Probeklausur — Elementare Zahlentheorie SoSe 2017

N-P. Skoruppa

20. Juli 2017

Name:	
Email des Korrektors:	

Lösen Sie die Aufgaben in der Übung und ggfs. den verbleibenden Rest zu Hause. Geben Sie Ihre Lösungen (zum Beispiel via Email) an Ihren Nachbarn. Er wird sie korrigieren und die Korrektur an Sie zurückgeben/schicken. Musterlösungen finden Sie ab Freitag Abend im Internet.

1 Grundbegriffe

...

2 Methoden

2.1

Bestimmen Sie alle rationalen Lösungen der Gleichung

$$x^2 + 5y^2 = 1$$

Antwort. Eine rationale Lösung ist $P := (1, 0)$. Das Geradenbüschel durch P ist $G_\lambda : y = \lambda(x - 1)$ ($\lambda \in \mathbb{Q}$). Der zweite Schnittpunkt S_λ von G_λ mit der Kurve $x^2 + 5y^2 = 1$ hat x-Koordinate

$$x^2 + 5[\lambda(x - 1)]^2 = 1,$$

d.h. (nach Division durch $x - 1$)

$$x + 1 + 5\lambda^2(x - 1) = 0.$$

Es folgt

$$S_\lambda = \left(\frac{5\lambda^2 - 1}{5\lambda^2 + 1}, \frac{-2\lambda}{5\lambda^2 + 1} \right).$$

Die von P verschiedenen rationalen Lösungen sind $\{S_\lambda : \lambda \in \mathbb{Q}\}$. □

2.2

Bestimmen Sie alle ganzahligen Lösungen der Gleichung

$$5x + 7y + 11z = 13.$$

Gibt es positive Lösungen?

Antwort. Eine Matrix in $\mathrm{GL}(2, \mathbb{Z})$ mit erster Spalte $(5, 7, 11)^t$ ist

$$U = \begin{pmatrix} 5 & 3 & 0 \\ 7 & 4 & 0 \\ 11 & 0 & 1 \end{pmatrix}.$$

Die gesuchte Lösungsmenge ist daher

$$L = \left\{ (13, u, v)U^{-1} : u, v \in \mathbb{Z} \right\}.$$

Wir haben

$$U^{-1} = \begin{pmatrix} -4 & 3 & 0 \\ 7 & -5 & 0 \\ 44 & -33 & 1 \end{pmatrix}.$$

Die allgemeinen Lösung ist also

$$(-52 + 7u + 44v, 39 - 5u - 33v, v).$$

□

2.3

Bestimmen Sie die Fundamentallösung der Pellschen Gleichung

$$x^2 - 27y^2 = 1.$$

Antwort. Die Lösung ist $26, 5$. Die Methode ist ausführlich im Skript zu finden und in den Übungen nochmals vorgeführt worden (Blatt 10, Aufgabe 3 und 4). □

2.4

Bestimmen Sie für die elliptische Kurve $E : y^2 = x^3+x+1$ die Gruppe $E(\mathbb{F}_7)$.

Antwort. Die Lösung findet man wie im entsprechenden ausführlichen Beispiel im Skript. Die richtige Antwort ist (sie ist natürlich zu begründen):

$$E(\mathbb{F}_7) = \{(0,1), (2,2), (0,-1), (2,-2), O\}.$$

Die Gruppe ist zyklisch. Setzt man $P = (0,1)$, so ist $2P = (2,-2)$, $3P = (2,2)$, $4P = (0,-1)$. □

2.5

Die elliptische Kurve $E : y^2 = x^3 - 77x/3 + 157/3$ besitzt die rationalen Punkte $P = (2,3)$ und $Q = (5,7)$. Berechnen Sie $P \oplus Q$.

Antwort. Die Summe kann zum Beispiel wie in der gestrigen Vorlesung oder nach der Methode im Skipt berechnet werden. Folgt man der ersten Methode, so hat man mit $F(x,y,z) = x^3 - 77xz^2/3 + 157z^3/3 - y^2$ das Polynom $G(U,V) = F(2U+5V, 3U+7V, U+V)$ in Linearfaktoren zu zerlegen. Man findet

$$G(U,V) = (-65U - 92V)UV.$$

Es ist also

$$P \oplus Q = [92(2,3,1) - 65(5,7,1)] = [-47/9 : -179/27 : 1] = (-47/3^2, -179/3^3).$$

□