Elliptic Curves and Modular Forms (Master)
Wintersemester 2017/18

JProf. Dr. Simon Lentner
Algebra and Number Theory
FB Mathematik, Universität Hamburg

Sheet 1

In this exercise sheet we study in the much easier case of conic sections (genus 0) some of the number theory and analysis, as it will later appear in our lecture for elliptic curves (genus 1).

Problem 1 (1+1+3+1+1 Points)

Consider the following Pell equation for given $D \in \mathbb{Z}\backslash\{0\}$

$$x^2 - Dy^2 = 1, \qquad x, y \in \mathbb{Z}$$

a) Find the smallest two integral solutions (up to signs) for $D = 7$.

b) Find all integral solutions of all cases $D < 0$.

c) Prove directly that for solutions (x_1, y_1) and (x_2, y_2) also the following is a solution

$$(x_1x_2 + Dy_1y_2, x_1y_2 + y_1x_2)$$

Prove that this composition endows the set of solutions with a group structure. Calculate another solution for $D = 7$.

d) Show that any solution gives an invertible element (unit) in $\mathbb{Z}[\sqrt{7}]$.

e) Which group is generated for $D = 7$ by the solutions you obtained above (including all possible signs)? Find also the group of solutions for $D < 0$.

Problem 2 (3 Points)

Show with elementary considerations, that all Pythagorean triples

$$x^2 + y^2 = z^2 \qquad x, y, z \in \mathbb{N}$$

are precisely of the form $(x, y, z) = (2st, s^2 - t^2, s^2 + t^2)$ for $s, t \in \mathbb{N}$ or they are common multiples thereof (ax, ay, az).

Hint: First check pairwise common divisors and divisibility by 2.

Problem 3 (1+2+1+1 Point)

We wish to parametrize rational solutions of $x^2 - Dy^2 = 1$ for any $D \neq 0$.

a) Prove that the expression

$$(x, y) = \left(\frac{1 + Dt^2}{1 - Dt^2}, \frac{2t}{1 - Dt^2}\right)$$

produces rational solutions for this equation

b) If you take on the other hand the following obvious parametrization, what is t?

$$(x, y) = \left(\cos(\phi\sqrt{-D}),\ \sin(\phi\sqrt{-D})/\sqrt{-D}\right)$$

c) For $D = +1$ explicitly rewrite this parametrization in terms of trigonometric hyperbolic functions.

d) What is the group structure on this set of solutions under the composition in Problem 1?

Problem 4 (2+1+2 Points)

We wish to find a parametrization of solutions of $x^2 - Dy^2 = 1$ as follows: Suppose $y(\phi)$ is a function such that the differential equation holds

$$y'(\phi)^2 - Dy(\phi)^2 = 1$$

a) Show that inverse function $y^{-1}(z)$ is given by the integral

$$y^{-1}(a) = \int_0^a \frac{1}{\sqrt{1 + Dz^2}}\, \mathrm{d}z + C$$

up to an arbitrary integration constant C.
(This is a general technique for first order differential equations without explicit ϕ-dependence, somtimes called separation of variables)

b) Calculate this integral and the function $y(\phi)$ explicitly using trigonometric substitution.

c) Calculate the integral again using the rational substitution $z(t) = \frac{2t}{1-Dt^2}$ from Problem 3. .

You can think about how the periodicity of sine follows in this approach using complex analysis.