S. Wewers, S. Wilke

Kryptographie, SS 06

Lösung 10

Aufgabe 3.

Wie bereits im Worksheet berechnet, gilt folgende Beziehung:

$$\begin{aligned} 1 \cdot (0,1) &= (0,1) \\ 2 \cdot (0,1) &= (2,5) \\ 3 \cdot (0,1) &= (2,2) \\ 4 \cdot (0,1) &= (0,6) \\ 5 \cdot (0,1) &= \mathcal{O} \end{aligned}$$

Man kann damit jedes Element als Vielfaches des Punktes $P = (0,1)$ darstellen; daraus lässt sich leicht die Gruppenstruktur ableiten, wenn man beachtet, dass stets $kP + lP = (k+l)P$. Zum Beispiel ist also $(2,5) + (0,6) = 2P + 4P = 6P = 1P = P$. Daraus ergibt sich folgende Verknüpfungstafel:

$+$	$\mathcal{O}$	$(0,1)$	$(2,5)$	$(2,2)$	$(0,6)$
$\mathcal{O}$	$\mathcal{O}$	$(0,1)$	$(2,5)$	$(2,2)$	$(0,6)$
$(0,1)$	$(0,1)$	$(2,5)$	$(2,2)$	$(0,6)$	$\mathcal{O}$
$(2,5)$	$(2,5)$	$(2,2)$	$(0,6)$	$\mathcal{O}$	$(0,1)$
$(2,2)$	$(2,2)$	$(0,6)$	$\mathcal{O}$	$(0,1)$	$(2,5)$
$(0,6)$	$(0,6)$	$\mathcal{O}$	$(0,1)$	$(2,5)$	$(2,2)$

Aufgabe 4.

(a) $z = 4 + 5i$.
Zunächst ist $N(z) = 4^2 + 5^2 = 16 + 25 = 41$. Nun ist 41 prim und $\equiv 1 \pmod 4$. Damit ist $41 = (5+4i)\cdot(5-4i)$ eine Zerlegung von 41 in Primelemente. Wegen der Eindeutigkeit der Primfaktorzerlegung ist damit $4 + 5i \sim 5 + 4i$ oder $4 + 5i \sim 5 - 4i$. Es ist $i(4+5i) = 4i - 5$ bzw. $(-i)(4+5i) = 5 - 4i$. Also ist $4 + 5i = i(5 - 4i)$ die gesuchte Zerlegung in Primelemente.

(b) $z = 13 + 11i$.
Zunächst ist $N(z) = 13^2 + 11^2 = 290 = 2 \cdot 5 \cdot 29$. Dabei ist $2 = (-i)(1+i)^2$, $5 = (2+i)(2-i)$, $29 = (5+2i)(5-2i)$ die entsprechende Zerlegung in Primelemente. Damit ist $z \sim (1+i)(2 \pm i)(5 \pm 2i)$ für eine gewisse Wahl von $\pm$. Ausprobieren liefert: $(2-i)(5+2i)(1+i) = 13 + 11i$, und das ist die Zerlegung in Primelemente.

(c) $z = 41 + 169i$.
Zunächst ist $N(z) = 41^2 + 169^2 = 30242 = 2 \cdot 15121$. Dabei ist $2 = (-i)(1+i)^2$, und $15121 \equiv 1 \pmod 4$ ist eine Primzahl, besitzt also eine Zerlegung $(a+ib)(a-ib)$ mit $a > b > 0$. Damit ist $z \sim (1+i)(a \pm ib)$. Wir können nun z durch $1+i$ teilen und erhalten

$$\frac{41 + 169i}{1+i} = \frac{(41+169i)(1-i)}{2} = \frac{210 + 128i}{2} = 105 + 64i.$$

Damit ist $41 + 169i = (1+i)(105 + 64i)$, wobei $105^2 + 64^2 = 15121$.