8.9 Die Anzahl invertierbarer Matrizen in einem Restklassenring

Ziel ist, eine möglichst genaue Vorstellung davon zu bekommen, wie groß die Anzahl

$$\nu_{ln} := \#GL_l(\mathbb{Z}/n\mathbb{Z})$$

der invertierbaren $l \times l$-Matrizen über dem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ ist.

Im Spezialfall $l = 1$ ist ν_{1n} die Anzahl der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$ selbst, und das ist der Wert $\varphi(n)$ der EULERschen φ-Funktion.

Eine *obere Schranke* für ν_{ln} ist leicht gefunden:

$$\nu_{ln} \leq \#M_{ll}(\mathbb{Z}/n\mathbb{Z}) = n^{l^2}.$$

Eine *untere Schranke* erhält man aus der Beobachtung, dass Matrizen der Gestalt (über einem Ring R)

$$\begin{pmatrix} 1 & & \\ & \ddots & \\ * & & 1 \end{pmatrix} \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_l \end{pmatrix} \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$$

stets invertierbar sind, wenn $d_1, \ldots, d_l \in R^\times$. Dadurch erhält man eine injektive Abbildung

$$R^{\frac{l(l-1)}{2}} \times (R^\times)^l \times R^{\frac{l(l-1)}{2}} \longrightarrow GL_l(R).$$

(Beweis der Injektivität: **Übungsaufgabe.**) Daraus folgt die Abschätzung

$$\nu_{ln} \geq n^{\frac{l(l-1)}{2}} \cdot \varphi(n)^l \cdot n^{\frac{l(l-1)}{2}} = n^{l^2-l} \cdot \varphi(n)^l.$$

Zusammengefasst:

Satz 9

$$n^{l^2-l} \cdot \varphi(n)^l \leq \nu_{ln} \leq n^{l^2}.$$

Bemerkungen

1. Die Idee, Matrizen in der Form $A = UDV$ wie oben zu schreiben – mit einer Diagonalmatrix D, einer unteren Dreiecksmatrix U mit Einser-Diagonale sowie einer oberen Dreiecksmatrix V mit ebenfalls Einser-Diagonale – ist gleichzeitig eine geeignete Methode, invertierbare Matrizen zu konstruieren, ohne lange zu probieren und Determinanten auszurechnen. Man erhält „fast alle" invertierbaren Matrizen auf diese Weise – in der Theorie der algebraischen Gruppen ist dies die „große BRUHAT-Zelle". Solche Matrizen sind auch wegen der Formel $A^{-1} = V^{-1}D^{-1}U^{-1}$ leicht zu invertieren.

2. Aus zwei unteren Schranken für die φ-Funktion, die hier ohne Beweis angegeben werden, ergeben sich handlichere Schranken für ν_{ln}. Die erste Abschätzung ist

$$\varphi(n) > \frac{6}{\pi^2} \cdot \frac{n}{\ln n} \quad \text{für } n \geq 7.$$

Daraus folgt für $n \geq 7$

$$\nu_{ln} > n^{l^2-l} \cdot \left(\frac{6}{\pi^2} \cdot \frac{n}{\ln n}\right)^l = \frac{6^l}{\pi^{2l}} \cdot \frac{n^{l^2}}{(\ln n)^l}.$$

3. Die andere Schranke ist

$$\varphi(n) > \frac{n}{2 \cdot \ln \ln n} \quad \text{für fast alle } n.$$

Daraus folgt

$$\nu_{ln} > \frac{1}{(2 \cdot \ln \ln n)^l} \cdot n^{l^2}$$

oder auch

$$\frac{1}{(2 \cdot \ln \ln n)^l} \quad < \quad \frac{\nu_{ln}}{n^{l^2}} \quad < \quad 1$$

für fast alle n.

Fazit: „Sehr viele“ bis „fast alle“ Matrizen in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ sind invertierbar. Was das im einzelnen bedeutet, wird weiter unten noch etwas genauer beleuchtet.

Beispiel. Für $n = 26$ lässt sich die untere Schranke aus Satz 9 noch stark vergröbern zu einer sehr übersichtlichen Form: Da $\varphi(26) = 12$, folgt

$$\nu_{l,26} \geq 26^{l^2-l} 12^l > 16^{l^2-l} 8^l = 2^{4l^2-l}.$$

Daraus erhält man die Abschätzungen $\nu_{2,26} > 2^{14}$, $\nu_{3,26} > 2^{33}$, $\nu_{4,26} > 2^{60}$, $\nu_{5,26} > 2^{95}$, so dass die Hill-Chiffre spätestens bei der Blockgröße 5 vor vollständiger Schlüsselsuche sicher ist.

Es gibt auch eine genaue Formel für ν_{ln}, die jetzt hergeleitet wird.

Hilfssatz 5 *Sei $n = p$ prim. Dann ist*

$$\nu_{lp} = p^{l^2} \cdot \rho_{lp} \quad \textit{mit} \quad \rho_{lp} = \prod_{i=1}^{l} \left(1 - \frac{1}{p^i}\right).$$

Insbesondere geht die relative Häufigkeit von invertierbaren Matrizen, ρ_{lp}, bei festem l mit wachsendem p gegen 1.

Beweis. Man baut eine invertierbare Matrix Spalte für Spalte auf und zählt jeweils die Möglichkeiten. Da $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein Körper ist, ist die erste Spalte ein beliebiger Vektor $\neq 0$. Davon gibt es $p^l - 1$ Stück.

Seien nun schon i Spalten gewählt; diese müssen linear unabhängig sein und spannen daher einen Unterraum von $\mathbb{F}_p^l$ aus p^i Elementen auf. Die $(i+1)$-te Spalte ist dann ein beliebiger Vektor außerhalb dieses Unterraums, und davon gibt es $p^l - p^i$ Stück. Insgesamt sind das

$$\prod_{i=0}^{l-1}(p^l - p^i) = \prod_{i=0}^{l-1} p^l(1 - p^{i-l}) = p^{l^2} \prod_{j=1}^{l} \left(1 - \frac{1}{p^j}\right)$$

Möglichkeiten. $\diamond$

Hilfssatz 6 *Sei $n = p^e$ mit p prim und $e \geq 1$. Dann gilt:*

(i) *Sei $A \in M_{ll}(\mathbb{Z})$. Dann ist $A \bmod n$ in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ genau dann invertierbar, wenn $A \bmod p$ in $M_{ll}(\mathbb{F}_p)$ invertierbar ist.*

(ii) *Die Anzahl der invertierbaren Matrizen in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ ist*

$$\nu_{ln} = p^{el^2} \cdot \rho_{lp}.$$

(iii) *Die relative Häufigkeit invertierbarer Matrizen in $M_{ll}(\mathbb{Z}/p^e\mathbb{Z})$ ist ρ_{lp}, unabhängig vom Exponenten e.*

Beweis. (i) Da $\mathrm{ggT}(p, \mathrm{Det}\, A) = 1 \iff \mathrm{ggT}(n, \mathrm{Det}\, A) = 1$, sind beide Aussagen zu $p \nmid \mathrm{Det}\, A$ äquivalent.

(ii) O. B. d. A. habe A nur Einträge in $[0 \ldots n-1]$. Dann schreibt man $A = pQ + R$ mit allen Einträgen von R in $[0 \ldots p-1]$ und allen von Q in $[0 \ldots p^{e-1} - 1]$. Nun ist $A \bmod n$ genau dann invertierbar, wenn $R \bmod p$ invertierbar ist; für R gibt es nach Hilfssatz 5 ν_{lp} Möglichkeiten und für Q noch $p^{(e-1)l^2}$. Zusammen ist das die behauptete Formel.

(iii) folgt direkt aus (ii). $\diamond$

Hilfssatz 7 *Sind m und n teilerfremd, so ist $\nu_{l,mn} = \nu_{lm}\nu_{ln}$.*

Beweis. Der vom chinesischen Restsatz gelieferte Ring-Isomorphismus

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

wird zu einem Isomorphismus der (nichtkommutativen) Ringe

$$M_{ll}(\mathbb{Z}/mn\mathbb{Z}) \longrightarrow M_{ll}(\mathbb{Z}/m\mathbb{Z}) \times M_{ll}(\mathbb{Z}/n\mathbb{Z})$$

fortgesetzt. Die Behauptung folgt, weil sie die Gleichheit der jeweiligen Anzahlen von invertierbaren Elementen aussagt. $\diamond$

Daraus folgt durch Induktion unmittelbar:

Satz 10 *Für $n \in \mathbb{N}$ gilt*

$$\nu_{ln} = n^{l^2} \cdot \prod_{\substack{p \text{ prim} \\ p|n}} \rho_{lp}.$$

Insbesondere hängt die relative Häufigkeit invertierbarer Matrizen, $\rho_{ln} = \nu_{ln}/n^{l^2}$ nicht von den Exponenten der Primfaktoren in n ab; die explizite Formel heißt

$$\rho_{ln} = \prod_{\substack{p \text{ prim} \\ p|n}} \rho_{lp} = \prod_{\substack{p \text{ prim} \\ p|n}} \prod_{i=1}^{l} \left(1 - \frac{1}{p^i}\right).$$

Beispiel. Für $n = 26$ ergibt die explizite Formel die Werte $\nu_{1,26} = 12$, $\nu_{2,26} = 157{\cdot}248$, $\nu_{3,26} = 1{\cdot}634{\cdot}038{\cdot}189{\cdot}056 \approx 1.6 \cdot 10^{12}$. Der Vergleich des letzteren Werts mit der oben hergeleiteten unteren Schranke $2^{33} \approx 8 \cdot 10^9$ zeigt, wie grob diese ist.

Übungsaufgabe. Sei $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ die aufsteigende Folge der Primzahlen. Sei $n_r = p_1 \cdots p_r$ für $r \geq 1$. Zeige, dass bei festem l

$$\lim_{r \to \infty} \rho_{ln_r} = 0.$$

D. h., der Anteil der invertierbaren Matrizen schwindet immer mehr. *Anleitung*: Sei ζ die RIEMANNsche ζ-Funktion. Welchen Wert hat ζ in den natürlichen Zahlen $i \geq 1$?