PROBLEMS ON FUNCTION FIELD ARITHMETIC, DISCRETE LOG COMPUTATION, AND CRYPTOGRAPHY

MIKE JACOBSON, JR.

(1) **Correctness of divisor addition**: Prove that the addition formula for divisors on a hyperelliptic curve is correct.

(2) **Simplification of addition formula**: Prove that, when adding divisors on a hyperelliptic curve given in Mumford representation, we can replace the expression for v with

$$v = v_2 + U\frac{u_2}{s}$$

where $U \equiv b(v_1 - v_2) + cw_2 \pmod{u_1/s}$.

(3) **Geometric method**: Given a genus 2 hyperelliptic curve over a field K given by $y^2 = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$, show how to add two divisors $D_1 = (u_1, v_1)$ and $D_2 = (u_2, v_2)$ using the geometric method (i.e., *without* converting to formal sums of points representations). Your method should involve solving a 2×2 linear system of equations over K to find the coefficients of the degree 3 polynomial $\ell(x)$ that interpolates the finite points in the supports of D_1 and D_2. For simplicity, you may assume that these supports yield four distint points.

(4) **Infrastructure computation**. Consider the split genus two hyperelliptic curve defined by $C : y^2 = x^6 + x^4 + 2x^3 + x^2 + x + 1$ over $\mathbb{F}_5$.
   (a) Enumerate all infrastructure ideals of C (use Mumford representation).
   (b) Compute the regulator and fundamental unit (product of the z_i obtained from each perturbed reduction step) of the function field of C.

(5) **Computing discrete logarithms**
   (a) Consider the elliptic curve E given by

$$E : y^2 = x^3 + 436743x + 67111 \text{ over } \mathbb{F}_{1048583} \ .$$

   The number of points on E is 1049580. Find the discrete logarithm $\log_P(Q)$ for $P = (169541 : 556330)$ and $Q = (858751 : 762468)$ using the Pohlig-Hellman attack. (Hint: use Sage or Magma to do the curve arithmetic.)

   (b) **Computing discrete logarithms**: Consider the elliptic curve E given by

$$E : y^2 = x^3 + 900410x + 465299 \text{ over } \mathbb{F}_{1048583} \ .$$

   The number of points on this curve is 1049623. Find the discrete log problem $\log_P(Q)$ for $P = (815314 : 582035)$ and $Q = (67861 : 1005415)$ using any Pollard-rho. (BONUS: try it with index calculus!).

(6) **DSA**: In the DSA signature scheme, show why k must be unpredictable (random).

(7) **DSA**: In the DSA signature scheme, show why k must never be re-used for a second signature.

Date: June 2, 2016.