Math 55—Fall 2025—Haiman
Homework 7

Some of the problems on this homework set require quite a bit of computation using a calculator (a programmable calculator may be helpful) or a computer. For that reason, I've assigned fewer problems than usual.

Problems from Rosen

Section 4.6

24. Show your steps.

26. Modified as follows. Use the same $n = 53 \cdot 61$ as in the problem, but use $e = 253$ for the encryption exponent, and 2642 3218 2887 1068 for the encrypted message. (It takes less work to find the answer with these numbers than with the numbers in the book.)

28.

30. Describe the steps and also find their shared key!

32. (Following the instructions preceding Exercises 31–33.)

Additional problems:

1. Pollard's factoring algorithm is described in the supplementary notes on factoring on bCourses (see the list of lecture topics and reading). Use Pollard's algorithm to factor the number $n = 7081$. Show your steps.

(2a) Show that if $a^2 \equiv b^2 \pmod{n}$, where $a \not\equiv \pm b \pmod{n}$, then $\gcd(a+b, n)$ and $\gcd(a-b, n)$ are non-trivial factors of n (i.e., they are factors and they are not equal to 1 or to n).

(2b) Use part (a) to factor the number $n = 6893$ by trying the first several integers a larger than $\sqrt{n}$ until you find one for which $a^2 \bmod n$ is a perfect square.

FYI: The method in this problem is Fermat's factoring algorithm. If n is composite, it typically takes about $\sqrt[4]{n}$ steps to find a number a such that $a^2 \bmod n$ is a perfect square and factor n, similar to the performance of Pollard's algorithm.