Advanced Cryptography Exercises – Master SCCI

Vanessa Vitse

2013-2014

Exercise 1. A monomial order $\prec$ on $K[X_1, \ldots, X_n]$ is called an *elimination order* for $X_1, \ldots, X_k$ ($k < n$) if the following property holds:

$$\forall\, P \in K[X_1, \ldots, X_n],\ LM(P) \in K[X_{k+1}, \ldots, X_n] \Rightarrow P \in K[X_{k+1}, \ldots, X_n]$$

1. Show that this definition is equivalent to

$$\forall\, m_1 \text{ monomial } \in K[X_1, \ldots, X_k],\ \forall\, m_2 \text{ monomial } \in K[X_{k+1}, \ldots, X_n],\ m_2 \preccurlyeq m_1$$

2. Show that the lexicographic order is an elimination order for $X_1, \ldots, X_k$, for any k. Are the graded and reverse graded lex order elimination orders?

3. Let $\prec_1$, resp. $\prec_2$, be a monomial order on $K[X_1, \ldots, X_k]$, resp. $K[X_{k+1}, \ldots, X_n]$. Show that there exists on $K[X_1, \ldots, X_n]$ an elimination order for $X_1, \ldots, X_k$, which is equal to $\prec_1$, resp. $\prec_2$ when restricted to monomials in first k variables, resp. last $n - k$ variables.

Exercise 2. Let $\prec_{\mathbb{R}^n}$ be the lexicographical order on $\mathbb{R}^n$, i.e.

$$(a_1, \ldots, a_n) \prec_{\mathbb{R}^n} (b_1, \ldots, b_n) \Leftrightarrow \exists\, i \text{ s.t. } \begin{cases} a_1 = b_1 \\ \vdots \\ a_{i-1} = b_{i-1} \\ a_i < b_i \end{cases}$$

Let $M \in GL(n, \mathbb{R})$. We define on monomials in $X_1, \ldots, X_n$ the order $\prec_M$ by

$$X_1^{\alpha_1} \ldots X_n^{\alpha_n} \prec_M X_1^{\beta_1} \ldots X_n^{\beta_n} \quad \Leftrightarrow \quad M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \prec_{\mathbb{R}^n} M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

1. Show that $\prec_M$ is a total order, compatible with the multiplication of monomials, and give a condition on M for $\prec_M$ to be a monomial order.

2. Describe the monomial orders corresponding to the following matrices:

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \qquad M_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$M_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad M_5 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix} \qquad M_6 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -1 & -1 & -1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

3. Show that two matrices M and M' define the same order if

$$M = \begin{pmatrix} \lambda_{11} & 0 & \cdots & 0 \\ \lambda_{21} & \lambda_{22} & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ \lambda_{n1} & \lambda_{n2} & \cdots & \lambda_{nn} \end{pmatrix} M' \quad \text{where } \lambda_{ii} > 0 \ \forall\, i.$$

4. Give a necessary and sufficient condition on M for the corresponding monomial order to be *graded*, i.e. $m_1 \prec_M m_2$ as soon as the total degree of m_1 is smaller than the total degree of m_2.

5. It can actually be proved that for any monomial order $\prec$, there exists an invertible matrix M such that $\prec$ is equal to $\prec_M$. Using this result and the previous questions, describe all graded monomial order on $K[x, y, z]$ with $x \succ y \succ z$.

Exercise 3.

1. Compute the remainder of the given polynomial $f = x^7y^2 + x^3y^2 - y + 1$ in the division by the (ordered) set $F = \{xy^2 - x, x - y^3\}$, first with the graded lex order, then with the lex order. Repeat with the order of F reversed.

2. Same question with $f = xy^2z^2 + xy - yz$, $F = \{x - y^2, y - z^3, z^2 - 1\}$ and cyclic permutations of F.

3. Check your result using a computer algebra system.

Exercise 4. Let $f = x^3 - x^2y - x^2z + x$, $f_1 = x^2y - z$ and $f_2 = xy - 1$.

1. Using the graded lex order, compute r_1, resp. r_2, the remainder of f in the division by $\{f_1, f_2\}$, resp. $\{f_2, f_1\}$. The results should be different; where in the division algorithm did the difference occur?

2. Is $r = r_1 - r_2$ in the ideal $\langle f_1, f_2 \rangle$? If yes, express r as a combination with polynomial coefficients of f_1 and f_2. If no, explain why.

3. Compute the remainder of r in the division by $\{f_1, f_2\}$. Was it possible to predict the answer before doing the division?

4. Find another polynomial $g \in \langle f_1, f_2 \rangle$ such that the remainder in the division by $\{f_1, f_2\}$ is not zero.

Exercise 5.

1. Let $f_1 = xy^2 - xz + y$, $f_2 = xy - z^2$, $f_3 = x - yz^4$, and let $I = \langle f_1, f_2, f_3 \rangle$ be an ideal of $\mathbb{R}[x, y, z]$ endowed with the lex order. Find a polynomial $g \in I$ such that
$$LM(g) \notin \langle LM(f_1), LM(f_2), LM(f_3) \rangle.$$
2. More generally, suppose that $I = \langle f_1, \ldots, f_s \rangle$ is a polynomial ideal such that $\langle LM(f_1), \ldots, LM(f_s) \rangle \neq LM(I)$. Show that there exists $g \in I$ whose remainder in the division by $f_1, \ldots, f_s$ is not zero.

Exercise 6. Let $I \subset K[X_1, \ldots, X_n]$ be a principal ideal. Show that a finite subset $G \subset I$ is a Gröbner basis of I if and only if it contains a generator of I.

Exercise 7. Let $f_1 = x - z$, $f_2 = y - z$, and $I = \langle f_1, f_2 \rangle \subset K[x, y, z]$.

1. Show that $\{f_1, f_2\}$ is a Gröbner basis of I for the lex order.
2. Divide $g = xy$ by $\{f_1, f_2\}$ (in that order) and then by $\{f_2, f_1\}$. Are the remainders equal, and why? Are the "quotients" equal?

Exercise 8. Determine if the following sets are Gröbner bases of the ideal they generate (this may or may not require the use of a computer algebra system).

1. $\{x^2 - y, x^3 - z\}$ for the graded lex order.
2. $\{x^2 - y, x^3 - z\}$ for the lex order with $z \succ y \succ x$.
3. $\{xy^2 - xz + y, xy - z^2, x - yz^4\}$ for the standard lex order.

Exercise 9. Let G be a Gröbner basis of an ideal $I \subset K[X_1, \ldots, X_n]$ and let P, Q be two polynomials.

1. Show that $\overline{P}^G + \overline{Q}^G = \overline{P + Q}^G$.
2. Find an exemple such that $\overline{PQ}^G \neq \overline{P}^G \overline{Q}^G$. Prove that however $\overline{PQ}^G = \overline{\overline{P}^G \overline{Q}^G}^G$

Exercise 10. We recall that for $P \in K[X_1, \ldots, X_n]$ of total degree d, its homogenization is the polynomial
$$P^h = X_0^d \, P(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}) \in K[X_0, \ldots, X_n].$$
Reciprocally, for Q homogeneous in $K[X_0, \ldots, X_n]$, its deshomogenization is
$$Q^* = Q(1, X_1, \ldots, X_n) \in K[X_1, \ldots, X_n].$$
To a monomial order $\prec$ on $K[X_1, \ldots, X_n]$, we associate an order $\prec_h$ on $K[X_0, \ldots, X_n]$ defined by
$$m_1 \prec_h m_2 \iff \begin{array}{c} \deg m_1 < \deg m_2 \\ \text{or} \\ \deg m_1 = \deg m_2 \text{ and } m_1^* \prec m_2^* \end{array}$$

1. Show that $\prec_h$ is indeed a monomial order. What are the orders associated to lex and reverse graded lex?
2. Show that for any homogeneous polynomial $Q \in K[X_0, \dots, X_n]$,
$$LM_{\prec}(Q^*) = (LM_{\prec_h}(Q))^*$$
3. Let $f_1, \dots, f_r \in K[X_1, \dots, X_n]$, and let $\{g_1, \dots, g_s\}$ be a Gröbner basis of the ideal $\langle f_1^h, \dots, f_r^h \rangle \subset K[X_0, X_1, \dots, X_n]$ composed of homogeneous polynomials. Prove that $\{g_1^*, \dots, g_s^*\}$ is a Gröbner basis of $\langle f_1, \dots, f_r \rangle \subset K[X_1, \dots, X_n]$.

Exercise 11 . A polynomial $P \in K[X_1, \dots, X_n]$ is called symmetric if it is invariant under any permutation of the variables, i.e. $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n) \quad \forall\, \sigma \in \mathfrak{S}_n$. It is well-known that any symmetric polynomial can be expressed in terms of the elementary polynomials

$$e_1 = X_1 + \cdots + X_n, \qquad \dots \qquad e_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} X_{i_1} \dots X_{i_k}, \qquad \dots \qquad e_n = X_1 \dots X_n,$$

i.e. for any symmetric polynomial P, there exists a unique polynomial Q such that

$$P(X_1, \dots, X_n) = Q(e_1(X_1, \dots, X_n), \dots, e_n(X_1, \dots, X_n)).$$

1. Let P and Q be as above. We consider the ideal $I \subset K[X_1, \dots, X_n, Y_1, \dots, Y_n]$ spanned by $Y_1 - e_1(X_1, \dots, X_n), \dots, Y_n - e_n(X_1, \dots, X_n)$. Show that $P(X_1, \dots, X_n) - Q(Y_1, \dots, Y_n) \in I$ (hint: write $Q(Y_1, \dots, Y_n)$ as $Q(Y_1 - e_1 + e_1, \dots, Y_n - e_n + e_n)$).
2. Deduce from the previous question a method for computing Q, knowing P (hint: use elimination theory).

Exercise 12. Use Buchberger's algorithm to find a Gröbner basis for each of the following ideals, first with the lex, then the graded lex order, and compare your results. Give the corresponding minimal reduced basis in each case. You may use a computer algebra system to compute S-polynomials and remainders.

1. $I = \langle x^2 y - 1, x y^2 - x \rangle$.
2. $I = \langle x^2 + y, x^4 + 2x^2 y + y^2 + 3 \rangle$. What does the result indicate about the corresponding variety?
3. $I = \langle x - z^4, y - z^5 \rangle$.

Exercise 13 . (Buchberger first criterion.) Let f, g be two polynomials in $\mathbb{K}[X_1, \dots, X_n]$ such that $LM(f) \wedge LM(g) = 1$ (f and g are called *foreign polynomials*). Show that the remainder of $S(f, g)$ in the division by $\{f, g\}$ is zero (hint: write $LT(f)$ as $f - f'$ with $LM(f') \prec LM(f)$ and similarly for $LT(g)$). How can this be used to simplify Buchberger's algorithm?

Exercise 14 . Let I be an ideal of $K[X_1, \dots, X_n]$. The *staircase* of I (with respect to a monomial order $\prec$) is defined as the set of monomials m that are not in $LM(I)$:

$$Staircase(I) = \{m \in K[X_1, \dots, X_n] \text{ monomial } : \forall f \in I,\ LM(f) \nmid m\}.$$

1. Explain how to determine the staircase from a Gröbner basis of I. Draw a picture of the staircases of the ideals in Exercise 12. Explain how to determine from the staircase the number of elements in a minimal Gröbner basis.

2. Show that the quotient $R = K[X_1, \ldots, X_n]/I$ is a K-vector space. Prove that the (equivalence classes of the) monomials in the staircase of I form a basis of R as a K-vector space. Deduce that the cardinality of the staircase is independent of the monomial order $\prec$.

Exercise 15. (Ideals of dimension 0.)

1. Let I be an ideal of $K[X_1, \ldots, X_n]$. Show that the following properties are equivalent:

   (a) $K[X_1, \ldots, X_n]/I$ is a finite dimensional vector space.

   (b) The staircase of I contains a finite number of monomials.

   (c) $\forall\, i \in [1, n],\ \exists k \in \mathbb{N},\ X_i^k \in LM(I)$.

   (d) $V(I) \subset \bar{K}^n$ is a finite set.

   An (non-trivial) ideal is said to have dimension 0 if it satisfies these properties. You may have to use a weak form of the *Nullstellensatz*: if a polynomial f vanishes identically on an algebraic set $V(I) \subset \bar{K}^n$, then there exists $k \in \mathbb{N}^*$ such that $f^k \in I$.

2. Let V be a finite set in K^n such that no points of V have a common n-th coordinate. Show that the minimal reduced lex order Gröbner basis of the (zero-dimensional) ideal of V has the following form (*shape lemma* position):

$$\{X_1 - g_1(X_n), X_2 - g_2(X_n), \ldots, X_{n-1} - g_{n-1}(X_n), g_n(X_n)\}$$

   with $\deg g_i < \deg g_n$ for all $i < n$.

Advanced Cryptography Exercises – Master SCCI

Vanessa Vitse

2013-2014

1 Basic algebraic geometry

Exercise 1.

1. Construct $\mathbb{P}^2(\mathbb{F}(2))$ and list all its lines.
2. Compute the number of points of $\mathbb{P}^n(\mathbb{F}(q))$.
3. How many points are there in each projective line of $\mathbb{P}^n(\mathbb{F}(q))$? Compute the number of projective lines of $\mathbb{P}^n(\mathbb{F}(q))$.

Exercise 2. Let K be an algebraic closed field. What are the algebraic sets of K^1 ?

Exercise 3. Prove that an affine algebraic set $V \subset K^n$ is irreducible if and only if the ideal $I = \mathbb{I}(V)$ is prime in $K[X_1, \ldots, X_n]$.

Exercise 4. Let $\mathcal{C} = V(Y^2 - X^3 - X^2)$ an affine algebraic subset of K^2 and $\phi(X, Y) = X/Y$, $\psi(X, Y) = Y/(X+1)$. What can be said about φ, φ^2 and ψ at the points $P_1 = (0, 0)$ and $P_2 = (-1, 0)$.

Exercise 5. We consider the curve C of equation $x^4 + 2x^2y^2 + y^4 - x^3 + 3xy^2 = 0$.

1. Plot the curve (it has the polar equation $r = \cos(3\theta)$).
2. What (if any) are the singular points of C?
3. Show that the local ring at $(0, 0)$ is not principal.

Exercise 6. Let $P = (x_0, y_0)$ be a smooth point on an algebraic plane curve of equation $f(x, y) = 0$. We recall that the maximal ideal of the local ring at P is principal and is generated by $\{x - x_0, y - y_0\}$. Let $T(x, y) = (x - x_0)\frac{\partial f}{\partial x}(x_0, y_0) + (y - y_0)\frac{\partial f}{\partial y}(x_0, y_0)$, so that $T(x, y) = 0$ is the equation of the tangent at P.

1. Show that $ord_P(T) \geqslant 2$.
2. Let $(a, b) \in K^2 \backslash \{(0, 0)\}$ and $l(x, y) = a(x - x_0) + b(y - y_0)$ be such that the line of equation $l(x, y) = 0$ is not the tangent at P. Prove that l is an uniformizer at P (hint: show that $\langle x - x_0, y - y_0 \rangle = \langle T, l \rangle$).

Exercise 7. Let $\mathcal{C} : Y^2 = X^3 + X$. Compute the order of Y, X, $2Y^2 - X$ at the point $P = (0, 0)$.

Exercise 8.

1. Let D and D' be two divisors on an algebraic curve C. Show that if $D \sim D'$ then there is an isomorphism between $\mathcal{L}(D)$ and $\mathcal{L}(D')$.
2. Let D be a divisor such that $\deg D < 0$. Show that $\mathcal{L}(D) = \{0\}$.

Exercise 9. Let C be an algebraic curve.

1. Let $D \in Div(C)$ a divisor and P a point of C. Show that if the dimension of the vector space $\mathcal{L}(D)$ is finite, then $\mathcal{L}(D + (P))$ also has finite dimension and $\ell(D + (P)) \leqslant \ell(D) + 1$.
2. Use the result of the previous section to prove by induction that $\mathcal{L}(D)$ has finite dimension for any divisor D and give an upper bound on $\ell(D)$.

Exercise 10.

1. Show that the genus of $\mathbb{P}^1$ is equal to zero and that $\mathrm{Pic}^0(\mathbb{P}^1)$ is trivial.
2. Show that if $\mathcal{O}$ is a distinguished point of a curve $\mathcal{C}$ with genus g, then any divisor $D \in \mathrm{Pic}^0(\mathcal{C})$ can be written as $D \sim (P_1) + \cdots + (P_g) - g(\mathcal{O})$ for some points $P_1, \ldots, P_g \in \mathcal{C}$.

2 Elliptic and hyperelliptic curves

Exercise 11. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over an odd characteristic field such that $j(E) = 0$ (resp. $j(E) = 1728$). Show that E has sextic or cubic twists (resp. quartic twist).

Exercise 12. Let $\mathcal{H} : y^2 + h_0(x)y = h_1(x)$ be an imaginary hyperelliptic curve of genus g and $\mathcal{O}$ be the point at the infinity.

1. Check that the order of x and y at $\mathcal{O}$ are -2 and $-(2g + 1)$ respectively.
2. Show that $(P) + (\iota(P)) - 2(\mathcal{O})$ is principal.

Exercise 13. Let $\mathcal{H} : y^2 = x^5 - 1$ be a curve defined over $\mathbb{F}_3$. Check that $\mathcal{H}$ is a genus 2 hyperelliptic curve. Using Cantor's algorithm, show that $(x^2 - x + 1, -x + 1) + (x - 1, 0) \sim (x^2 - x - 1, x - 1)$.

Exercise 14. Show that it is possible to recover the classical elliptic curve law from Cantor's algorithm.

Exercise 15. Let $E : y^2 = x^3 + 77x + 28$ be an elliptic curve defined over $\mathbb{F}_{157}$. Apply Pohlig-Hellman reduction to compute the discrete logarithm of the point $Q = (2, 70)$ in base $P = (9, 115)$ (which has order $162 = 2 \cdot 3^4$).

Exercise 16. Let $\mathcal{H} : y^2 = x^7 + 4x^5 + 3x^3 + 4x^2 + 3x + 4$ be a genus 3 hyperelliptic curve defined over $\mathbb{F}_5$. We want to apply the index calculus method to solve discrete logarithms in the Jacobian of this curve using a smoothness bound B equal to 1 (this exercise requires the use of either Sage or Pari/GP on a computer).

1. Compute the set of $\mathbb{F}_5$-rational points of $\mathcal{H}$ and give a convenient factor basis for the index calculus.
2. Let $D_0 = (x^3 + 4x^2 + 3x + 3, x^2 + 2x + 2)$ and $D_1 = (x^3 + x^2 + 4x + 2, 2x^2 + x + 2)$ be divisors in the Jacobian of $\mathcal{H}$. Check that their order is 263.
3. Find relations and deduce the discrete logarithm of D_1 in base D_0.

3 Rational maps and morphisms between curves

Exercise 17. Let $E : Y^2Z = X^3 + X^2Z \subset \mathbb{P}^2$ be an elliptic curve and $\phi([X : Y : Z]) = [Y/X, 1] = [Y, X]$ and $\psi : \mathbb{P}^1 \to E$, $[S : T] \mapsto [S^2T - T^3 : S^3 - ST^2 : T^3]$ be two rational maps. Show that $\psi \circ \phi$ and $\psi \circ \phi$ are the identity wherever they are defined. Are ψ or ϕ morphisms?

Exercise 18. Let $\phi_1 : C_1 \to C_2$ and $\phi_2 : C_2 \to C_3$. Show that

$$e_{\phi_2 \circ \phi_1}(P) = e_{\phi_1}(P) \cdot e_{\phi_2}(\phi_1(P)).$$

Exercise 19. Let K be a field of characteristic different from 2 and 3, $E : y^2 = x^3 - x$ be an elliptic curve defined over K (with distinguished point $\mathcal{O}$ being the point at infinity) and $\phi : E \to \mathbb{P}^1$, $(x, y) \mapsto x$ be a morphism.

1. Compute the degree of the morphism ϕ.
2. What is the ramification index of ϕ at $P = (x, y)$ (consider the cases where $y = 0$ and $y \neq 0$)? at the point $\mathcal{O}$?
3. Same questions but with the morphism $\psi : E \to \mathbb{P}^1$, $(x, y) \mapsto y$ instead of ϕ.

Exercise 20. Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$, $z \mapsto z^n$ be a morphism.

1. Compute the degree of the morphism ϕ.
2. What is the ramification index of ϕ at ∞? at $a \neq \infty$ (consider the cases where $a = 0$ and $a \neq 0$)?

Exercise 21. Let C_1, C_2 be two smooth curves, D_1, D_2 two divisors of $\mathrm{Div}(C_1)$ and $\mathrm{Div}(C_2)$ respectively, f a function of C_2 and $\phi : C_1 \to C_2$ a morphism. Show that

1. $\deg(\phi^*(D_2)) = \deg(D_2) \deg \phi$,
2. $\deg(\phi_*(D_1)) = \deg(D_1)$,
3. $\phi_* \circ \phi^*(D_2) = (\deg \phi) D_2$,
4. $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$,
5. $\mathrm{div}\, f = f^*((0) - (\infty))$, and in particular $\deg \mathrm{div}\, f = 0$.

4 Pairings

Exercise 22. Let $E|\mathbb{F}_q$ be an elliptic curve such that $|E(\mathbb{F}_q)| = q-1$, and assume that $q-1$ is almost prime, i.e. is of the form cm where m is a prime and c is a small cofactor. Show that there is a non-degenerate bilinear *self-pairing* $G_1 \times G_1 \to G_2$ where G_1 is a cyclic order m subgroup of E and G_2 is a cyclic order m subgroup of $\mathbb{F}_q^*$.

Exercise 23. Let $P, Q \in E[m]$ and f_P, f_Q two functions such that $\operatorname{div} f_P = m(P) - m(O)$ and $\operatorname{div} f_Q = m(Q) - m(O)$. Show that

$$e_m(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \frac{f_Q(-S)}{f_Q(P-S)}$$

for any $S \notin \{O, P, -Q, P-Q\}$ (hint: apply the definition with $D_P = (P-S) - (-S)$ and $D_Q = (Q) - (O)$, and observe that $D_P = \tau_S^*((P) - (O))$).

Exercise 24. Let $E : y^2 = x^3 + 7$ over $\mathbb{F}_{13}$.

1. Compute the cardinality of $E(\mathbb{F}_{13})$ and the largest prime m such that $m|E(\mathbb{F}_{13})$. Deduce the corresponding embedding degree k.
2. Let $P = (11, 5) \in E$, compute $f_P \in \mathbb{F}_{13}(E)$ such that $\operatorname{div} f_P = m(P) - m(\mathcal{O})$ with Miller's algorithm.
3. Let $Q = (4, 7t + 10) \in E(\mathbb{F}_{13^2})[7]$ where $t \in \mathbb{F}_{13^2}$ is such that $t^2 + t + 1 = 0$. Compute the Tate pairing evaluated at P and Q.

Exercise 25. Show that if E is defined over a prime field $\mathbb{F}_p$ with $p \geqslant 5$ and is supersingular then $|E(\mathbb{F}_p)| = p + 1$.

5 Point counting

Exercise 26. Let $E_{|\mathbb{F}_q}$ be an elliptic curve such that $j(E) \notin \{0, 1728\}$ (and $p \geqslant 5$), and denote by t its trace, so that $|E(\mathbb{F}_q)| = q + 1 - t$. Let E' be the quadratic twist of E, i.e. E' is isomorphic to E over $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$. Show that the cardinality of $E'(\mathbb{F}_q)$ is $q + 1 + t$.

Exercise 27. How many Koblitz curves are there over $\mathbb{F}_{2^{131}}$? What are their cardinalities?

Exercise 28. Devise a point counting algorithm whose complexity is in $\tilde{O}(q)$ operations in $\mathbb{F}_q$.

Exercise 29. Assume that the cardinality of $E(\mathbb{F}_q)$ is a prime. Devise a (probabilistic) point counting algorithm whose complexity is in $O(q^{1/2})$ operations in $\mathbb{F}_q$.

Exercise 30. Assume that the cardinality of $E(\mathbb{F}_q)$ is a prime. Devise a (probabilistic) point counting algorithm whose complexity is in $O(q^{1/4})$ operations in $\mathbb{F}_q$ (hint: think baby-step giant-step). Can it be adapted to the case where $E(\mathbb{F}_q)$ is only assumed to be cyclic? More difficult: can it be adapted to the general case?

6 Point counting

Exercise 31. Let ℓ be an Atkin prime for an elliptic curve E, and $\lambda \in \mathbb{F}_{\ell^2}$ a root of the (irreducible) characteristic polynomial $X^2 + t_\ell X + q_\ell \in \mathbb{F}_\ell[X]$. We keep the notations introduced above.

1. Show that if r is even, then λ^r is not a square in $\mathbb{F}_\ell$.
2. Show that if $\ell \equiv 1 \bmod 4$ and q is a quadratic residue modulo ℓ, then r is odd. How can this be used to speed up the SEA algorithm?
3. Assume that r is even and $\ell \equiv 3 \bmod 4$. Explain how to tell if $\lambda^r = q_\ell^{r/2}$ or $\lambda^r = -q_\ell^{r/2}$. Show that $s = r/2$ in the first case and $s = r$ in the second, and that this gives $\varphi(r)$ choices for t_ℓ in both cases.
4. Prove the formula: $(-1)^{(\ell+1)/r} = \left(\frac{q}{\ell}\right)$