Cryptography I, homework sheet 12

Due: 14 January 2011, 10:45

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 $\psi(S) = R$.