

Rozkládáme číslo 3977 algoritmem Pollard p-1.

1. zvolíme  $B := 25$

2. zvolíme náhodně  $a := 127, d := \gcd(3977, 127) = 1$

3. (a)  $p_1 := 2$

$$e := \lfloor \log_2(25) \rfloor = 4$$

$$a := 127^{2^4} \bmod 3977 = 775$$

$$d := \gcd(3977, 774) = 1$$

(b)  $p_2 := 3$

$$e := \lfloor \log_3(25) \rfloor = 2$$

$$a := 775^{3^2} \bmod 3977 = 3782$$

$$d := \gcd(3977, 3781) = 1$$

(c)  $p_2 := 5$

$$e := \lfloor \log_5(25) \rfloor = 2$$

$$a := 3782^{5^2} \bmod 3977 = 2133$$

$$d := \gcd(3977, 2132) = 41$$

4. return 41

Zjistili jsme, že 41 je faktor čísla 3977. Platí  $\frac{3977}{41} = 97$ . Obě čísla jsou prvočísla. Tudíž 97, 41 je prvočíselný rozklad 3977.