MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #11

Problems for all

Problem 1. Factor 53477 using the Pollard rho algorithm.

Problem 2. Suppose that n balls are randomly thrown into m bins.

(a) Approximately what is the probability that there is a bin with two balls in it, assuming m is much larger than n?
(b) What is the probability that there is a bin with no balls in it? If m is large, show that this probability is approximately $me^{-n/m}$. *[Hint: Use* $\lim_{x\to\infty}(1+1/x)^x = e$*.]*
(c) In terms of m, what is the smallest value of n so that there is a $\geq 1/2$ chance that no bin is empty?
(d) Suppose you are asked to fill an auditorium with people so that every day is a birthday for some person in the auditorium. What is the smallest number of people which gives you better than an even chance? Test your estimate at

`https://chaka.uvm.edu:8000/home/pub/8`

Problem 3. Show that any odd composite integer can be factored as a difference of two squares.

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 $s \in [0,1]$ define $L_s : \mathbb{R}_{>e} \to \mathbb{R}$ (where $e = \exp(1)$) by

$$L_s(x) = \exp\left((\log x)^s (\log\log x)^{1-s}\right).$$

(a) Show that $L_0(x) = \log x$ and $L_1(x) = x$.
(b) Show that

$$L_s(x) \leq L_t(x)$$

for all $x \in \mathbb{R}_{>e}$ whenever $s \leq t$.

Date: Due Friday, November 12, 2010.

(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 of the inequality $L_{1/2}(x) \leq x^{\epsilon}$ and use l'Hôpital's rule.]

Additional problems for 395A

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, $2 \leq t \leq \sqrt{x}$ and $\sqrt{x} \leq t \leq x$, and estimate each piece separately.]

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

$$\pi(x) = \#\{p \leq x : p \text{ prime}\} = \mathrm{Li}(x) + O(\sqrt{x}\log x).$$

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