WOLFGANG K. SEILER
Tel. 2515

B6, B4.18

18. Mai 2020

10. Übungsblatt Elliptische Kurven

Aufgabe 1: *(4 Punkte)*
Faktorisieren Sie $N = 72263$ nach POLLARDS $(p-1)$-Methode mit Suchgrenze $B = 10$!

Aufgabe 2: *(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 $a_i = g$ für jeden Primteiler p_i von $p-1$ die Bedingungen des Primzahltests von POCKLINGTON erfüllt!

Aufgabe 3: *(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 4: *(7 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.

Abgabe bis zum Freitag, dem 22. Mai 2020, um 12.00 Uhr