Mathematisches Institut
der Universität München
Pascal Reisert

Wintersemester 2015/2016
Übungsblatt 3
11. November 2015

Übungen zur Algorithmischen Zahlentheorie
Lösung

Aufgabe 10

Wir identifizieren

```
A B C D E F G H I/J K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
1 2 3 4 5 6 7 8 9   10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25.
```

Unser verschlüsselter Text nimmt damit die Form

$$(11, 8, 8, 2, 11, 1, 4, 24, 19, 23, 9, 20, 3, 25, 4, 4, 10, 15, 10, 21, 19, 11, 25, 23, 13, 5, 7)$$

an. Wir wissen, dass $z_1 = -8, z_2 = 0, z_3 = 3$, also

$$a \cdot 0 + b = 3, a \cdot (-8) + b = 0 \Rightarrow b = 3, a = (-8)^{-1} \cdot (-3) = 3 \cdot (-3) = -9.$$

Damit können wir das Pseudo-One-Time-Pad $(z_0, \ldots, z_{27})$ berechnen zu

$$([4], -8, 0, 3, 1, 19, 7, 15, 18, 16, 9, 22, 5, 8, 6, 24, 12, 20, 23, 21, 14, 2, 10, 13, 11, 4, 17, 0)$$

Es ergibt sich als Klartext

$$(19, 8, 5, 1, 17, 19, 14, 6, 3, 14, 12, 15, 20, 19, 5, 17, 15, 17, 14, 7, 17, 1, 12, 12, 9, 13, 7)$$

The art of computer programming.

Zusatzaufgabe

Behauptung 1. Seien g, h Elemente der Ordnung $\operatorname{ord}(g)$, $\operatorname{ord}(h)$ in einer endlichen abelschen Gruppe G. Dann gibt es ein Element der Ordnung $\operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h))$.

Beweis. In der Vorlesung wurde die Aussage für $\gcd(\operatorname{ord}(g), \operatorname{ord}(h)) = 1$ gezeigt. Sei jetzt $\gcd(\operatorname{ord}(g), \operatorname{ord}(h))$ beliebig und $x := g^{\gcd(\operatorname{ord}(g), \operatorname{ord}(h))}$ von Ordnung $\operatorname{ord}(g)/\gcd(\operatorname{ord}(g), \operatorname{ord}(h))$. Dann gilt $\gcd(\operatorname{ord}(x), \operatorname{ord}(h)) = 1$ und somit gibt es ein Element der Ordnung $\operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h)) = \operatorname{ord}(g)\operatorname{ord}(h)/\gcd(\operatorname{ord}(g), \operatorname{ord}(h))$ in G.

Behauptung 2. Die multiplikative Gruppe eines endlichen Körpers mit $n + 1$ Elementen ist zyklisch.

Beweis. Sei l das kleinste gemeinsame Vielfache der Ordnungen aller Elemente von G, dann ist jedes Element von G eine Nullstelle von $X^l - 1$. Da es maximal l Nullstellen von $X^l - 1$ geben kann, folgt $l \geqslant n = |G|$ und damit $l = n$. Nach *Behauptung 1* finden wir ein Element mit Ordnung n. □