

Homework 26

1. Use the method of squares to factor $N = 121477$, with factor base $\{-1, 2, 3, 5, 7, 11\}$. Square the following integers modulo N , and then find relations: 349, 604, 697, 698, 773, 917, 1047, 1207, 1208, 1247.
2. Suppose $N = 78899$ is used as an RSA modulus with encoding exponent 19 and decoding exponent 4123. Show how this information can be used to quickly factor N .