Die Anzahl invertierbarer Matrizen in einem Restklassenring[1]

[In diesem Abschnitt werden keine vollständigen Beweise gegeben.]

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

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

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

Im Spezialfall $l = 1$ ist $\nu_{1,n}$ 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 $\nu_{l,n}$ ist leicht gefunden:

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

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

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

Zusammengefasst:

Satz 1

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

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

[1] Klaus Pommerening, Kryptologie; 26. Juni 2002, letzte Änderung: 1. Juli 2002

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. Es gibt eine genaue Formel für $\nu_{l,n}$. Zunächst sei $n = p$ prim. Dann ist

$$\nu_{l,p} = p^{l^2} \cdot \rho(p,l) \quad \text{mit} \quad \rho(p,l) = \prod_{i=1}^{l} \left(1 - \frac{1}{p^i}\right).$$

Im allgemeinen Fall ist

$$\nu_{l,n} = n^{l^2} \cdot \prod_{\substack{p \text{ prim} \\ p|n}} \rho(p,l).$$

3. Aus zwei unteren Schranken für die φ-Funktion, die hier ebenfalls ohne Beweis verwendet werden, ergeben sich handlichere Schranken für $\nu_{l,n}$. Die erste Abschätzung ist

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

Daraus folgt für $n \geq 7$

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

4. Die andere Schranke ist

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

Daraus folgt

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

oder auch

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

für fast alle n. *Fazit*: „Fast alle“ Matrizen in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ sind invertierbar.