Summer School – Number Theory for Cryptography, Warwick
Exercises for lectures by D. J. Bernstein and T. Lange, June 26, 2013

1. Horner's rule, given α and given $n \geq 1$ coefficients $f_0, f_1, \ldots, f_{n-1}$ of a polynomial $f = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}$, computes $f(\alpha)$ using $n-1$ multiplications and $n-1$ additions. How quickly, starting from the same input, can you compute the vector $(f(\alpha), f(-\alpha))$?

2. The following recursive "binary" strategy constructs nP by additions starting from P, where n is a positive integer: double $(n/2)P$ if n is even; add P to $(n-1)P$ if n is odd. This construction uses $O(\lg n)$ additions, typically around $1.5 \lg n$ additions, where $\lg = \log_2$.

   Present an explicit strategy that uses only $(1 + (1 + o(1))/\lg\lg n)\lg n$ additions as $n \to \infty$. (Brauer, 1939. Erdős showed in 1960 that $1 + o(1)$ is optimal for most values of n.)

3. A more general "binary" strategy constructs $n_1 P_1 + \cdots + n_k P_k$, starting from $P_1, \ldots, P_k$, using $O(k \lg n)$ additions if $n_1, \ldots, n_k$ are all bounded by n. Show that one can beat $k \lg n$ by *more* than a constant factor when $k \to \infty$ and $n \to \infty$. (Straus, 1964.)

4. Assume that $d = 1 - s^2 \notin \{0, 1\}$ and $S = (1-s)/(1+s)$ and $D = S^2$.

   (a) Show that $(x, y) \mapsto (X, Y)$ defined by $X = (1+s)xy$ and $Y = (1-(1+s)x^2)/(1-(1-s)x^2)$ is a 2-isogeny from the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ to the Edwards curve $X^2 + Y^2 = 1 + DX^2Y^2$.

   (b) Show that the dual isogeny is $(X, Y) \mapsto (x, y)$ defined by $x = (1-Y^2)/(X(1-SY^2))$ and $y = (1+S)Y/(1+SY^2)$, i.e., that doubling is the composition of this map and the previous map.

   (c) Can doubling also be decomposed this way in the non-elliptic case $d = 0$?

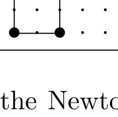
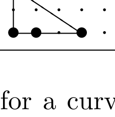
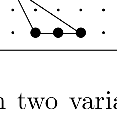
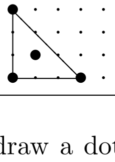
5. For distinct positive real numbers (a, b) define $A = (a+b)/2$ and $B = \sqrt{ab}$. Then the iteration $(a, b) \mapsto (A, B)$ converges rapidly to (M, M), where M is Gauss's "arithmetic-geometric mean" of (a, b).

   (a) Show that taking $s = B/A$ in the previous exercise implies that d is a function of (a, b) and D is the same function of (A, B), so $(a, b) \mapsto (A, B)$ induces a map $d \mapsto D$.

   (b) Show that the iteration $d \mapsto D$ converges. What does the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ converge to?

   (c) Apply the corresponding sequence of 2-isogenies to a point (x, y), obtaining a sequence of points on various Edwards curves. Does this sequence converge?

6. Here are four examples (under suitable nondegeneracy assumptions) of elliptic-curve shapes and their Newton polygons:

Edwards	short Weierstrass	Montgomery	Hessian
$x^2 + y^2 = 1 + dx^2y^2$	$y^2 = x^3 + ax + b$	$y^2 = x^3 + ax^2 + x$	$x^3 + y^3 + 1 = 3dxy$
			

   To draw the Newton polygon for a curve $f = g$ in two variables x, y, draw a dot at each (i, j) such that the coefficient of x^iy^j in $f - g$ is nonzero, and then draw the convex hull of the dots.

   Each of these elliptic-curve polygons has exactly one interior lattice point. More generally, Baker observed in 1893 that (under suitable nondegeneracy assumptions) the genus of a plane curve is the number of interior lattice points in the Newton polygon of the curve.

(a) What is the effect on the Newton polygon of replacing $f - g$ with $x^a y^b (f - g)$, where a and b are integers? What is the effect on the curve?

(b) What about replacing $f - g$ with $f(x^a y^b, x^c y^d) - g(x^a y^b, x^c y^d)$ where a, b, c, d are integers with $ad - bc \in \{1, -1\}$? Why is the $\{1, -1\}$ restriction important?

(c) There are infinitely many Newton polygons having exactly one interior lattice point. However, there are only finitely many classes of these polygons modulo the transformations in (a) and (b). What are elliptic-curve shapes in each of those classes?

See "The Newton polygon of plane curves with many rational points" by Beelen and Pellikaan (2000) for a precise statement and proof of the genus formula. See "Lattice polygons and the number 12" by Poonen and Rodriguez-Villegas (2000) for more context.

7. The equation $E : y^2 + xy = x^3 + x^2 + 1$ defines an elliptic curve over $\mathbb{F}_2$. Construct $\mathbb{F}_4$ as $\mathbb{F}_4 \cong \mathbb{F}_2[z]/(z^2 + z + 1)\mathbb{F}_2[z]$.

   (a) Find all points on this curve over $\mathbb{F}_2$.

   (b) Find all points on this curve over $\mathbb{F}_4$.

   (c) $P = (1, z)$ is a point on this curve. Compute $3P$.

   (d) Compute the number of points over $\mathbb{F}2^{131}$

   (e) Let $Q = (x, y)$ be a point on $E(\mathbb{F}_{2^n})$ for some integer n. Show that $\sigma(Q) = (x^2, y^2)$ is in $E(\mathbb{F}_{2^n})$.