MATH/CS 295: CRYPTOGRAPHY
HOMEWORK #3 ADDITIONAL PROBLEMS

Problem 1.A. The digits in base 16 are written with $10 = A, 11 = B, ..., 15 = F$; e.g. $(9B)_{16} = 9 \cdot 16 + 11 = 155$. Write 12538 in binary and hexadecimal.

Problem 1.B. Let $a, b \in \mathbb{Z}_{>0}$ with $a > b$.

(a) Show that $a - b$ can be computed in time $O(\log a)$.

(b) Suppose that the Euclidean algorithm is performed on $r_0 = a, r_1 = b$ with successive quotients q_i defined by $r_{i-1} = q_i r_i + r_{i+1}$. Show (by induction) that $a \geq q_1 \cdots q_t$, so that $\log a \geq \sum_i \log q_i$. Conclude that the Euclidean algorithm runs in time $O\big((\log a)(\log b)\big)$.

Problem 1.C. The ring $\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\}$ is Euclidean under the norm $N(x + yi) = x^2 + y^2$. Let $a, b \in \mathbb{Z}[i]$ be not both zero, and suppose $N(a) > N(b)$. Show that the number of divisions performed in the Euclidean algorithm for $\mathbb{Z}[i]$ is $O(\log N(b))$.