Sławomir Górawski

Lista 4, zadanie 5. Pokaż jak można rozłożyć na dwa czynniki liczbę złożoną n, która w teście Millera–Rabina okazała się złożona, ponieważ dla pewnego a wyliczyliśmy $a^{2^k r} \not\equiv \pm 1, a^{2^{k+1} r} \equiv 1$ modulo n.

Rozwiązanie. Niech $x = a^{2^k r}$; wtedy $x^2 = a^{2^{k+1} r}$. Wiemy, że:

$$\begin{aligned} x &\not\equiv \pm 1 \mod n, \\ x^2 &\equiv 1 \mod n. \end{aligned}$$

Z pierwszej równości wiemy, że n nie dzieli $x + 1$ ani $x - 1$. Przekształcając drugą, otrzymujemy:

$$(x + 1)(x - 1) \equiv 0 \mod n.$$

Jeśli n nie dzieli żadnego z powyższych, to oba muszą zawierać w swoim rozkładzie czynniki n niebędące 1 ani n. Możemy je znaleźć, wyliczając $\gcd(n, x + 1)$ oraz $\gcd(n, x - 1)$.