Lattices

Exercise 1:
Prove Theorem 50 for the non-homogeneous linear system

\[ a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \mod N. \]

Wiener’s attack

Exercise 2:
What is the bound on secret RSA-key \( d \) in Wiener’s attack when \( N \) is a product of three equal size distinct primes? Does this make the attack more/less effective?

Coppersmith’s method

Exercise 3:
Let \( c = m^3 \mod N \) and \( c' = (m + r)^3 \mod N \) be two RSA-ciphertexts for message \( m \) with known padding \( r \). Provide an efficient algorithm to recover \( m \) using \( c, c', r \) and \( N \).

Exercise 4:
Consider a monic polynomial of degree 2

\[ f(x) = x^2 + ax + b \]

with \( f(x_0) = 0 \mod M \) and \( |x_0| < X \). Using the proof of Theorem 59 provide a more tight estimation for \( X \) s.t. the Coppersmith’s method finds \( x_0 \) in polynomial in \( \log M \) time. Use \( m = 3 \).