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

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

Sheet 3

Problem 1 (2+2 Points)

a) Determine the points of order 2 in the group $\mathbb{C}/L$ and their image under the isomorphism Φ to the group of solutions of the projective completion of the elliptic curve $Y^2 = 4X^3 - g_2X - g_3 = 4(X - e_1)(X - e_2)(X - e_3)$.

Give also a geometric interpretation with respect to the geometric group law on the typical graph of an elliptic curve.

b) Express $\wp(2z)$ as a rational function of $\wp(z)$. The denominator determines again the points of order 2.

Problem 2 (2 Points)

Prove from the addition theorem that $e_1+e_2+e_3 = 0$ and thus $4(x-e_1)(x-e_2)(x-e_3)$ has vanishing quadratic term for any lattice L.

Problem 3 (3+2+3 Points)

a) For our favourite elliptic curve $Y^2 = X^3 - n^2X$ (square lattice) give by geometric reasoning a rational expression for the composition $(x_{1+2}, y_{1+2}) = (x_1, y_1) * (x_2, y_2)$ of two solutions as rational functions in x_1, y_1, x_2, y_2. Your answer should consist of several cases. *Remark: This works similarly for any elliptic curve. One could also deduce this formula from the addition theorem.*

b) Show from this that any "double solution" $(x_1, y_1) * (x_1, y_1)$ of a rational solution gives either the infinite point (for the trivial points of order 2 in Problem 1) or it gives solutions (x_{1+1}, y_{1+1}) where x_{1+1} is a rational square with even denominator, hence solutions to the congruent number problem. *Remark: We shall later see, that this is if-and-only-if.*

c) For $n = 5$ and $n = 7$ (Euler) guess an integral solution to the elliptic curve (which is not of order 2). Then calculate the double of this solution and reverse our initial steps to obtain a right triangle solving the congruent number problem.

Hint: 141052024 *is divisible by* 674.

Problem 4 (2+2+2 Points)

a) Determine the finite order of the point $(2, 4)$ on the elliptic curve $y^2 = x^3 + 4x$. We found this solution from the lemniscate solution $(sl(\pm K), sl'(\pm K)) = (\pm 1, 0)$ on $Y^2 = 1 - X^4$.

b) For our favourite elliptic curve $y^2 = x^3 - n^2 x$ with n squarefree show that there are no rational points of order 4 except the trivial points of order 2 (Problem 1).

c) Determine the group of rational solutions of the elliptic curve $y^2 = x^3 - 432$ (hexagonal lattice) using the substitution $(x, y) = (12/(u+v), 36(u-v)/(u+v))$ and Fermat's last theorem for $n = 3$.