

1. Berechnen Sie das Produkt $97531 \otimes 86420$ in $\mathbf{Z}_{9699690}$ mit Hilfe des Chinesischen Restsatzes.

Lösung: Die Zahl 9699690 ist das Produkt der ersten acht Primzahlen $p_1 = 2, p_2 = 3, \dots, p_8 = 19$. Nach dem Chinesischen Restsatz ist, da die p_i paarweise teilerfremd sind,

$$\mathbf{Z}_{p_1 p_2 \dots p_8} \cong \mathbf{Z}_{p_1} \times \mathbf{Z}_{p_2} \times \dots \times \mathbf{Z}_{p_8}$$

und die Additions- und Multiplikationsrechnung in $\mathbf{Z}_{p_1 p_2 \dots p_8}$ kann auf $\mathbf{Z}_{p_1} \times \mathbf{Z}_{p_2} \times \dots \times \mathbf{Z}_{p_8}$ übertragen werden, wo komponentenweise gerechnet wird.

Sei ψ die Abbildung $x \mapsto (x \bmod p_1, x \bmod p_2, \dots, x \bmod p_8)$. Es ist

$$\psi(97531) = (1, 1, 1, 0, 5, 5, 2, 4), \quad \psi(86420) = (0, 2, 0, 5, 4, 9, 9, 8)$$

und

$$\psi(97531) \otimes \psi(86420) = (0, 2, 0, 0, 9, 6, 1, 13).$$

Dieses Ergebnis muss nun rücktransformiert werden in den Ring $\mathbf{Z}_{9699690}$. Dazu ist es gut, wenn man die Urbilder jener Tupel kennt, die genau an der i -ten Stelle den Wert 1 und an allen übrigen Stellen den Wert 0 haben. Diese Urbilder bekommt man, indem man das modulare Inverse (bezüglich der Primzahl p_i) zum Produkt der übrigen Primzahlen, also zu $p_1 p_2 \dots p_8 / p_i$, berechnet und den erhaltenen Wert mit p_i multipliziert. Es ist

$$\begin{aligned} \psi^{-1}((1, 0, 0, 0, 0, 0, 0, 0)) &= 4849845 \\ \psi^{-1}((0, 1, 0, 0, 0, 0, 0, 0)) &= 3233230 \\ \psi^{-1}((0, 0, 1, 0, 0, 0, 0, 0)) &= 3879876 \\ \psi^{-1}((0, 0, 0, 1, 0, 0, 0, 0)) &= 8314020 \\ \psi^{-1}((0, 0, 0, 0, 1, 0, 0, 0)) &= 6172530 \\ \psi^{-1}((0, 0, 0, 0, 0, 1, 0, 0)) &= 3730650 \\ \psi^{-1}((0, 0, 0, 0, 0, 0, 1, 0)) &= 9129120 \\ \psi^{-1}((0, 0, 0, 0, 0, 0, 0, 1)) &= 9189180. \end{aligned}$$

Die berechneten Zahlen sind Elemente in $\mathbf{Z}_{p_1 p_2 \dots p_8}$. Die i -te dieser Zahlen stellt in \mathbf{Z}_{p_i} das Einselement, in $\mathbf{Z}_{p_j}, j \neq i$ das Nullelement dar. Wir benötigen in unserem Fall nur die 2., 5., 6., 7. und 8. Zahl. Zur Berechnung der obigen Zahlen kann man den erweiterten euklidischen Algorithmus verwenden. Wir zeigen dies für den letzten Fall. Man rechnet, als würde man den größten gemeinsamen Teiler von $9699690 : 19 = 510510$ und 19 bestimmen. Der ist natürlich 1, aber es geht nicht darum, sondern um die dabei gewonnenen Koeffizienten.

$$\begin{aligned} \begin{bmatrix} 19 \\ 18 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & -26868 \end{bmatrix} \begin{bmatrix} 510510 \\ 19 \end{bmatrix} \\ \begin{bmatrix} 18 \\ 1 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \end{bmatrix} \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & -18 \end{bmatrix} \begin{bmatrix} 18 \\ 1 \end{bmatrix} \end{aligned}$$

Es ist

$$\begin{bmatrix} 0 & 1 \\ 1 & -18 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -26868 \end{bmatrix} = \begin{bmatrix} -1 & 26869 \\ 19 & -510510 \end{bmatrix},$$

also

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 & 26869 \\ 19 & -510510 \end{bmatrix} \begin{bmatrix} 510510 \\ 19 \end{bmatrix}$$

und somit

$$1 = (-1) \cdot 510510 + 26869 \cdot 19.$$

Es ist $-510510 \bmod 9699690 = 9189180$, $9189180 \bmod 19 = 1$ und $9189180 \bmod p_i = 0$ für $i = 1, \dots, 7$.

Nun kann $\psi^{-1}((0, 2, 0, 0, 9, 6, 1, 13))$ berechnet werden: $\psi^{-1}((0, 2, 0, 0, 9, 6, 1, 13)) = (2 \otimes 3233230) \oplus (9 \otimes 6172530) \oplus (6 \otimes 3730650) \oplus (1 \otimes 9129120) \oplus (13 \otimes 9189180) = 6566560 \oplus 7054320 \oplus 2984520 \oplus 9129120 \oplus 360360 = 9298100$.

2. ([2], Exercise 4.31) Eine Zahl in Dezimaldarstellung ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist. Beweisen und verallgemeinern Sie diese Aussage.

Lösung: Sei $x = \sum_{k=0}^n a_k \cdot 10^k$ und $y = \sum_{k=0}^n a_k \cdot (10 \bmod 3)^k$ (y ist die Quersumme von x bei Darstellung im Zehnersystem). Es ist $x \bmod 3 = 0$ genau dann, wenn $y \bmod 3 = 0$ ist, d.h. wenn y durch 3 teilbar ist.

Allgemein: In einem Zahlensystem mit Basis b gilt für eine beliebige Zahl x , deren Quersumme y und eine Zahl d mit $b \bmod d = 1$: $d \mid x$ genau dann, wenn $d \mid y$.

3. [2], Exercise 4.10) Berechnen Sie $\varphi(999)$.

Lösung: $\varphi(999) = 999 \cdot (1 - 1/3) \cdot (1 - 1/37) = 648$.

4. ([1], Übung 6.1) Zeigen Sie, dass das Inverse der Fibonacci-Zahl F_n modulo F_{n+1} gleich F_{n-1} ist, falls n ungerade ist.

Lösung: Für die Fibonacci-Zahlen gilt bekanntlich

$$\begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix}$$

und damit auch

$$\begin{bmatrix} F_1 \\ F_0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}^n \begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix}. \quad (1)$$

Die n -ten Potenzen der Matrix $\begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}$ entwickeln sich folgendermaßen:

$$\begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}, \begin{bmatrix} -1 & 2 \\ 2 & -3 \end{bmatrix}, \begin{bmatrix} 2 & -3 \\ -3 & 5 \end{bmatrix}, \begin{bmatrix} -3 & 5 \\ 5 & -8 \end{bmatrix}, \begin{bmatrix} 5 & -8 \\ -8 & 13 \end{bmatrix}, \begin{bmatrix} -8 & 13 \\ 13 & -21 \end{bmatrix} \dots$$

Man erkennt, dass die Koeffizienten dieser Matrizen vorzeichenbehaftete Fibonacci-Zahlen sind. Es gibt einen charakteristischen Vorzeichenwechsel.

Man kann das Bildungsgesetz

$$\begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}^n = \begin{bmatrix} (-1)^n F_{n-1} & (-1)^{n+1} F_n \\ (-1)^{n+1} F_n & (-1)^n F_{n+1} \end{bmatrix}$$

vermuten. Wir erhärten es durch Induktion:

Induktionsbeginn:

$$\begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}^1 = \begin{bmatrix} -F_0 & F_1 \\ F_1 & -F_2 \end{bmatrix}.$$

Induktionsschritt:

$$\begin{aligned} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}^n &= \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} (-1)^{n-1} F_{n-2} & (-1)^n F_{n-1} \\ (-1)^n F_{n-1} & (-1)^{n+1} F_n \end{bmatrix} \\ &= \begin{bmatrix} (-1)^n F_{n-1} & (-1)^{n+1} F_n \\ (-1)^{n+1} (F_{n-2} + F_{n-1}) & (-1)^n (F_{n-1} + F_n) \end{bmatrix} \\ &= \begin{bmatrix} (-1)^n F_{n-1} & (-1)^{n+1} F_n \\ (-1)^{n+1} F_n & (-1)^n F_{n+1} \end{bmatrix} \end{aligned}$$

Nun kann die Gleichung (1) folgendermaßen geschrieben werden:

$$\begin{bmatrix} F_1 \\ F_0 \end{bmatrix} = \begin{bmatrix} (-1)^n F_{n-1} & (-1)^{n+1} F_n \\ (-1)^{n+1} F_n & (-1)^n F_{n+1} \end{bmatrix} \begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix}. \quad (2)$$

Aus der ersten Zeile von (2) erhält man

$$1 = (-1)^n F_{n-1} F_{n+1} + (-1)^{n+1} F_n F_n,$$

für gerade n insbesondere

$$1 = F_{n-1} F_{n+1} + (-F_n) F_n. \quad (3)$$

Da $-F_n \bmod F_{n+1} = F_{n-1}$ ist, ist damit gezeigt, dass für gerade n die Fibonacci-Zahl F_{n-1} das F_{n+1} -modulare Inverse von F_n ist.

5. RSA-Verschlüsselung: Der Modulus sei $N = 11 \cdot 17 = 187$. Die Botschaft x werde mit dem öffentlichen Exponenten $e = 107$ zu $y = x^e \bmod 187 = 101$ verschlüsselt und übermittelt. Wie lautet die Botschaft x in "Klartext"?

Lösung: Es ist $\varphi(187) = 10 \cdot 16 = 160$ (Euler'sche φ -Funktion) und der geheime Exponent d ist das 160-modulare Inverse von e . Dieses kann man mit Hilfe des erweiterten euklidischen Algorithmus bestimmen, indem man pro forma den ggT von $e = 107$ und $\varphi(187) = 160$ berechnet und in geeigneter Form darstellt. Es ist

$$\begin{bmatrix} 107 \\ 53 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 160 \\ 107 \end{bmatrix}, \begin{bmatrix} 53 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 107 \\ 53 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -53 \end{bmatrix} \begin{bmatrix} 53 \\ 1 \end{bmatrix}.$$

Das Produkt der drei Matrizen (Reihenfolge!) ist

$$\begin{bmatrix} 0 & 1 \\ 1 & -53 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ * & * \end{bmatrix}.$$

Aus

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ * & * \end{bmatrix} \begin{bmatrix} 160 \\ 107 \end{bmatrix}$$

erhält man die Beziehung $1 = (-2) \cdot 160 + 3 \cdot 107$, der man entnimmt, dass 3 das 160-modulare Inverse von 107 ist, d.h. $d = 3$.

Die Botschaft y entschlüsselt man also, indem man sie mit $d = 3$ potenziert (modulo 187). Das kann man entweder direkt rechnen (Taschenrechner) oder in $\mathbf{Z}_{11} \times \mathbf{Z}_{17}$. In $\mathbf{Z}_{11} \times \mathbf{Z}_{17}$ hat y die Darstellung $(2, -1)$. Es ist $(2, -1)^3 = (8, -1) = (2, -1) + (6, 0)$. $(1, 0) \in \mathbf{Z}_{11} \times \mathbf{Z}_{17}$ stellt die Größe $34 \in \mathbf{Z}_{187}$ dar (dies sieht man entweder "so", oder man entnimmt es der Gleichung $1 = 2 \cdot 17 + (-3) \cdot 11$, die man ebenfalls mit dem erweiterten euklidischen Algorithmus erhält). Also steht $(8, -1)$ für die Größe $(6 \cdot 34 + 101) \bmod 187 = 305 \bmod 187 = 118$. Die Klartext-Botschaft lautet somit $x = 118$.

Literatur

- [1] O. Forster. *Algorithmische Zahlentheorie*. Vieweg-Verlag, 1996.
- [2] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics*. Addison-Wesley, second edition, 1994.