Wolfgang K. Seiler
Tel. 2515

A5, C201

19. November 2013

10. Übungsblatt Elliptische Kurven

Aufgabe 1: *(6 Punkte)*
E sei modulo 35 gegeben durch die Gleichung $y^2 = x^3 + x + 3$. Faktorisieren Sie 35, indem Sie das Vierfache des Punktes $(1,4)$ berechnen!

Aufgabe 2: *(8 Punkte)*
E sei in der affinen Ebene über $\mathbb{Z}/29\mathbb{Z}$ gegeben durch die Gleichung $y^2 = x^3 + x + 5$.

a) Zeigen Sie, daß der Punkt $(3,8)$ der zugehörigen projektiven Kurve die Ordnung 15 hat.

b) Folgern Sie daraus, daß 29 eine Primzahl ist.

Aufgabe 3: *(3 Punkte)*
p sei eine Primzahl und g eine primitive Wurzel modulo p, d.h. alle Elemente von $\mathbb{F}_p^\times$ lassen sich als Potenzen von g darstellen. Zeigen Sie, daß dann $a_\ell = g$ für jeden Primteiler ℓ von $p-1$ die Bedingungen des Primzahltests von Pocklington-Lehmer erfüllt!

Aufgabe 4: *(3 Punkte)*
Angenommen, eine natürliche Zahl N wird sowohl mit Pollards $(p-1)$-Methode als auch mit Hilfe einer elliptischen Kurve E faktorisiert, p sei ein Primteiler von N und der verwendete Basispunkt $P \in E(\mathbb{F}_p)$ habe die Ordnung $p-1$. Ist es möglich, daß einer der beiden Algorithmen den Faktor p findet, der andere aber nicht?

Abgabe bis zum Dienstag, dem 26. November 2013, um 15.25 Uhr