Lab assignment 1, CS 165

Friday, September 27, 2013

TA: Rachid Ounit.

Email: rouni001@cs.ucr.edu

TA office hours: Monday 5pm-6pm, Friday 10am-11am.

Part I Primes

Question 1

(a) Lemma 1: For any integer n > 0, d is the smallest divisor of n (d prime):

If n is not a prime then d ≤√(n).

Prove the Lemma 1.

(b) Implement a function *IsPrime* in C or C++ that takes an integer n as input and return whether or not n is prime. If the input number is not prime then your function should also print the smallest divisor d of n.

So the output must be "Y n" or "N d".

Do the application for these numbers: Are 399, 4294967297, and 51557463436816307 primes?

If not, give their decomposition (you may implement a function *Decompose* that uses *IsPrime* recursively).

Question 2

Alice is secretly in love with Bob, she is about to encrypt a message (using the RSA encryption) for him but then she realized that she cannot find her favorite list of large prime numbers! She is sure she has left that piece of paper on her desk few days before...

Anyway, she at least remembers that it was a list of 12 prime numbers from the interval $[2^{64}-500, 2^{64}-1]$...

She also does remember (from her Computer Security class) that 2 prime numbers (secretly chosen) are needed for RSA encryption, so she decides to recreate her former precious list.

Working with 64 bits integers, she quickly recovers all prime numbers in the interval $[2^{64}-500, 2^{64}-1]$ using the previous lemma. She claims that: "there is only 12 prime numbers and the last digit is 9 for 1 of them, 7 for 4 of them, 3 for 5 of them, 1 for 2 of them."

(a) Like Alice, give all prime numbers in the interval $[2^{64}-500, 2^{64}-1]$, using the lemma proved earlier. Do you agree with her statement?

(b) Actually, Alice could not find her list because Carole stole it from her. Carole also knows requirements for RSA encryption (she also stole Alice's lessons of CS 165), so she's aware that Alice needs two primes to encrypt her messages to Bob. But Carole has no clue which pair of prime Alice will choose...

Given a list of 12 prime numbers, if Carole tries to guess Alice's choice, how many pairs of primes are there to consider in the worst case?

What is the probability that Carole finds out the correct pair after two guesses (or less)?

You can assume Alice choose her pairs of prime randomly.

Question 3

(a) Lemma 2: For any integer n, if 2^n+1 is prime then n is a power of 2.

Prove the Lemma 2.

(b) Evaluate these numbers at least for n=0, 1, ...5.

(c) How about "For any integer n, if n is a power of 2 then 2^n+1 is prime"?

Fermat conjectured all Fermat numbers are primes. A young Mathematician from Switzerland claimed in 1732 that this conjecture was unfortunately wrong. What do you think about this conjecture? Prove it in detail or just give a precise counter-example.

Part II Congruence

Question 1

Prove that for any integer n, 7 divides $9^n - 2^n$.

To go further...

Chinese Remainder Theorem

See question on board.