Rozkládáme číslo 3977 algoritmem ECM.

1. zvolíme $B \coloneqq 13$
2. zvolíme náhodně $a \coloneqq 3, d \coloneqq \gcd(3977, 4 \cdot 3^3 + 27) = 1$
3. máme tedy $e_B = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 360360$
4. $P_0 = [0, 1]$ a snažíme se spočítat $e_B \cdot P_0$ pomocí metody "binárního násobení"viz přednáška. Definujeme $Q = 0, P = P_0$
5. Číslo e_B je dělitelné 2^3 viz výše. Spočítáme tedy bod $P = 2^3 P_0 = 8P_0 = [70, 1353]$ a přičteme ho k $Q \implies Q = 8[0, 1] = [70, 1353]$.
6. V proměnné P je nyní hodnota $8[0, 1] = [70, 1353]$. V dalším kroku chceme počítat bod $P = P+P = 16[0, 1] = [70, 1353]+[70, 1353]$. Při výpočtu inverzu $(2 \cdot 1353)^{-1} = 2706^{-1} \mod 3977$ výpočet selže, jelikož inverz neexistuje, protože $\gcd(2706, 3977) \neq 1$
7. spočteme tedy $\gcd(2706, 3977) = 41$ a máme faktor 3977. Druhý dopočítáme vydělením první faktorem.
8. Dostaneme $3977 = 41 \cdot 97$