Cryptography I, homework sheet 12

Due: 13 January 2012, 10:45

For these exercises you'll need to compute modulo some small numbers. Of course you can ask your computer for help but this type of computations is what you'll need to be able to do quickly in the exam; so this might be a good training opportunity.
Montgomery curves are explained below. An Edwards curve is a twisted Edwards curve with $a = 1$.

1. Find all (affine) points (x_1, y_1) on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$.
2. Verify that $P = (6, 3)$ and $Q = (3, 7)$ are on the curve. Compute $R = [2]P + Q$ in affine coordinates.
3. Compute a birationally equivalent Montgomery curve; state the birational equivalence ϕ from the Edwards curve to the Montgomery curve and the inverse map ψ.
4. Compute $\phi(P)$ and $\phi(Q)$ and $S = [2]\phi(P) + \phi(Q)$ on the Montgomery curve.
5. Verify that $\psi(S) = R$.

Montgomery curves:
This is another way of writing elliptic curves, which is very close to Weierstrass curves:

$$Bv^2 = u^3 + Au^2 + u,$$

where $A \neq \{-2, 2\}, B \neq 0$. For two points $P_1 = (u_1, v_1)$ and $P_2 = (u_2, v_2)$ with $u_1 \neq u_2$ define $\lambda = \frac{v_1 - v_2}{u_1 - u_2}$; for $P_1 = P_2 = (u_1, v_1)$ with $u_1 \neq 0$ define $\lambda = \frac{3u_1^2 + 2Au_1 + 1}{2Bv_1}$. Then $P_1 + P_2 = (u_3, v_3)$ with $u_3 = B\lambda^2 - A - u_1 - u_2$ and $v_3 = \lambda(u_1 - u_3) - v_1$. The curve has a special point P_∞ like a Weierstrass curve; it is the neutral element of the group. The rules are $P_1 + P_\infty = P_\infty + P_1 = P_1, (u_1, v_1) + (u_1, -v_1) = P_\infty$.

Each twisted Edwards curve $E_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2$ can be mapped to a Montgomery curve $E_{M,A,B} : Bv^2 = u^3 + Au^2 + u$ and vice versa. The map ψ is given by fractions of polynomials and works for almost all points on the Edwards curve and its inverse works for almost all points on the Montgomery curve; and it holds that $\psi(P + Q) = \psi(P) + \psi(Q)$. Such a map is called a birational map and the resulting curves are called *birationally equivalent*. Put $A = 2\frac{a+d}{a-d}$ and $B = \frac{4}{a-d}$, then the point (x, y) on $E_{E,a,d}$ corresponds to the point $(\frac{1+y}{1-y}, \frac{1+y}{(1-y)x})$ on $E_{M,A,B}$; the inverse map is given by $(u, v) \mapsto (\frac{u}{v}, \frac{u-1}{u+1})$. If you start with the Montgomery curve $E_{M,A,B}$ the curve parameters of the twiwsted Edwards curve are given by $a = \frac{A+2}{B}$ and $d = \frac{A-2}{B}$.

Some points cannot be mapped this way, in particular $(0, \pm 1)$ on the Edwards curve, and $P_\infty, (0, 0)$ and potentially 2 more points on the Montgomery side. To make the group law fit one can associate the neutral elements $(0, 1)$ and P_∞ and the points of order 2, namely $(0, -1)$ and $(0, 0)$.