Exercise 1: (RSA - Bad choice of primes)
For the RSA method, one calculates at first two prime numbers p and q and builds the product $n = p \cdot q$. The number n is later known in public, while p and q are kept secret.
If p and q are close together, then they can be calculated with the *Fermat factorization method*.
If $n = p \cdot q$ with $p > q$, then

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$

Therefore one gets for $p = \lceil\sqrt{n}\rceil + \hat{p}$ and $q = \lceil\sqrt{n}\rceil + \hat{q}$ the equation

$$\left(\lceil\sqrt{n}\rceil + \frac{\hat{p}+\hat{q}}{2}\right)^2 - n = \left(\frac{\hat{p}-\hat{q}}{2}\right)^2.$$

Here $\lceil x \rceil$ is the *ceiling function* which rounds up to the next integer.

1. Explain how the factors of n can be obtained using the last equation and program the corresponding algorithm.
2. Use this method to factorize the following number
   4143977748966434243307454492626122211734875100576213552709682305695820526691442409

(6 points)

Exercise 2: (Modular Logarithm/Babystep-Giantstep method)
Let be $p \in \mathbb{P}$ and $n = \lfloor\sqrt{p}\rfloor$. Then we get

$$x \equiv \log_a b \mod p \iff a^r \equiv b a^{-qn} \mod p, \tag{1}$$

where $x = q \cdot n + r$ with $0 \le q, r < n$. Here $\lfloor x \rfloor$ is the *floor function* which rounds down to the next integer.

(a) Prove the equivalence (1).

(b) The equivalence (1) justifies the approach used in the following *Babystep-Giantstep method* for the determination of the modular logarithm.

  (i) Build a set M with the elements $a^r \mod p$ for $r = 0, \ldots, n-1$.
  (ii) Check if $ba^{-qn} \mod p$ is contained in M ($q = 0, \ldots, n-1$).
  If for a couple (q, r) the relation $a^r \equiv ba^{-qn} \mod p$ is valid, then determine the (minimal) modular logarithm $x = q \cdot n + r$.
  Hint: One can determine $ba^{-qn} \equiv b\left(a^{-n}\right)^q \mod p$ from $\left(a^{-n}\right)^{q-1} a^{-n} \mod p$ from the previous iteration.

  Program your algorithm.

(c) Test your program on the following examples

  (i) $\log_2 5 \mod 7$
  (ii) $\log_5 8 \mod 13$
  (iii) $\log_{16643} 3376 \mod 104729$.

  Give the number of the steps which are necessary in the worst case to determine the modular logarithm using the previous algorithm.

(10 points)

Deadline: at the latest Thursday, 11.07.2013, 08.15 h to nana@mathematik.uni-kassel.de. More informations under `http://www.mathematik.uni-kassel.de/~koepf/ca-SS2013.html`