Tanja Lange
TU/e

10 Mar 2010

2. Take-home exercises mastermath class
"Algebraic Geometry in Cryptology"
Deadline: March 21, 2010, 23:59 GMT (this is the real deadline)

Exercise 4 requires material that will be covered in class on March 16. Note that on March 16 the course takes place in Buys Ballot Lab, room 205.

To submit your homework attach a sws, pdf or jpeg to an email and send it to `tanja@hyperelliptic.org`. You are encouraged to use latex for your presentation but a scan of a handwritten solution is also acceptable. Word documents will NOT be accepted. You may use a computer algebra system such as sage in your calculations.

1. Let k be a field with $\mathrm{char}(k) \neq 2$. The curve $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ is defined over k and is given by $aX^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2$, where $a, d \in k \setminus \{0\}$ and $a \neq d$.

   (a) Study C for singularities.

   (b) We define two sets of addition laws on C.

$$((X_1 : Z_1), (Y_1 : T_1)) + ((X_2 : Z_2), (Y_2 : T_2)) =$$
$$\begin{cases} \big((X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2 : Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2), \\ \quad (Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2 : Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2)\big) & \text{if defined,} \\ \big((X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1 : aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2), \\ \quad (X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1 : X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2)\big) & \text{if defined} \end{cases}$$

   In [2] it is shown that these two addition laws give the same result – if defined (a result is not defined if it contains $(0 : 0)$ as part because that is not a point in $\mathbb{P}^1$). For $k = \mathbb{F}_{11}$ and $a = 1, d = 4$ the points $P = ((2 : 1), (3 : 1))$ and $Q = ((10 : 1), (0 : 1))$ are on the curve. Compute $2P$ and $2P + Q$.

   (c) Using the points P and Q from the previous part, define the divisor $D = 2P + 5Q - 4((1 : 1), (0 : 1))$. Compute $\deg(D)$ and $2D$.

2. An attack is called a *generic attack* if it does not depend on the representation of the group (i.e. it works irrespective of whether the group is the multiplicative group of a finite field or the group of points on an Edwards curve). The Pohlig Hellman attack is one such generic attack which computes the discrete logarithm in a group by computing corresponding discrete logarithms in subgroups. Let $G = \langle g \rangle$ be the cyclic group generated by g, and let the group operation be given as multiplication. The task is to find k given $h \in G$ so that $h = g^k$; k is the discrete logarithm of $h \in G$ to the base g.

   Let $\mathrm{ord}(g) = n$ and let $\ell | n$. Then the element $g^{n/\ell}$ has order ℓ. To get information on k we can start by computing k modulo ℓ by computing $h^{n/\ell}$ and comparing the result

to $g^{n/\ell}, g^{2n/\ell}, g^{3n/\ell}, \ldots, g^{(\ell-1)n/\ell}$. If $k = k_1\ell + k_0$ then $h^{n/\ell} = g^{n/\ell(k_1\ell+k_0)} = g^{k_0 n/\ell}$, so this comparison will reveal k_0. If $\ell^2|n$ this process can be iterated by first computing $h' = hg^{-k_0}$, so that h' has discrete logarithm $k' = k_1\ell$ and then comparing $h'^{n/(\ell^2)}$ to $g^{n/(\ell^2)}, g^{2n/(\ell^2)}, g^{3n/(\ell^2)}, \ldots, g^{(\ell-1)n/(\ell^2)}$ to find k'_1 with $k' = k'_2\ell^2 + k'_1\ell$.

This process can be repeated with every factor ℓ_i of n. To retrieve k from the information $k \bmod \ell_i$ we can solve this system of modular congruences using the Chinese Remainder Theorem. For more details see e.g. [4] and [3].

This exercise is about the discrete logarithm problem in $\mathbb{F}_{41}$.

(a) Prove that the multiplicative order of 7 is 40. How many exponentiations are necessary for this?

(b) Show how the Pohlig-Hellman algorithm reduces the problem of computing m with $7^m = c$ to two smaller problems.

(c) Set up all preliminary work to solve $7^m = c$ in general, i.e. precompute the sets of powers of 7 to compare the target to.

(d) Solve $7^m = 29$ in this way.

3. For large groups it becomes cumbersome to enumerate all group elements to solve the individual discrete logarithms in the previous exercise. The Baby-Step Giant-Step attack and Pollard's rho attack are examples that run in time $O(\sqrt{\ell})$ in a group of order ℓ. Read [4] or [3] for details on these attacks.

(a) Use the Baby-Step Giant-Step attack to compute the discrete logarithm of $h = 57$ with base $g = 4$ in $\mathbb{F}^*_{107}$. You may use that the order of 4 is 53.

(b) Use Pollard's rho method with iteration function

$$r_{i+1} = \begin{cases} r_i g & r_i \equiv 0 \bmod 3 \\ r_i^2 & r_i \equiv 1 \bmod 3 \\ r_i h & r_i \equiv 2 \bmod 3 \end{cases}$$

and starting point $r_0 = g$ to compute the discrete logarithm of $h = 569$ with base $g = 4$ in $\mathbb{F}^*_{1019}$. You may use that the order of 4 is 509.

4. This exercise deals with elliptic curves.

(a) Let E/k be an elliptic curve over a field k and let E be given by a Weierstrass equation. Show how to find a function F so that the divisor of the form $Q - P_\infty$ in the class of $P_1 + P_2 + \cdots + P_5 - 5P_\infty, P_i \in E(k)$ can be computed in one reduction step. You may assume that the P_i are affine and in general position.

(b) Read the section on "Short normal forms and invariants" (pp.69 – 73) in [1]. Note that this chapter is currently available online. Use this to compute a short Weierstrass form for the elliptic curve $E/\mathbb{F}_7$ defined by $E : y^2 + xy + y = x^3 + 2x^2 + 4x + 5$. Note that you need not show that E is an elliptic curve.

References

[1] Roberto M. Avanzi, Henri Cohen, Christophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *The Handbook of Elliptic and Hyperelliptic Curve Cryptography*. (CRC Press 2005), http://www.hyperelliptic.org/HEHCC/

[2] Daniel J. Bernstein, Tanja Lange, *A complete set of addition laws for incomplete Edwards curves*, (ePrint archive 2009), http://eprint.iacr.org/2009/580

[3] Alfred Menezes, Paul van Oorschot, Scott Vanstone, *Handbook of Applied Cryptography*, (CRC Press 1996), http://www.cacr.math.uwaterloo.ca/hac

[4] Henk van Tilborg, *Fundamentals of Cryptology*, (Kluwer academic Publishers 2000), http://www.win.tue.nl/∼henkvt/cryptobook/cryptodict.pdf