COMP-547B Homework set #1

<u>Due Thursday October, 8 2020 until 23:59</u>

To be submitted via MyCourse.

A. **<u>THEORY</u>:** Consider an expression of the form

$$ax^2 + bx + c \equiv 0 \pmod{N}.$$

[10%] **1.** Show that the x's of the following form are solutions of the above system:

$$x \equiv \left(-b \pm \sqrt{b^2 - 4ac}\right)(2a)^{-1} \pmod{N}$$

when $\gcd(2a, N) = 1$ and $b^2 - 4ac$ is a **Quadratic Residue** mod N. (Here $\sqrt{q}$ is an integer square root of a quadratic residue q mod N.)

[10%] **2.** Give all the necessary and sufficient conditions for existence of solutions to the above system and for any tuple of parameters (a, b, c, N) specify how many solutions exist ? Be as exhaustive as possible.

B. **<u>THEORY</u>: Probability**

Calculate a best upper bound on the probability that we mistakenly output a composite number instead of a prime after the following two events occurred:

- pick a random m-bit integer N such that $\gcd(N, 210) = 1$
- the procedure $\mathrm{Miller{-}Rabin}(N, t)$ returns 'prime'

[10%] 1) Express your bound as a function of m and t.

<u>(Assume that the prime number theorem is exact.)</u>

$$\frac{\pi(N)m}{N} = \log_2 e$$

...more on back...

[10%] 2) If I want a random **4096**-bit prime p, what t should be used in $\text{Miller-Rabin}(N, t)$ to guarantee probability at most $1/2^{50}$ of outputting a composite number?

C. <u>**THEORY**</u>: **Running time**

Calculate a best upper bound (in Big *O* notation) on the *expected* running-time for generating random numbers ***p*** and ***g*** as described below:

• pick a random m-bit integer q such that $\gcd(q, 210) = 1$ until q is *declared* prime and $p := 2q + 1$ is *declared* an $(m+1)$-bit **Sophie-Germain** prime. For simplicity, assume that whenever $\text{Miller-Rabin}(N, t)$ is ran on a composite number N, it declares prime with probability exactly 4^{-t}.

• pick a random integer g, $1 \le g \le p - 1$, a primitive element of $\mathbb{F}_p$.

[10%] 1) Express your *expected* time bound as a function of m and t. Assume all primality testing is done via $\text{Miller-Rabin}(N, t)$ at cost $O(m^3 t)$ time. Assume the probabilities that q and $p := 2q + 1$ be prime are independent.

<u>**(Assume that the following statement is exact.**</u>

$$\frac{\phi(N) \log \log N}{N} \ge e^{-\gamma} \approx 0.5614594836$$

[10%] 2) If I want a random **4096**-bit Sophie-Germain prime p, what t should be used in $\text{Miller-Rabin}(N, t)$ to guarantee probability at most $1/2^{50}$ of outputting a number which is not a Sophie-Germain prime p ? You may assume that the probabilities that q and $p := 2q + 1$ be prime to be independent.

(Let $P_{m,t}$ be the correct answer to question B,1). You may use $P_{m,t}$ as part of your current answer. In other words, no need to solve B,1) to solve the current question.)

[10%] D. <u>Varia</u>

1) Prove that in Algorithm 13.31 (square root extraction mod a prime) the case where p is 3 mod 4 is not really necessary as the case where p is 1 mod 4 would work as well on numbers p congruent to 3 mod 4 and return $a^{\frac{p+1}{4}} \pmod{p}$.

...more on back...

[10%] 2) Given $\forall a \in \mathbb{F}_q \backslash \{0\}, a^{q-1} = 1$ and the theorem provided in class:

Let $l_1, l_2, \ldots, l_k$ be the prime factors of $q-1 = l_1 \cdot l_2 \cdots l_k$ and

$$m_1 = \frac{q-1}{l_1}, m_2 = \frac{q-1}{l_2}, \ldots, m_k = \frac{q-1}{l_k}.$$

An element g is **primitive** over $\mathbb{F}_q$ if and only if

- $g^{q-1} = 1$
- $g^{m_i} \neq 1$ for $1 \leq i \leq k$.

Prove that if g is a primitive element of $\mathbb{F}_q$, and n is such that $\gcd(n, q-1) = 1$ then g^n is also a primitive element of $\mathbb{F}_q$.

E. Small number calculations

Let N = 262 915 409 be a reasonably small integer and s be your 9-digit student id number. (Show all your calculations)

[5%] 1) Show that exactly one $y \in \{s, -s, 3s, -3s\}$ is a quadratic residue mod N.

[5%] 2) Find all the square roots of y modulo N.

[5%] 3) Show that for any x s.t. $\gcd(x, N) = 1$, we also have that exactly one $y \in \{x, -x, 3x, -3x\}$ is a quadratic residue modulo N.
What is special about 3 and N that makes this work (modulo N)?

[5%] 4) Find a base a such that $\text{Miller-Rabin}(N,1)$ returns ***composite***.

…more on back…