ĆW Faktoryzacja (Discrete Log problem)

Algorytm faktoryzacji N (Discrete Log problem=DL)

```
1. Wybrać losowo 0 < a < N.
```

2.

$$\gcd(N, a) > 1 \implies \text{Print } \gcd(N, a). \text{ Stop.}$$

 $\gcd(N, a) = 1 \implies \text{Go to } 3.$

3. Rozwiązać DL (Discrete Log problem): $a^r \equiv 1 \mod N$.

4.

$$2 \mid r \Rightarrow \text{Go to } 5.$$

 $2 \nmid r \Rightarrow \text{Go to } 1.$

5. Obliczyć $\gcd(N, a^{\frac{r}{2}} \pm 1)$.

6.

$$\gcd(N,a^{\frac{r}{2}}+1)>1 \text{ or } \gcd(N,a^{\frac{r}{2}}-1)>1 \quad \Rightarrow \quad \text{Print jeden z } \gcd(N,a^{\frac{r}{2}}\pm1), \text{ który jest}>1. \text{ Stop. } \gcd(N,a^{\frac{r}{2}}+1)=1 \text{ and } \gcd(N,a^{\frac{r}{2}}-1)=1 \quad \Rightarrow \quad \text{Go to 1.}$$

Przykład.
$$N=12, a=5$$
 $\gcd(12,5)=1, \, \mathrm{DL} \colon 5^2\equiv 1 \mod 12 \; (\mathrm{czyli} \; r=2)$ $\gcd(12,5^{\frac{2}{2}}\pm 1)=\gcd(12,4), \gcd(12,6)=4,6$

x		0	1	2	3	4	5	
$5^x \mod$	12	1	5	1	5	1	5	

Zadanie. Wyświetlić a, r dla rozwiązania DL. Wyświetlić jeden dzielnik.

- (1) 12 (2) 91 (Fałszywa liczbza pierwsza) (3) 57 (Liczba pierwsza Grothendiecka)
- (4) 143 (2011, 4 qubits) (5) 1737 (Iloczyn Eulera) (6) 1859 (Hipoteza Riemanna) (7) 13843
- (8) 988027

Zob. YouTube Hipoteza Riemanna — Zagadka Wszech Czasów (Szczególnie: Louis de Brange 1932– w samym początku wideo; RSA, VeriSign od 28 min./47:55)

Algorytm Euklidesa (C++)

```
int gcd(int a, int b){
    if (a\%b == 0)
        return b;
    else
        return gcd(b, a\%b);
}
```

Algorytm Euklidesa (Python)

```
def gcd(a, b):

while b:

a, b = b, a\%b

return abs(a)
```