COMP-547B Homework set #1

Due Tuesday February, 3 2015 in class at 13:00

Send to cs547@cs.mcgill.ca all your Maple code before the deadline.

A. THEORY: Consider an expression of the form

\[ 0 = a x^2 + b x + c \pmod{n} \]

[10%] 1. Show that the \(x\)'s of the following form are solutions to the above system

\[ x = (-b \pm \sqrt{b^2 - 4ac})(2a)^{-1} \pmod{n} \]

when \(\gcd(2a,n)=1\) and where \(\sqrt{\cdot}\) returns an integer square root of a \(\text{QR}_n\).

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

B. MAPLE: Let \(p\) be a prime such that \(5 \in \text{QR}_p\).

[5%] 1. Give a complete characterization of all such \(p\) in terms of \(p \pmod{10}\).

[5%] 2. Choose a random 100-bit prime \(p\) such that \(5 \in \text{QR}_p\) and let \(r\) be a square root of \(5 \pmod{p}\). Show us your values of \(p\) and \(r\).

[5%] 3. Compute \(\varphi = (1+r)/2 \pmod{p}\).

[5%] 4. Define \(F(n) = (\varphi^n - (-1)^n + \varphi^n) \div r \pmod{p}\). 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 \(\pmod{p}\) is a relation about a function \(f\) such that

\[ a_k f(n+k) + a_{k-1} f(n+k-1) + \ldots + a_1 f(n+1) + a_0 f(n) \pmod{p} = 0 \]

where the \(a_i\)'s are integer coefficients.

Using the result of 5. exhibit a simple linear recurrence \(\pmod{p}\) for function \(F\).

...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 \(\mathbb{QR}_p\).
An integer \(a, 0 < a < p\), gives the key to \(\sqrt{x}\) if \((a^2 - x)\mod p\) is not in \(\mathbb{QR}_p\).

1) 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 \(\sqrt{x}\).

2) 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. **MAPLE:** KALAI

1. Write a MAPLE™ 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 \([p_1,p_2,\ldots,p_k]\)).
Use every possible trick you may come up with to speed up your algorithm. To help you, I provide you with an alternative procedure to MAPLE’s “isprime” called “estpremier” (the French words for “is prime”). The Maple code for estpremier may be found on the course web page. On average, it is roughly 20% faster than isprime…

2. Use your procedure to find random primes

- \(r_{260}\) in the range \([2^{260}..2^{261}-1]\) with known factorization of \(r_{260}-1\),
- \(r_{320}\) in the range \([2^{320}..2^{321}-1]\) with known factorization of \(r_{320}-1\), and
- \(r_{380}\) in the range \([2^{380}..2^{381}-1]\) with known factorization of \(r_{380}-1\).

3. For each of \(r_{260}, r_{320}, \text{ and } r_{380}\) find a random primitive element \(g_i\) modulo \(n_i\).