LABORATORIUM III
ZADANIA

Zadanie 1 (obowiazkowe), 1 pkt. Uzupełnić kod w pliku `fermat_test.cpp` tak, aby całość dawała testowanie pierwszości testem Fermata. Za pomocą tego programu (spróbować) uzasadnić, że liczba RSA - 617 jest złożona (jest ona zapisana w pliku `rsa617.txt`). Dodatkowo program powinien wypisywać "świadka złożoności", czyli podstawę za pomocą, której stwierdzamy, iż liczba jest złożona.

Zadanie 2 (obowiazkowe), 1 pkt. Wiadomo, że liczba

$$N = 15902312310431783769516984 01$$

jest liczbą Carmichaela (zob. ciąg A006931 w OEIS). Sprawdźmy to "doświadczalnie" – w tym celu proszę zmodyfikować program z zadania pierwszego by wykonywał 20 prób testu Fermata i dla każdego ze świadka złożoności wypisywał jego największy wspólny z liczbą N.

Dodatkowo korzystając z pakietu Mathematica obliczyć jakie jest prawdopodobieństwo, iż wylosowana liczba będzie świadkiem złożoności.

Liczba N zapisana jest w pliku `carmichael.txt`.

Zadanie 3 (obowiazkowe), 2 pkt. Napisać program, który implementuje test Millera - Rabina. Za jego pomocą zbadać, czy liczby $F_1, \ldots, F_{15}$ są złożone czy też (prawdopodobnie) pierwsze. Tutaj $F_n = 2^{2^n} + 1$. Prawdopodobieństwo pomyłki (dla pojedynczej liczby F_k) powinno wynosić co najwyżej $\frac{1}{2^{30}} \approx 9.3 \cdot 10^{-10}$.