Sławomir Górawski

Lista 4, zadanie 4. W jaki sposób znając dwie reszty b, c modulo n takie $b \neq \pm c \mod n$ i $b^2 = c^2 \mod n$ można znaleźć rozkład n na dwa czynniki.

Rozwiązanie. Przekształcając drugą równość, otrzymujemy:

$$\begin{aligned} b^2 &= c^2 \mod n \\ b^2 - c^2 &= 0 \mod n \\ (b+c)(b-c) &= 0 \mod n. \end{aligned}$$

Wiemy z założenia, że ani $b + c$, ani $b - c$ nie przystają do 0 modulo n, ale ich iloczyn tak. W takim razie w rozkładzie na czynniki oba muszą mieć w sobie dzielniki n. Jeden z szukanych czynników to $\gcd(b - c, n)$. Możemy go znaleźć np. algorytmem Euklidesa. Drugi możemy znaleźć, dzieląc n przez pierwszy.