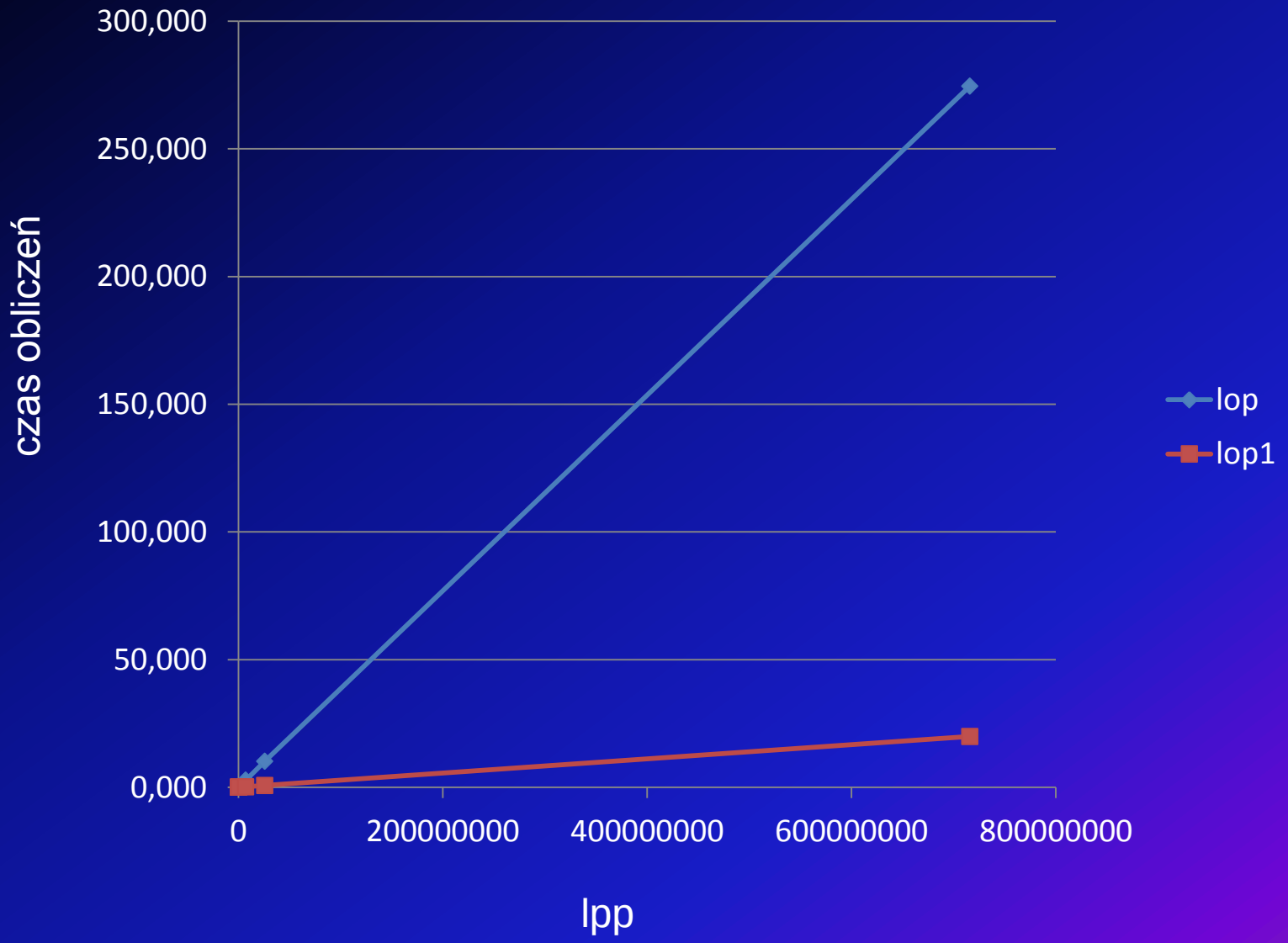
```
import time
def lop(lpp):
    t=time.time()
    if lpp==0 or lpp==1:
        return False
    for i in range(lpp):
        if i==0 or i==1:
            continue
        elif lpp%i==0:
            return False
    print(time.time()-t)
    return True
```

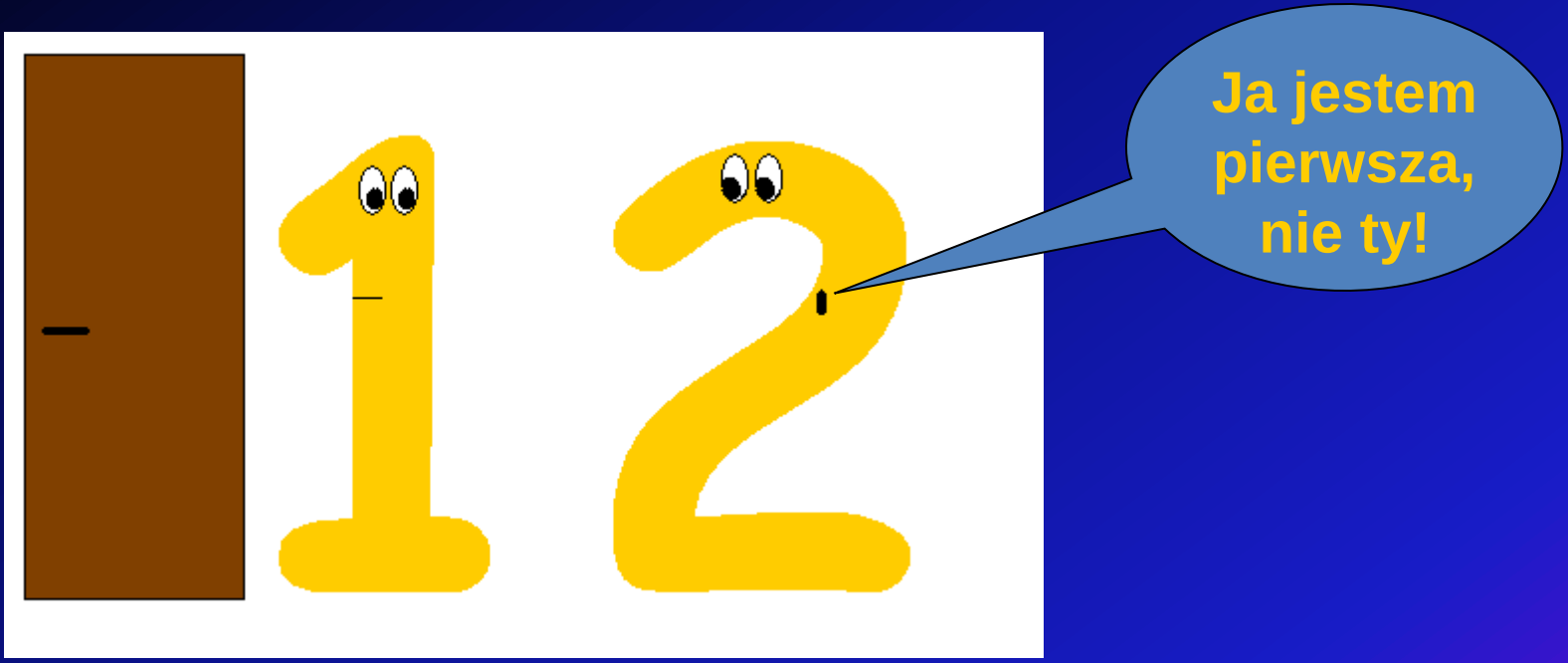
```
def lop1(lpp):
    t=time.time()
    for i in [2,3,5]:
      if lpp%i==0:
        return False
    for i in range(7,round(lpp/5),2):
      if lpp%i==0:
        return False
    print(time.time()-t)
    return True
```

Porównanie czasów obliczeń

Liczba pierwsza	Czas [s]		lop/lop1
	lop	lop1	
2351	0.001	0.000	-
43691	0.015	0.001	15.0010
436913	0.165	0.012	13.7499
7158271	2.751	0.197	13.9645
25781083	10.132	0.712	14.2303
715827883	274.57	19.904	13.7947

Porównanie czasów obliczeń





Dziękujemy za uwagę

Jan Ciurej i Radosław Żak