6. Übung Elementare Algorithmen in der Algebra

Priv. Doz. Dr. G. Nebe **(SS 00)**

Aufgabe 21. Sei E die elliptische Kurve, die durch $Y^2 = X^3 - X$ definiert ist.

a) Bestimmen Sie $E(\mathbb{F}_5)$.

b) Zeigen Sie, dass für $p \equiv 3 \pmod 4$ die Ordnung von E gleich $|E(\mathbb{F}_p)| = p + 1$ ist.

(Hinweis zu b): Zeigen Sie, dass (-1) kein Quadrat in $\mathbb{F}_p^*$ ist, und deshalb $\mathbb{F}_p^* = (\mathbb{F}_p^*)^2 \dot\cup (-1)(\mathbb{F}_p^*)^2$.)

Aufgabe 22. Zeigen Sie, dass im Fall $P_1 \neq P_2$, der durch die Addition $P_1 + P_2 =: P_3 = (x_3, y_3)$ definierte Punkt in $E(\mathbb{F}_p)$ liegt und dass $(x_3, -y_3) = -P_3$ genau der 3. Schnittpunkt von E mit der Geraden durch P_1 und P_2 ist.

Aufgabe 23. Entwerfen Sie ein Verfahren, Nachrichten mit RSA zu authentifizieren.

Abgabe: Donnerstag, den 25.5.00, in der Übung 12:30 Uhr im kl. physik. Hörsaal