CSC 373 Lecture 32

Announcements:

Next assignment due Friday, Dec 2; term test 3 on Monday, Dec 5. last class Wed, Dec 7.

Today

- Go over any questions on the assignment
- What course topics are of special interest for reviewing? Send me suggestions!
- Compositeness (primality) testing

Primality Testing

- I now want to turn attention to one of the most influential randomized algorithms, namely a poly time randomized algorithm for primality (or perhaps better called compositeness) testing.
- History of polynomial time algorithms:
  - 1-sided error with prob[ALG says *N* composite|*N* prime] = 0; prob[ALG say *N* prime|*N* composite] <= *delta* < *1*. Can then repeat.
  - Independently shown by Solovay and Strassen, and Rabin ~ 1974
  - The Rabin test is related to an algorithm by Miller ~1976 that gives a det poly time alg assuming (the unproven) ERH
  - 0-sided error alg (expected poly time) by Goldwasser and Kilian ~1986
  - deterministic poly time alg by Agarwal, Kayal and Saxena ~ 2002

- Even though there is a deterministic alg, it is not nearly as efficient as the 1-sided error algs which are used in practice and which also spurred the interest in this topic, had a major role in various cryptographic developments (which required random primes) and more generally became the impetus for the major interest in randomized algorithms.
- While our other examples of randomized algorithms night be considered reasonably natural (even if the analysis might not be easy), the following algorithm requires understanding of the subject matter and is not something that one can just naturally think of.

Some basic number theory

- We need some number theory results (some mentioned before) and a basic result from group theory. Here is what we need:
- *(Z*_N) = {a in Z_N: gcd(a,N) = 1}* is a (commutative) group under multiplication (*mod N*).
- If *N* is prime, then for *a* not 0 *mod N, a^{N-1} = 1 (mod N)* "Fermat's Little Theorem". Furthermore, if *N* is prime then (Z*_N,*) is a cyclic group; that is, there exists a generator *g* such that *{g , g^2, ...,g^{N-1}) = Z_N* which implies that *g^i* is not 1 for *1 <= i < N-1*.
- If *N* is prime, then 1 in *Z*_N* has precisely two square roots {-1,1}
- The Chinese remainder Theorem: Whenever *N_1* and *N_2* are relatively prime, then for all *v_1* and *v_2*, there exists a unique *w < N_1 * N_2* such the *w = v_1 mod N_1* and *w = v_2 mod N_2*.

Simple but not quite correct algorithm

- We need two basic computational facts:

  a^i mod N can be efficiently computed

  gcd(a,b) can be efficiently computed

- Here is a simple algorithm that would work except for an annoying set of numbers (called Carmichael numbers).

  Choose *a* in *Z_N* be uniformly at randomly
  If *gcd(a,N)* not equal 1 then output composite
  If *a^{N-1}* not equal 1, then output composite
  Else output prime.

When does simple algorithm work?

- *S = {a| gcd(a,N) = 1 and a^{N-1} = 1}* is a subgroup of *Z^*_N*
- So if there exists an *a* in *Z*_N* such that *gcd(a,N) = 1* and *a^{N-1}* not = 1, then *S* is a proper subgroup and hence */S/* divides *N-1* and thus can be at most half of *N-1*. Then simple algorithm has prob < ½ of error when *N* is composite.
- The only numbers *N* that give us trouble are the Carmichael numbers *N* (false primes) for which *a^{N-1} = 1* for all *a* such that *gcd(a,N) = 1*. It was only (relatively speaking) recently in 1994 proven that there are an infinite number of Carmichael numbers.
- The first three Carmichael numbers are 561, 1105, 1729; there are only 255 Carmichael numbers <= 100,000,000

Miller-Rabin 1-sided error algorithm

Let *N-1 = (2^t) u* with *u* odd % since *N* is odd, t >=1
Choose non-zero (possible certificate) *a* randomly in *Z_N*.

x_0 = a^u % all computation is mod *N*

For *i = 1 ..t*

x_i := x_{i-1}^2

if *x_i =1* and x_{i-1} not in {-1,1} then report composite

End for

If x_t not = 1 then report composite *%x_t = x^{N-1}*

Else report prime

We need to show Prob[*a* certifies *N* is composite|N is composite] >=1/2. (Note: this is what one generally needs to show a set is in RP, namely lots of certificates.)

Analysis for anyone interested

Let *a* be a non witness (non-certificate).

Since a^{N-1} = 1, a*a^{N-2} = 1 and *a* has an inverse so that *a* in *Z*_N*

We now want to show that the non-witnesses are a proper subgroup *Z*_N* which gives us what we want.

Case 1: *N* is not a Carmichael number in which case we are done.

Case 2: For every *b* in *Z*_N, b^{N-1} = 1* i.e. N is Carmichael implying

*N = N_1 * N_2* with *N_1* and *N_2* relatively prime and odd

The non witnesses must include some *b*

b^{(2^i) u} = -1 and hence *b^{(2^i) u} = -1 mod N_1*

By the Chinese Remainder Theorem, there exists

w = v mod N_1 and *w = 1 mod N_2* and hence

w^{(2^I u)} = -1 mod N_1 and *w^{(2^i) u} = 1 mod N_2*

This implies that *w^{2^i u}* is not in *{-1,1} mod N*.