PMATH 145 Assignment 4

Patrick Ingram

Due November 3 at 12:30PM

Problem 1. Suppose that you compute $\gcd(a, b)$ using the Euclidean algorithm, where $b > a > 0$ are integers, and you get remainders $a = r_0, r_1, \ldots$. That is, your calculation looks like this:

$$\begin{aligned} b &= q_1 a + r_1 \\ a &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \end{aligned}$$

where $r_n = \gcd(a, b)$. Show that for each j, $r_{j+2} < \frac{1}{2} r_j$. Use this to show that the Euclidean algorithm always computes $\gcd(a, b)$ in at most $\log_2(b)$ steps (when $b > a > 0$). This means that it is a polynomial-time algorithm.

Problem 2. Suppose that Alice posts the public RSA key $m = 713$, $e = 313$ on her website, and Bob sends her the three-part (encrypted) message: 110, 676, 110. What's he trying to say? (For this problem, I converted the original message into numbers using A$\rightarrow$ 11, B$\rightarrow$ 12, $C \rightarrow 13$, ...).

Problem 3. This time Alice has posted the key $m = 7081$ and $e = 1789$, and Bob sends 5192, 2604, 4222. What was the message (now the original message was broken up into blocks of two letters, using the system above, e.g., AD$\rightarrow$ 1114).

The following list of primes up to 100 might help you with factoring: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.