COMP-547B Homework set #1

Due Wednesday February, 1 2017 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 solutions to the above system

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

when $\gcd(2a,n)=1$ and where $\sqrt{q}$ returns an integer square root of an integer q which is a **Quadratic Residue** modulo n.

[10%] ***2.** (**BONUS**) Give all the necessary and sufficient conditions for existence of solutions to the above system.
For any tuple of parameters (a,b,c,n) how many solutions exist ?

B. **MATHEMATICA**: Let p be a prime such that $5 \in QR_p$.

[5%] **1.** Give a full characterization of all such p (in terms of $p \bmod 10$).

[5%] **2.** Choose a random (uniform) **200-bit prime** p such that $5 \in QR_p$ and let r be a square root of $5 \bmod p$. Show us your values of p and r.

[5%] **3.** Compute $\varphi = (1+r) \div 2 \bmod p$.

[5%] **4.** Define $F(n) = (\varphi^n - (-1)^n \div \varphi^n) \div r \bmod p$.
Calculate the first **100** values of $F(0), F(1),\ldots,F(99)$.

[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

$$a_k\, f(n+k) + a_{k-1}\, f(n+k-1) + \ldots + a_1\, f(n+1) + a_0\, f(n) \bmod p = 0$$

where the a_i's are integer coefficients.

Using the result of **(5.)** exhibit a simple linear recurrence **mod** p for **F**.

…more on back…

C. **<u>THEORY</u>: from Brassard-Bratley's book**

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

[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 *give the key to* $\sqrt{x}$.

Consult handout for appropriate **HINT**.

D. **<u>MATHEMATICA</u>: KALAI**

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

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

r_{300} in the range $[2^{300}..2^{301}-1]$ with known factorization of $r_{300}-1$,
r_{350} in the range $[2^{350}..2^{351}-1]$ with known factorization of $r_{350}-1$, and
r_{400} in the range $[2^{400}..2^{401}-1]$ with known factorization of $r_{400}-1$.

[15%] 3. For each of r_{260}, r_{320}, and r_{380} find a <u>random</u> (uniform) primitive element g_{300} (modulo r_{300}), g_{350} (modulo r_{350}), and g_{400} (modulo r_{400}).

…more on back…