Cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

7. Assignment: Index calculus, generators and cyclic subgroups

(Due: Thursday, 17 December 2009, 23^{59})

Exercise 7.1 (smooth numbers and index calculus). *In the first part of this exercise, consider the factor base* $\mathcal{B} = \{2, 3, 5, 7, 11\}$ *consisting of the first five prime numbers.*

We want to get a feeling for the probability that a randomly chosen number in the range from 1 *to* 1000 *factors over* $\mathcal{B}$*, i.e. is* B-smooth.

(i) (3 points) In a loop, draw random integers between 1 *and* 1000*. Test whether they factor over* $\mathcal{B}$ *(note that no complete factorization is required for this). Repeat until you have found* 20 B*-smooth numbers. The fraction* $20/i$*, where* i *is the total number of performed iterations, is an estimate for the fraction of* B*-smooth numbers among the integers between* 1 *and* 1000*. What is yours?*

In the second part, we want 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 $\mathcal{B}$*.*

(ii) (3 points) Instead of randomly choosing exponents e *and testing, whether* $g^e \mod p$ *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* $g^e \mod p$ *over* $\mathcal{B}$ *and the corresponding linear congruence modulo* $(p-1)$ *involving the discrete logarithms of the elements in* $\mathcal{B}$*.*

(iii) *(2 points) The discrete logarithm of the generator $g = 2$ is obviously 1, but even with this information, the three linear relations from (ii) are not enough to determine the remaining four unknown discrete logarithms. Find one additional linear congruence from an exponent $e > 10$ yourself.*

(iv) *(3 points) 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 $(p-1)$. 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 module, e.g.* `msolve` *in* MAPLE, `solve_mod` *in* SAGE *and* `LinearSolve[A, b, Modulus -> m]` *in* MATHEMATICA.*)*

Once we have found the discrete logarithms for the elements in the factor base, we can finally compute the discrete logarithm of any element x in the group with the following method:

- *Choose random exponents e until $xg^e \mod p$ factors over $\mathcal{B}$, say $xg^e \equiv p_1^{\beta_1} p_2^{\beta_2} \cdots p_h^{\beta_h}$.*
- *The corresponding linear relation reads*

  $$\operatorname{dlog}_g x + e = \beta_1 \operatorname{dlog}_g p_1 + \beta_2 \operatorname{dlog}_g p_2 + \cdots + \beta_h \operatorname{dlog}_g p_h \mod (p-1)$$

- *Since all the $\operatorname{dlog}_g p_i$ have already been determined in the preprocessing step, you can solve this equation modulo $(p-1)$ for $\operatorname{dlog}_g x$.*

(v) *(3 points) Apply this procedure to compute $\operatorname{dlog}_2 224$ in $\mathbb{Z}_{227}^\times$.*

EXERCISE 7.2 (Change of generators). *Let G be a finite cyclic group of order d. Let g be a generator of G. Let us see, what we can find about possible other generators of G and the consequences for DL_G.*

(i) *(3 points) Given a generator g, only certain powers g^i qualify as generators of G. Find out which and prove your criterion.*

(ii) *(2 points) Given two generators g and g', the respective discrete logarithms for an arbitrary element $x \in G$ are linked by the fundamental identity*

$$\mathrm{dlog}_{g'} x = \mathrm{dlog}_g x \, \mathrm{dlog}_{g'} g.$$

Prove it.

(iii) *(3 points) Given two generators g and g' of G, prove the polynomial-time equivalence*

$$\mathrm{DL}_g = \mathrm{DL}_{g'}.$$

Exercise 7.3 (Cyclic subgroups). *Given a finite group G of* composite *order d. Since G itself need not be cyclic, we are looking for cyclic subroups. Our tool to study subgroups of G is the exponention map π_e, defined for $e \in \mathbb{N}$ by*

$$\pi_e : G \to G, \quad \pi_e(x) = x^e.$$

Let $H_e \subseteq G$ be the image of π_e.

(i) *(1 point) Prove that H_e is a subgroup of G.*

(ii) *(2 points) Assume $\gcd(e, d) = 1$ and prove that π_e is a permutation of G.*

Let p be a prime that divides d exactly once. We ask ourselves, if there is a subgroup of order p. The following theorem answers that question.

Theorem. *If a prime p divides the order of a group, then this group contains an element of order p.*

Now, that such an element – and therefore a subgroup – of order p is guaranteed to exist, we look for a way to actually find a subgroup of order p. Our candidate is $H_{d/p}$.

(i) *(2 points) Prove that every element in $H_{d/p}$ has either order 1 or order p using the lemma from the lecture on the effects of the exponentation map π_e on a cyclic group and its generators.*

(ii) *(2 points) Use the theorem from above to prove that $H_{d/p}$ contains elements of order p. This proves that p divides $\#H_{d/p}$.*

(iii) *(3 points) Finally, prove that* $\#H_{d/p}$ *is equal to* p *by assuming the contrary and arriving at a contradiction using the beforementioned theorem once again.*

(iv) *(2 points) Find a subgroup of order* 11 *in* $\mathbb{Z}_{331}^{\times}$ *and name a generator.*