COMP-547B Homework set #1

Due Thursday February, 1 2018 until 23:59

To be submitted via MyCourse.

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

$$0 \equiv a x^2 + b x + c \pmod{n}.$$

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

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

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.)

[+10%] *__2.__ (**BONUS**) 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) how many solutions exist ?

B. **MATHEMATICA:** Let p be a prime such that $5 \in \mathbf{QR}_p$.

[5%] **1.** Give a full characterization of all such p (**mod 10**), i.e. a subset $\mathbf{F} \subseteq \{0,1,2,3,4,5,6,7,8,9\}$ such that $5 \in \mathbf{QR}_p \Leftrightarrow p \bmod 10 \in \mathbf{F}$.

[5%] **2.** Choose a random (uniform[1]) **200-bit prime** p such that $5 \in \mathbf{QR}_p$ and let $r < p/2$ be a square root of $5 \bmod p$. Show us your values of p and r.

[5%] **3.** Compute and provide $\varphi = (1+r)2^{-1} \bmod p$.

[5%] **4.** Define $\mathbf{F}_p(n) = (\varphi^n - (-\varphi)^{-n})\, r^{-1} \bmod p$. Calculate and provide the first **50** values of $\mathbf{F}_p(n)$, i.e. $\mathbf{F}_p(0), \mathbf{F}_p(1), \ldots, \mathbf{F}_p(49)$.

[5%] **5.** What do you find special about this sequence of numbers **???**

[5%] **6.** A linear recurrence **mod** p is a relation about a function **f** such that

$$a_k \mathbf{f}(n+k) + a_{k-1} \mathbf{f}(n+k-1) + \ldots + a_1 \mathbf{f}(n+1) + a_0 \mathbf{f}(n) \equiv 0 \pmod{p}$$

where the a_i's are integer coefficients. Using the result of **(4–5.)** exhibit a simple linear recurrence **mod** p for $\mathbf{F}_p$.

---

[1] You are required that your number's most significant bits be the binary representation of your student number, this way you each get a very different prime.

…more on back…

C. **THEORY: from Brassard-Bratley's book**

8.5.13 Let $p \equiv 1 \pmod 4$ be a prime, and let x be in QR_p. We say that an integer a ($0 < a < p$) *gives the key* to $\sqrt{x}$ if $(a^2-x) \bmod p$ is not in QR_p.

[10%] I. Prove that Algorithm **rootLV** finds a square root of x if and only if it randomly chooses an integer a that *gives the key to* $\sqrt{x}$.

[10%] II. Prove that exactly $(p+3)/2$ of the $p-1$ possible choices for a (more than 50% of them) *give the key to* $\sqrt{x}$.

Consult handout for appropriate **HINT**.

D. **MATHEMATICA: KALAI**

[10%] 1. Write a **MATHEMATICA™** procedure **Kalai_range(e)** which outputs a uniformly generated integer r in the range $[2^e \ldots 2^{e+1}-1]$, with its prime factorization (as a list $[p_1, p_2, \ldots, p_k]$ such that $r = p_1 \times p_2 \times \ldots \times p_k$).

[15%] 2. Use your procedure to find random (uniform[2]) primes

r_{318} in the range $[2^{318} \ldots 2^{319}-1]$ with known factorization of $r_{318}-1$,
r_{348} in the range $[2^{348} \ldots 2^{349}-1]$ with known factorization of $r_{348}-1$, and
r_{398} in the range $[2^{398} \ldots 2^{399}-1]$ with known factorization of $r_{398}-1$.

[15%] 3. For each of r_{318}, r_{348}, and r_{398} find a random (uniform[3]) primitive element g_{318} (modulo r_{318}), g_{348} (modulo r_{348}), and g_{398} (modulo r_{398}).

[+5%] [2] You are ***not required*** that your numbers' most significant bits be the binary representation of your student number. **(BONUS)** Why would it be a problem if I requested that ???

[3] You are again required that your numbers' most significant bits be the binary representation of your student number, this way you each get a very different primitive element.

…more on back…