TMA4155 — Exercise 10

Kristian Gjøsteen

2005-11-02

NB! This exercise will be in the auditorium F2.

Task 1 — Pollard's ρ-method

Let p, q be primes, and let g have order q modulo p. Suppose that $y = g^x \bmod p$ for some random x in $\{0, 1 \ldots, q-1\}$. Our goal is to find x from y.

a. Show that if we can find a, a', b, b' such that

$$g^a y^b \equiv g^{a'} y^{b'} \pmod{p},$$

with $a \not\equiv a' \pmod{q}$, then we can find x (the discrete logarithm of y to the base g modulo p).

b. Let $(a_i)_i$ and $(b_i)_i$ be sequences of random numbers satisfying $0 \le a_i, b_i < q$, and construct the sequence $(z_i)_i$ by $z_i = g^{a_i} y^{b_i} \bmod p$. Argue that some number will with high probability appear twice within the first $O(\sqrt{q})$ elements of the sequence.

Argue also that it is unlikely that any one pair appears twice in the sequence $((a_i, b_i))_i$ within the first $O(\sqrt{q})$ elements of that sequence.

c. Explain how you can use the above results to compute discrete logarithms to the base g modulo p.

d. Let $\sigma : \{0, 1, \ldots, p-1\} \to \{0, 1, 2\}$ be a function (e.g. $\sigma(z) = z \bmod 3$), and define the sequences $(a_i)_i$, $(b_i)_i$ og $(z_i)_i$ as follows: $a_0 = b_0 = 0$,

$$a_{i+1} = \begin{cases} a_i + 1 \bmod q & \sigma(z_i) = 0, \\ 2a_i \bmod q & \sigma(z_i) = 1, \\ a_i & \sigma(z_i) = 2, \end{cases} \quad \text{and} \quad b_{i+1} = \begin{cases} b_i & \sigma(z_i) = 0, \\ 2b_i \bmod q & \sigma(z_i) = 1, \\ b_i + 1 \bmod q & \sigma(z_i) = 2, \end{cases}$$

and $z_i = g^{a_i} y^{b_i} \bmod p$. Show that $z_{i+1} = f(z_i)$, where

$$f(x) = \begin{cases} xg \bmod p & \sigma(x) = 0, \\ x^2 \bmod p & \sigma(x) = 1, \\ xy \bmod p & \sigma(x) = 2. \end{cases}$$

e. Explain how we can use the above to compute discrete logarithms with a (heuristically) expected time $O(\sqrt{q})$ using little memory space. (This is Pollard's ρ-algorithm for computing discrete logarithms.)

f. Produce suitably p, q, g and (random) y in Maple and compute the discrete logarithm of y to the base g modulo p.

Task 2 — Pohlig-Hellman

a. Let $p = 2ab + 1$, $\gcd(a,b) = 1$, and let g have order ab modulo p, and let $y = g^x \bmod p$. Show that $g^a \bmod p$ has order b and $g^b \bmod p$ has order a, and that

$$y^b \equiv (g^b)^{x \bmod a} \pmod{p} \text{ and } y^a \equiv (g^a)^{x \bmod b} \pmod{p}.$$

b. Let p, a, b, g, y be as above. Show that if you know the discrete logarithm of $y^b \bmod p$ to the base $g^b \bmod p$ and the discrete logarithm of $y^a \bmod p$ to the base $g^a \bmod p$, then you can easily compute the discrete logarithm of y to the base g.

c. Argue that if $p-1$ is a product of distinct primes, the largest of which is ℓ, then you can compute discrete logarithms modulo $p-1$ in time essentially $O(\sqrt{\ell})$.

Construct a suitable p such that $p-1$ is a product of many distinct small primes, choose random g and y and compute the discrete logarithm of y to the base g modulo p.

d. Let p, ℓ be primes such that ℓ^2 divides $p-1$ but ℓ^3 does not divide $p-1$. Suppose g has order ℓ^2 modulo p, and that $y = g^x \bmod p$, $0 \le x < \ell^2$. Show that

$$y^\ell \equiv (g^\ell)^{x \bmod \ell} \pmod{p}.$$

Use this to show how you can find $x_0 = x \bmod \ell$ in time essentially $O(\sqrt{\ell})$.

e. Let p, ℓ, g, y, x, x_0 be as above. Let $x = x_0 + x_1\ell$, $0 \le x_1 < \ell$. Set $y_1 = yg^{-x_0} \bmod p$ and show that

$$y_1 \equiv (g^\ell)^{x_1} \pmod{p}.$$

Use this to show that once you know x_0, you can find x_1 in time essentially $O(\sqrt{\ell})$. How fast can you find both x_0 and x_1?

f. Extend the results from the previous two tasks to any prime power ℓ^k dividing $p-1$. Argue that if ℓ is the largest prime dividing $p-1$, then you can compute discrete logarithms modulo p in time $O(\sqrt{\ell})$.

Construct a suitable p such that $p-1$ is a product of many small-prime powers, choose random g and y and compute the discrete logarithm of y to the base g modulo p.