18.782 Introduction to Arithmetic Geometry **Fall 2013**
Problem Set #1 **Due: 09/17/2013**

Description

These problems are related to the material covered in Lectures 1-2. I have made every effort to proof-read these problems, but there are may be errors that I have missed. The first person to spot each error will receive 1-5 points of extra credit on their problem set, depending on the severity of the error.

The problem set is due before the start of class (2:30 pm) on 09/17/2013 and are to be submitted electronically as a pdf-file e-mailed to drew@math.mit.edu. You can use the latex source for this problem set as a template for writing up your solutions; be sure to include your name in your solutions (you can just replace the due date in the header with your name). Don't forget to do the last problem, which is a survey whose results will help to shape future problem sets and lectures.

Problem 1. Smooth conics (10 points)

Recall that a conic is a plane projective curve of degree 2. Let C/k be a geometrically irreducible conic over a field whose characteristic is not 2. Prove that C must be smooth (non-singular).

Problem 2. Plane cubics that define elliptic curves (30 points)

Show that over a field k of characteristic not 2, 3 (and for part (b), not 7), each of the following irreducible cubic curves C/k with a rational point P defines an elliptic curve that can be put in the form

$$y^2z = x^3 + Axz^2 + Bz^3$$

via a change of variables that takes the point P to the point $(0 : 1 : 0)$.

(a) $C\colon X^3 + Y^3 + Z^3 = 0, \quad P = (1 : -1 : 0).$

(b) $C\colon X^3 + Y^3 + Z^3 + XYZ = 0, \quad P = (1 : 0 : -1).$

Be sure to verify that the curves are smooth (but you can take it is as given that they are irreducible and have genus 1).

Problem 3. Rational points on conics (60 points)

In Lecture 2 we reduced the problem of finding a rational point on an irreducible conic over $\mathbb{Q}$ to the problem of finding an integer solution (x_0, y_0, z_0) to the equation

$$x^2 - dy^2 = nz^2, \qquad (1)$$

where d and n are positive square-free integers. We solved (1) using Legendre's method of descent, which can be described as a recursive algorithm $\textsc{Solve}(d, n)$. To facilitate the recursion, we let d and n also take negative square-free values.

$\textsc{Solve}(d, n)$

1. If $d, n < 0$ then **`fail`**.
2. If $|d| > |n|$ then let $(x_0, y_0, z_0) = \textsc{Solve}(n, d)$ and return (x_0, z_0, y_0).
3. If $d = 1$ return $(1, 1, 0)$; if $n = 1$ return $(1, 0, 1)$; if $d = -n$ return $(0, 1, 1)$.
4. If $d = n$ then let $(x_0, y_0, z_0) = \textsc{Solve}(-1, d)$ and return (dz_0, x_0, y_0).
5. If d is not a quadratic residue modulo n then **`fail`**.
6. Let $w^2 \equiv d \bmod n$, with $|w| \le |n|/2$, and set $x_0 = w, y_0 = 1$ so that $x_0^2 \equiv dy_0^2 \bmod n$.
7. Let $t_1 t_2^2 = (x_0^2 - dy_0^2)/n$ with t_1 square-free, let $(x_1, y_1, z_1) = \textsc{Solve}(d, t_1)$, and return $(x_0 x_1 + dy_0 y_1, x_0 y_1 + y_0 x_1, t_1 t_2 z_1)$.

Your task is to implement $\textsc{Solve}$ and use it to find rational points on a conic.

(a) Let a and b be the first two primes greater than your MIT ID, and let $-c$ be the least prime greater than b for which $-bc$, $-ac$, and $-ab$ are squares modulo a, b, and c, respectively. Use $\textsc{Solve}$ to find an integer solution (x_0, y_0, z_0) to

$$ax^2 + by^2 + cz^2 = 0. \tag{2}$$

Have $\textsc{Solve}$ print out the values (d, n) just before step 1 so that you can see how the descent progresses. Include a copy of this output, along with the values of a, b, and c, as well as the final solution (x_0, y_0, z_0) in your answer. You do not need to include your code (but you are welcome to if you wish).

Tip: In `sage` you can use `m=Integers(n)(d)` to obtain d as an element m of the ring $\mathbb{Z}/n\mathbb{Z}$, and then use `m.is_square()` to check whether m is a square. If it is, you can then use `w=m.sqrt().lift()` to get a square-root of m and lift it to an integer w in the interval $[0, n-1]$ (you may then need to subtract n from w in order to ensure that $|w| \le |n|/2$).

The solution returned by $\textsc{Solve}$ is typically much larger than necessary. As noted by Cremona and Rusin [1], the algorithm can be easily improved by modifying step 6 so that it chooses a solution (x_0, y_0) to the congruence $x_0^2 \equiv dy_0^2 \bmod n$ that minimizes $x_0^2 + |d|y_0^2$. This is achieved by finding a shortest integer vector (u_0, v_0) that minimizes the $\mathbb{Z}^2$-norm

$$\|(u, v)\|^2 = (wu + nv)^2 + |d|u^2,$$

where w, d, and n are as in step 6. One can then use $x_0 = u_0 w + v_0 n$ and $y_0 = u_0$. To find the vector (u_0, v_0), apply the standard 2-dimensional lattice reduction algorithm to the basis $\mathcal{B} = \{(1, 0), (0, 1)\}$: iteratively shorten the longer of the two vectors in $\mathcal{B}$ (where length is measured by the norm $\|\cdot\|$), by adding or subtracting copies of the shorter vector until no further improvement is possible.

(b) Repeat part (a) using a modified version of $\textsc{Solve}$ that minimizes $x_0^2 + |d|y_0^2$ as above.

(c) Using your answer from (b), parameterize the solutions to (2) and find 2 more projectively inequivalent solutions that are also inequivalent under sign changes.

Problem 4. Survey

Complete the following survey by rating each of the previous problems on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Novelty
9/5	Introduction			
9/10	Rational points on conics			
9/12	Finite fields			

Feel free to record any additional comments you have on the problem sets or lectures; in particular, how you think they might be improved.

References

[1] J.E. Cremona and D. Rusin, *Efficient solution of rational conics*, Mathematics of Computation **72** (2003), 1417–1441.