MATH 75: MATHEMATICAL CRYPTOGRAPHY
HOMEWORK #7

Problems

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 $n \in \mathbb{Z}_{>0}$ 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. 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, and n is large in comparison to m, 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?

Problem 5.

(a) Find a nontrivial factorization of $n = 999999999999999919$ by hand.
(b) Let $n = 2^{29} - 1$. Given that

$$\begin{aligned} 258883717^2 &\equiv -2 \cdot 3 \cdot 5 \cdot 29^2 \\ 301036180^2 &\equiv -3 \cdot 5 \cdot 11 \cdot 79 \pmod{n} \\ 126641959^2 &\equiv 2 \cdot 3^2 \cdot 11 \cdot 79 \end{aligned}$$

discover a factor of n.

Date: Due Wednesday, 18 May 2016.