Invertierung der Schlüsselmatrix mit dem Gauss-Algorithmus

Dieses Tutorial zeigt, wie Sie die Schlüsselmatrix K aus dem Artikel mittels des Gauss-Algorithmus modulo 26 invertieren, also $K^{-1} \pmod{26}$ berechnen.

Ausgangspunkt ist K:

$$K = \begin{pmatrix} 20 & 2 & 1 & 21 \\ 16 & 11 & 25 & 20 \\ 14 & 18 & 7 & 12 \\ 25 & 22 & 23 & 4 \end{pmatrix}$$

Schreiben Sie K und die Einheitsmatrix I_n passender Dimension (hier also die vierreihige Einheitsmatrix I_4) nebeneinander, getrennt durch einen senkrechten Strich. Die Klammern außen lassen Sie der Einfachheit halber weg:

$$\left.\begin{array}{cccc|cccc} 20 & 2 & 1 & 21 & 1 & 0 & 0 & 0 \\ 16 & 11 & 25 & 20 & 0 & 1 & 0 & 0 \\ 14 & 18 & 7 & 12 & 0 & 0 & 1 & 0 \\ 25 & 22 & 23 & 4 & 0 & 0 & 0 & 1 \end{array}\right.$$

Sie führen nun *elementare Zeilenumformungen* durch, um die linke Seite, also K, in die Einheitsmatrix I_4 zu überführen. Die gleichen Umformungen nehmen sie auf der rechten Seite vor, auf der zu Anfang I_4 steht. Sobald sie damit links die Einheitsmatrix I_4 konstruiert haben, steht auf der rechten Seite K^{-1}. Erlaubte elementare Umformungen sind dabei das Vertauschen von Zeilen, die Multiplikation von Zeilen mit einer Zahl ungleich Null sowie das Subtrahieren des Vielfachen einer Zeile von einer anderen Zeile. Alle Berechnungen werden modulo 26 durchgeführt. Wichtig ist, dass alle Operationen immer in identischer Weise auf beiden Seiten durchgeführt werden!

Zunächst wollen Sie das Element links oben (also die 20 in der 1. Zeile, 1. Spalte) zu 1 machen. Beim Rechnen ohne Modulo-Arithmetik würden Sie die 1. Zeile durch 20 dividieren. In der Berechnung mit Restklassen verwenden Sie stattdessen das modular Inverse (modulo 26) des jeweiligen Elements. Nun hat 20 kein solches Inverses (20 und 26 sind nicht teilerfremd, sie haben den gemeinsamen Teiler 2). Sie müssen also die 1.

Zeile mit einer anderen Zeile vertauschen. Die 2. und 3. Zeile kommen dafür nicht in Frage, da ihre jeweiligen Elemente in der 1. Spalte ebenfalls gerade sind und damit nicht teilerfremd zu 26. Vertauschen Sie also die 1. und die 4. Zeile, denn die 25 ganz links in der 4. Zeile ist invertierbar modulo 26: Nach Tausch 1. und 4. Zeile:

$$\left(\begin{array}{cccc|cccc} 25 & 22 & 23 & 4 & 0 & 0 & 0 & 1 \\ 16 & 11 & 25 & 20 & 0 & 1 & 0 & 0 \\ 14 & 18 & 7 & 12 & 0 & 0 & 1 & 0 \\ 20 & 2 & 1 & 21 & 1 & 0 & 0 & 0 \end{array}\right)$$

Das Inverse zu 25 ist 25 selbst, denn $25 \cdot 25 = 625 = 24 \cdot 26 + 1$. Sie multiplizieren also die erste Zeile mit 25

$$\left(\begin{array}{cccc|cccc} 625 & 550 & 575 & 100 & 0 & 0 & 0 & 25 \\ 16 & 11 & 25 & 20 & 0 & 1 & 0 & 0 \\ 14 & 18 & 7 & 12 & 0 & 0 & 1 & 0 \\ 20 & 2 & 1 & 21 & 1 & 0 & 0 & 0 \end{array}\right)$$

und reduzieren modulo 26, betrachten also nur die Divisionsreste bei Division durch 26:

$$\left(\begin{array}{cccc|cccc} 1 & 4 & 3 & 22 & 0 & 0 & 0 & 25 \\ 16 & 11 & 25 & 20 & 0 & 1 & 0 & 0 \\ 14 & 18 & 7 & 12 & 0 & 0 & 1 & 0 \\ 20 & 2 & 1 & 21 & 1 & 0 & 0 & 0 \end{array}\right)$$

Nun erzeugen Sie in der 1. Spalte überall Nullen außer in der 1. Zeile, indem Sie ein geeignetes Vielfaches der 1. Zeile von der jeweiligen Zeile abziehen. Sie ziehen also das 16-fache der 1. Zeile von der 2. Zeile ab, das 14-fache der 1. von der 3. Zeile und das 20-fache der 1. von der 4. Zeile, wie immer mit anschließender Reduktion modulo 26:

$$\left(\begin{array}{cccc|cccc} 1 & 4 & 3 & 22 & 0 & 0 & 0 & 25 \\ 0 & 25 & 3 & 6 & 0 & 1 & 0 & 16 \\ 0 & 14 & 17 & 16 & 0 & 0 & 1 & 14 \\ 0 & 0 & 19 & 23 & 1 & 0 & 0 & 20 \end{array}\right)$$

Nun multiplizieren Sie die 2. Zeile mit 25, um das Element in der 2. Zeile und 2. Spalte zu 1 zu machen:

$$\left(\begin{array}{cccc|cccc} 1 & 4 & 3 & 22 & 0 & 0 & 0 & 25 \\ 0 & 1 & 23 & 20 & 0 & 25 & 0 & 10 \\ 0 & 14 & 17 & 16 & 0 & 0 & 1 & 14 \\ 0 & 0 & 19 & 23 & 1 & 0 & 0 & 20 \end{array}\right)$$

Im nächsten Schritt wollen Sie ober- und unterhalb der gerade erzeugten 1 Nullen haben und ziehen dazu das 4-fache der 2. Zeile von der 1. Zeile ab sowie das 14-fache der 2. von der 3. Zeile. In der 4. Zeile steht schon eine Null in der 2. Spalte, hier ist also nichts zu tun:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 15 & 20 & 0 & 4 & 0 & 11 \\ 0 & 1 & 23 & 20 & 0 & 25 & 0 & 10 \\ 0 & 0 & 7 & 22 & 0 & 14 & 1 & 4 \\ 0 & 0 & 19 & 23 & 1 & 0 & 0 & 20 \end{array}\right)$$

Jetzt muliplizieren Sie die 3. Zeile mit dem modular Inversen von 7, also 15 (wegen $7 \cdot 15 = 104 = 4 \cdot 26 + 1$), um in der 3. Zeile und 3. Spalte eine 1 zu erreichen:

$$\begin{array}{cccc|cccc} 1 & 0 & 15 & 20 & 0 & 4 & 0 & 11 \\ 0 & 1 & 23 & 20 & 0 & 25 & 0 & 10 \\ 0 & 0 & 1 & 18 & 0 & 2 & 15 & 8 \\ 0 & 0 & 19 & 23 & 1 & 0 & 0 & 20 \end{array}$$

An dieser Stelle subtrahieren Sie geeignete Vielfache der 3. Zeile von den übrigen Zeilen, um in der 3. Spalte Nullen zu erhalten außer beim gerade erzeugten Pivot-Element 1:

$$\begin{array}{cccc|cccc} 1 & 0 & 0 & 10 & 0 & 0 & 9 & 21 \\ 0 & 1 & 0 & 22 & 0 & 5 & 19 & 8 \\ 0 & 0 & 1 & 18 & 0 & 2 & 15 & 8 \\ 0 & 0 & 0 & 19 & 1 & 14 & 1 & 24 \end{array}$$

Es ist $19 \cdot 11 = 209 = 8 \cdot 26 + 1$, also ist 11 das modular Inverse zu 19 (modulo 26). Sie multiplizieren deshalb die 4. Zeile mit 11:

$$\begin{array}{cccc|cccc} 1 & 0 & 0 & 10 & 0 & 0 & 9 & 21 \\ 0 & 1 & 0 & 22 & 0 & 5 & 19 & 8 \\ 0 & 0 & 1 & 18 & 0 & 2 & 15 & 8 \\ 0 & 0 & 0 & 1 & 11 & 24 & 11 & 4 \end{array}$$

Im letzten Schritt ziehen Sie geeignete Vielfache der 4. Zeile von den übrigen Zeilen ab, um in den ersten drei Zeilen Nullen in der 4. Spalte zu erhalten:

$$\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 20 & 20 & 3 & 7 \\ 0 & 1 & 0 & 0 & 18 & 23 & 11 & 24 \\ 0 & 0 & 1 & 0 & 10 & 12 & 25 & 14 \\ 0 & 0 & 0 & 1 & 11 & 24 & 11 & 4 \end{array}$$

Auf der linken Seite steht nun die Einheitsmatrix I_4, Sie haben also erfolgreich die inverse Matrix K^{-1} berechnet, sie steht auf der rechten Seite. Sie überzeugen sich leicht, dass es die im Artikel genannte inverse Schlüsselmatrix ist.

Die beschriebenen Umformungen lassen sich auch gut nachprogrammieren, um die Berechnung zu automatisieren. Ferner gibt es Mathematik-Software, die entsprechende Funktionen bereitstellt.

Wäre übrigens die Schlüsselmatrix K nicht invertierbar modulo 26 gewesen, hätte also $ggT(det(K), 26) \neq 1$ gegolten, wäre im Verlauf der Umformung die Situation eingetreten, dass Sie kein Pivot-Element 1 auf der Hauptdiagonalen hätten erzeugen können. Ein Beispiel ist eine Schlüsselmatrix mit ausschließlich geraden Elementen in der 1. Spalte.