Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 6

Aufgabe 1
Nachträge zu den *p*-adischen Zahlen, also den Ringen $\mathbb{Z}_{(p)}$.
Die Metrik auf ihnen hat ja die Eigenschaft, daß die Dreiecksungleichung verschärft ist zu $d(x,z)\leq \max\{d(x,y),d(y,z)\}$ (ultrametrische Ungleichung).
(*M*,*d*) sei ein ultrametrischer Raum, also ein metrischer Raum, in dem die ultrametrische Ungleichung gilt.

a) Man zeige: Haben zwei offene Kugeln in *M* nicht leeren Schnitt, so ist eine Teilmenge der anderen.

b) Man zeige: *M* ist „total unzusammenhängend", d.h. besitzt eine Teilmenge $L\subset M$ mindestens zwei Elemente, so gibt es nicht-leere disjunkte offene Teilmengen $U,V\subset M$ mit $L\subset U\cup V$ [1].

c) Man zeige: Die Menge der Abstände von Punkten in einem kompakten ultrametrischen Raum ist eine diskrete Teilmenge[2] reeller Zahlen.

d) Man beweise oder widerlege: $\mathbb{Z}_p$ ist kompakt.

Aufgabe 2
Man betrachte die bijektive lineare Abbildung $f:\mathbb{Z}_2^{1023}\rightarrow\mathbb{Z}_2^{1023}$, die gegeben ist durch $(x_0,x_1,\ldots,x_{1022})\mapsto(x_1,x_2,\ldots,x_{1023})$, wobei $x_{1023}:=x_0+x_7$ (Addition in $\mathbb{Z}_2$).
Für $x=(x_0,\ldots,x_{1022})\in\mathbb{Z}_2^{1023}$ setze man $\pi(x):=x_{1022}$.
Gibt man jetzt eine Bitfolge $a_0\cdots,a_{1022}$ vor, so kann man für $n\geq 1022$ rekursiv definieren $a_{n+1}:=\pi(f(a_{n-1022},\ldots,a_n))$. Wir werden in der Vorlesung lernen, daß die so definierte Folge die riesige Periode $2^{1023}-1$ besitzt, falls nicht alle $a_0\cdots,a_{1022}$ gleich 0 waren.

Offenbar kann man, bei Kenntnis von 1023 aufeinanderfolgende Folgengliedern alle weiteren Folgenelemente berechnen. Diese Vorhersage ist bei der folgendermaßen abgeleiteten Folge *b* nicht mehr möglich, *b* ist daher bei zufällig gewähltem Startwert *a* eine gute Zufallsfolge:

Wir betrachten jeweils 2 Bit der Folge *a*. Ist das erste Bit gleich 1, so geben wir in der Folge *b* den Wert des zweiten Bits aus. Ist das erste Bit gleich 0, so geben wir in der Folge *b* nichts aus.
(self shrinking)

Man schreibe ein Pariprogramm
```
generate(a,n)
```
welches *n* Bits der Folge *b* berechnet, ausgehend von einem Startwert $a=(a_{0,}\cdots a_{11})$.[3]

---

1 d.h. nur höchstens einelementige Teilmengen sind zusammenhängend. Die rationalen Zahlen und die irrationalen Zahlen sind als metrischer Raum total unzusammenhängend, ebenfalls die Cantormenge, die sogar im Gegensatz zu im Gegensatz zu den vorigen Beispielen kompakt ist.
2 d.h. jeder Punkt besitzt eine offene Umgebung, die keinen weiteren Punkt der Menge enthält
3 Wir schauen dann, wer das schnellste Programm hat.