Cryptography, winter 2013/2014

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

3. Exercise sheet
Hand in solutions until Saturday, 16 November 2013, 23:59:59

Exercise 3.1 (Smooth numbers). (11 points)

For Index Calculus B-smooth numbers were important. Denote by $\psi(x, B)$ the number of positive integers less than or equal to x whose prime divisors are at most B.

(i) List all 2-smooth numbers and all 3-smooth numbers up to 20 and give the values of $\psi(20, 2)$ and $\psi(20, 3)$. 2

(ii) Compute $\psi(10\,000, 3)$ and $\psi(10\,000, 100)$. 2

For fixed x and B consider the set $\{p_1, \ldots, p_h\}$ of all prime numbers up to B and let $v = \lfloor \ln(x)/\ln(B) \rfloor$, $(a_1, a_2, \ldots, a_v) \in \{p_1, \ldots, p_h\}^v$, and $a = a_1 a_2 \cdots a_v$.

(iii) Show that a is B-smooth. 2

(iv) Conclude that $\psi(x, B) \geq h^v/v!$. 2

In the course we have used that $\psi(x, B) \geq h^v/v! \approx xu^{-u}$ with $u = \ln(x)/\ln(B)$.

(v) Compute the estimates $h^v/v!$ and xu^{-u} of 3-smooth numbers and of 100-smooth numbers less than 10 000. Compare these estimates to the exact values. What do you observe? 3

Exercise 3.2 (Hands on index calculus). (10 points)

We are going to see the index calculus in action. We are interested in the multiplicative group $G = \mathbb{Z}_p^\times$ with $p = 227$ and generator $g = 2$. We choose as factor base $\mathcal{B} = \{2, 3, 5, 7, 11\}$ with all primes up to the bound $B = 11$.

In the preprocessing step we compute the discrete logarithms of all elements in the factor base $\mathcal{B}$.

(vi) Instead of randomly choosing exponents e and testing whether g^e rem p factors over $\mathcal{B}$, we have already prepared a list with suitable exponents for you. Let e take values from $\{40, 59, 66\}$, give the factorization of g^e rem p over $\mathcal{B}$ and the corresponding linear congruence modulo $(p-1)$ involving the discrete logarithms of the elements in $\mathcal{B}$. [3]

[1] (vii) Compute the discrete logarithm of the generator $g = 2$.

[2] (viii) The three linear relations from (i) are not enough to determine the remaining four unknown discrete logarithms. Find one additional linear congruence from an exponent $e > 10$ yourself.

[2] (ix) Assuming that your additional congruence is linearly independent from the three previous ones, solve the system of congruences for the discrete logarithms of the base elements. (If you do this by hand, note that division by 2 is impossible modulo $(p-1)$ be careful with division that might occur. If you use a computer algebra system, note that those are aware of this problem and have special commands to solve systems of congruences with a given modulus, e.g. `msolve` in MAPLE and `solve_mod` in SAGE.)

Once we have found the discrete logarithms for the elements in the factor base, we can finally compute the discrete logarithm as shown in the lecture.

[2] (x) Compute $\operatorname{dlog}_2 224$ in $\mathbb{Z}_{227}^\times$.