MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #2

Problems for all

Problem 1. Let $a, b \in \mathbb{Z}$.

(a) Let $\gcd(a, b) = g \neq 0$. Prove that $\gcd(a/g, b/g) = 1$.
(b) Prove that $\gcd(a + kb, b) = \gcd(a, b)$ for all $k \in \mathbb{Z}$.

Problem 2. Use the extended Euclidean algorithm to compute 367^{-1} in $(\mathbb{Z}/1001\mathbb{Z})^*$ and 1001^{-1} in $(\mathbb{Z}/367\mathbb{Z})^*$.

Problem 3. 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 4. 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 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 5. Let $f_0 = f_1 = 1$ and $f_{i+1} = f_i + f_{i-1}$ for $i \geq 1$ denote the Fibonacci numbers.

(a) Use the Euclidean algorithm to show that $\gcd(f_i, f_{i-1}) = 1$ for all $i \geq 1$.
(b) Find $\gcd(11111111, 11111)$.
(c) Let $a = 111 \cdots 11$ be formed with f_i repeated 1s and let $b = 111 \cdots 11$ be formed with f_{i-1} repeated 1s. Find $\gcd(a, b)$. *[Hint: Compare your computations in parts (a) and (b).]*

Additional problems for 395A

Problem 6. 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 in the Euclidean algorithm for $\mathbb{Z}[i]$ to compute $\gcd(a, b)$ is $O(\log N(b))$.

Problem 7. Let $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Show that a^{-1} can be computed in time $O(\log^2 n)$.

Computational challenges

Problem C1. Write a computer program that computes the r-adic expansion of a positive integer a for any $r \in \mathbb{Z}_{>1}$.

Date: Due Wednesday, 17 September 2008.