Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 5

Aufgabe 1
Sei p eine ungerade Primzahl.
Beschreiben Sie die größte Untergruppe von $\mathbb{Z}_p^*$, auf der die Abbildung $x \mapsto x^2$ bijektiv ist.
Überprüfen Sie Ihre Theorie am Beispiel p=41.

Aufgabe 2
Seien p eine ungerade Primzahl, K ein Körper und η eine primitive p-te Einheitswurzel in K^*.
Man bilde die Gauß-Summe $G := \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \eta^i$ und zeige: $G^2 = (-1)^{\frac{p-1}{2}} p$.
(Vielleicht zu schwierig, andererseits nur elementare Summenmanipulation und elementare Eigenschaften des Legendre-Symbols (kein Reziprozitätsgesetz). Nachzulesen z.B. bei Koblitz. Ggf. nur nachrechnen für p=3,5,7. Man muß den Körper K gar nicht explizit angeben.)

Aufgabe 3
Sei p prim. Wir können jede natürliche Zahl a im Zahlsystem zur Basis p darstellen, also $a = \sum_{i=0}^{m} a_i p^i$, wobei $0 \le a_i < p$. Damit ist jede natürliche Zahl eindeutig repräsentiert durch eine endliche Folge $a_n, \ldots, a_0$ von Elementen in $\mathbb{Z}_p$, und man kann Addition und Multiplikation. als Operationen auf diesen Folgen interpretieren. Diese Operationen lassen sich in natürlicher Weise auf unendliche Folgen fortsetzen: um den i-ten Koeffizienten einer Summe oder eines Produkts solcher Folgen zu berechnen, benötigt man nur endlich viele Operationen. Die Menge dieser Folgen bildet mit dieser Addition und Multiplikation einen Ring, der ein Oberring von $\mathbb{Z}$ ist: -1 z.B. entspricht dabei offenbar der konstanten Folge $\ldots p-1, \ldots, p-1$. Man nennt diesen Ring den Ring der ganzen p-adischen Zahlen und schreibt dafür oft $\mathbb{Z}_{(p)}$.

$\mathbb{Z}_{(p)}$ ist in natürlicher Weise ein vollständiger metrischer Raum, und zwar mit der Metrik $d(a,b) := |a-b|$, wobei $|a| := \begin{cases} 0 & \text{falls} \quad a = 0 \\ p^{-n} & \text{falls} \quad a_0 = 0, \ldots, a_{n-1} = 0 \text{ und } a_n \neq 0 \end{cases}$.

a) Offenbar ist dann $|a| = 0 \Leftrightarrow a = 0$. Zeigen Sie, daß $|ab| = |a||b|$ und daß $|a+b| \le \max\{|a|, |b|\}$. (Damit ist d Metrik auf $\mathbb{Z}_{(p)}$ ist, wobei sogar $d(a,c) \le \max\{d(a,b), d(a,c)\}$. Machen Sie sich klar, was es bedeutet, daß eine Folge in $\mathbb{Z}_{(p)}$ eine Nullfolge oder eine Cauchyfolge ist.)

b) Zeigen Sie, daß jedes Element a mit $a_0 \neq 0$, ein Inverses bezüglich der Multiplikation besitzt. (Dazu konstruieren Sie rekursiv $b_0 := a_0^{-1} \in \mathbb{Z}_p$ und b_{n+1} aus $b_n, \ldots, b_0$. Damit haben Sie b definiert und zeigen dann durch Induktion, daß $ab = 1$.) Berechnen Sie so 3^{-1} in $\mathbb{Z}_{(2)}$

c) Nehmen Sie an, daß $b^3 = a$ [1] in $\mathbb{N}$ und damit in $\mathbb{Z}_{(p)}$.

---

1 Die dritte Wurzel wird hier nur als Beispiel genommen. Jede andere würde genauso behandelt.

Sie können dann b_0 als dritte Wurzel von $a \in \mathbb{Z}_p$ finden und anschließend durch Lösen linearer Gleichungen b_{n+1} aus $b_n, \ldots, b_0$ berechnen. Sobald Sie mit n über ein Drittel der Stellenzahl von a hinaus sind, haben Sie auch die Gleichung in $\mathbb{N}$ gelöst! Das Rechnen in $\mathbb{Z}_{(p)}$ kann also beim Rechnen in $\mathbb{N}$ oder $\mathbb{Z}$ und bei zahlentheoretischen Problemen helfen: Man löst das Problem in $\mathbb{Z}_{(p)}$ durch Einsatz von Analysis-Methoden, die durch die vollständige Metrik ermöglicht werden und zeigt, daß die Lösung in dem Unterring $\mathbb{Z} \subset \mathbb{Z}_{(p)}$ liegt.

Finden Sie mit dem oben geschilderten Ansatz zunächst eine dritte Wurzel von 1331 in $\mathbb{Z}_{(2)}$ und damit in $\mathbb{N}$ und schreiben Sie nach Möglichkeit ein Pari-Programm, welches so dritte oder gar n-te Wurzeln zieht.