COMP-547B Homework set #1

Due Thursday February, 6 2020 until 23:59

To be submitted via MyCourse.

A. **THEORY:** Consider an expression of the form

$$\mathbf{0 \equiv a x^2 + b x + c \ \ (\bmod\ n).}$$

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

$$x \equiv (-b \pm \sqrt{b^2 - 4ac})\,(2a)^{-1} \ \ (\bmod\ n)$$

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

[15%] **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 ?

B. THEORY: Probability

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

- pick a random m-bit integer n such that $\gcd(n,210)=1$
- the procedure **Miller-Rabin_*prime*(n,k)** returns 'prime'

[15%] 1) Express your bound as a function of m and k.

(Assume that the prime number theorem is exact.)

$$\frac{\pi(n)\log n}{n} = 1$$

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

...more on back...

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

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

- pick a random ***m***-bit integer ***n*** such that ***n*+1 = *p* is prime** with known factorisation of ***n*** (using Kalai's *randfact*)
- pick a random integer ***g***, 1 ≤ ***g*** ≤ ***n***, that is a primitive element in $\mathbb{F}_p$.

[10%] 1) Express your time bound as a function of ***m*** and ***k***.
(assume all primality testing is done via **Miller-Rabin_*prime*** at cost $O(m^3k)$)

<u>(Assume that the following statements are exact.</u>

$$\frac{\phi(n)\log\log n}{n} \geq e^{-\gamma} \approx 0.5614594836$$

$$M_n \log n = e^{-\gamma} \approx 0.5614594836$$

[15%] 2) If I want a random **4096** bits prime ***p***, what ***k*** should be used in **Miller-Rabin_*prime*** **(*p*,*k*)** to guarantee probability at most $\mathbf{1/2^{50}}$ of outputting a composite number or that ***p*** not be uniform ?

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

D. <u>Small number calculations</u>

Let ***n*** = 262 915 409 be a reasonably small integer and ***s*** be your 9-digit student id number. (<u>Show all your calculations</u>)

[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 *Pseudo*(***a***,***n***) returns ***composite***.

[5%] 5) What is $\varphi(n)$?

…more on back…