MasterMath 2007-2008 // Version 2

Exercise Sheet on Elliptic Curves

1. Diophantus writes in Lemma VI.12 of the *Arithmetica* that if $A+C$ is a square, then $Ax^2+C=y^2$ has infinitely many rational solutions. Give all these solutions in parametric form.

2. Prove: on a nondegenerate conic with a rational point, the set of rational points is dense in the set of real points of the conic.

3. Prove that the point $Q=\left(\left(\frac{41}{7}\right)^2, \frac{720\cdot 41}{7^3}\right)$ on the curve $E : y^2=x^3-31^2\,x$ cannot be written as $2P$ for some $P\in E(\mathbf{Q})$. What is the smallest field k such that such a P exists with $P\in E(k)$?

4 Diophantus asked: given a number, such as 6, divide this number into two parts, such that the product of the parts is a cube minus its root. He means the following: if y is one of the "parts", and x is the "root", find (x,y) rational numbers such that $y(6-y)=x^3-x$. This has a trivial solution $P=(-1,0)$. Find a non-trivial solution by computing $2P$. Transform the equation to Weierstrass form, and indicate what the points corresponding to P and $2P$ are.

5. Define a "new" addition on a plane elliptic curve as follows: fix a point $O\in E$ and fix three points C_1,C_2,C_3 on E. For $P,Q\in E$, define $P*Q$ to be the sixth intersection point of the unique conic through the five points C_1,C_2,C_3,P and Q with E, and define $P+Q:=O*(P*Q)$. Investigate the dependence of $P+Q$ on the points C_1,C_2,C_3. What happens if those points are collinear? Can you make such a construction where you fix more than three points and consider the unique curve of a certain degree through those points and P and Q, to give a unique further intersection point with E that you call $P*Q$?

6. The Lemniscate of Bernoulli is a plane curve in the (x,y)-plane with equation $r^4+r^2-2x^2$, with $r^2=x^2+y^2$. Draw a picture of the Lemniscate. Fagnano has proven the following: Let $s(r_0)$ denote the arc length on the lemniscate from the point $r=0$ to the point $r=r_0$. Then $s(r)=2s(u)$ is equivalent to

$$r^2=\frac{4u^2(1-u^4)}{(1+u^4)^2}.$$

Show that this implies the following: given a point on the lemniscate, there exists a construction with ruler and compass only of (1) a point that has exactly the double arc length of the given point from the initial point $r=0$; (2) a point that has exactly half the arc length of the given point from the initial point $r=0$. Study the Galois group of the polynomial satisfied by u for a fixed choice of r.

7. Prove that an N-torsion point of an elliptic curve over a field K is always defined over a finite field extension of K.

8. Prove: the cubic Fermat equation $x^3+y^3=z^3$ is an elliptic curve E equivalent to Weierstrass form $y^2=x^3-432$.

9. Fermat asked the following question in a letter to Mersenne: find three coprime positive integers (X,Y,Z) that are sides of a right angled triangle, such that the hypothenuse of the triangle, and the sum of the other two sides are both squares. In formulas: $X^2+Y^2=Z^2, Z=b^2, X+Y=a^2$. Transform this into an elliptic curve.

10. An integer is called *congruent* if it is the surface of a right angled triangle with rational sides. For example, 6 is congruent, since it is the surface of a triangle with sides $(3,4,5)$. Fermat proved that 1, 2 and 3 are not congruent, an Fibonacci proved that 5 is congruent via $(3/2,20/3,41/6)$. For n square-free, one can show that the following statements are equivalent: (a) n is congruent, i.e., $n=ab/2$ for $a^2+b^2=c^2$; (b) in an arithmetic sequence with difference n, there are three consecutive squares; (c) There is a rational point on the elliptic curve $y^2=x^3-n^2x$ different from $(0,0)$ and $(\pm n,0)$.

11. For which positive integers m,n is the sum of the first m integers equal to the sum of the first n squares? Convert this problem into finding the positive integral points on a certain elliptic curve.