MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #10

Problems for all

Problem 1. For the following integers either provide a witness for the compositeness of n or conclude that n is probably prime by providing 5 numbers that are not witnesses.

(a) $n = 1009$.
(b) $n = 2009$.

Problem 2. Using big-O notation, estimate the number of bit operations required to perform the witness test on a number n enough times so that, if n passes all of the tests, it has less than a 10^{-m} chance of being composite.

Problem 3. Factor 53477 using the Pollard rho algorithm.

Problem 4.

(a) Find a nontrivial factorization of $n = 999999999999999919$ *without* using any technological aid.
(b) Let $n = 642401$. Given
$$516107^2 \equiv 7 \pmod{n}$$
and
$$187722^2 \equiv 2^2 \cdot 7 \pmod{n}$$
factor n.
(c) Why doesn't the fact that
$$3^2 \equiv 670726078^2 \pmod{670726081}$$
help you to factor $n = 670726081$?

Problem 5. For $e \in [0, 1]$ define $L_e : \mathbb{R}_{>1} \to \mathbb{R}$ by
$$L_e(x) = \exp\left((\log x)^e (\log\log x)^{1-e}\right).$$

(a) Show that $L_0(x) = \log x$ and $L_1(x) = x$.
(b) Show that
$$L_e(x) \leq L_f(x)$$
for all $x \in \mathbb{R}_{>1}$ whenever $e \leq f$.
(c) Show that the function
$$L_{1/2}(x) = \exp(\sqrt{\log x \log\log x})$$
is *subexponential*: i.e., show that for every $\epsilon > 0$, we have
$$L_{1/2}(x) = O(x^{\epsilon}).$$
[Hint: Take the logarithm of both sides and use l'Hôpital's rule.]

Date: Due Wednesday, 12 November 2008.

Problem 6. The *logarithmic integral function* $\mathrm{Li}(x)$ is defined to be

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

(a) Prove that

$$\mathrm{Li}(x) = \frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} + O(1).$$

[Hint: Use integration by parts.]

(b) Compute the limit

$$\lim_{x\to\infty} \frac{\mathrm{Li}(x)}{x/\log x}.$$

[Hint: Break the integral in (a) into two pieces, $2 \le t \le \sqrt{x}$ and $\sqrt{x} \le t \le x$, and estimate each piece separately.]

(c) The *Riemann hypothesis* is equivalent to the statement

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x).$$

Use formula (b) to show that the Riemann hypothesis implies the prime number theorem.

Problem 7. Read §3.7 in Hoffstein-Piper-Silverman. *[Hint: No, you don't have to turn anything in.]*