WOLFGANG K. SEILER
Tel. 2515
A5, C201

2. Februar 2005

13. Übungsblatt Kryptologie

Aufgabe 1: (*5 Punkte*)

a) Zeigen Sie: Die Gleichung $y^2 = x^3 + 3x + 9$ definiert genau dann eine elliptische Kurve über dem Körper $\mathbb{F}_p$, wenn $p \notin \{2, 3, 5, 17\}$.

b) Was passiert in den vier Ausnahmefällen?

Aufgabe 2: (*6 Punkte*)

a) Bestimmen Sie alle Punkte der elliptischen Kurve $y^2 = x^3 + 3x + 2$ über dem Körper $\mathbb{F}_7$!

b) Zeigen Sie, daß diese (zusammen mit dem Punkt O natürlich) eine zyklische Gruppe bilden!

Aufgabe 3: (*5 Punkte*)

Zeigen Sie:

a) Die Punkte der (genauen) Ordnung zwei auf der elliptischen Kurve $y^2 = x^3 + ax + b$ sind genau die Kurvenpunkte der Form $(x, 0)$.

b) Falls das Polynom $x^3 + ax + b$ in $\mathbb{F}_p$ drei verschiedene Nullstellen hat, bilden die Punkte der elliptischen Kurve $y^2 = x^3 + ax + b$ keine zyklische Gruppe.

Aufgabe 4: (*4 Punkte*)

Finden Sie eine untere und eine obere Schranke für die Anzahl der Punkte einer elliptischen Kurve $y^2 = x^3 + ax + b$ über dem Körper $\mathbb{F}_q$ mit q Elementen!

Abgabe bis zum Dienstag, dem 8. Februar 2005, um 12.00 Uhr