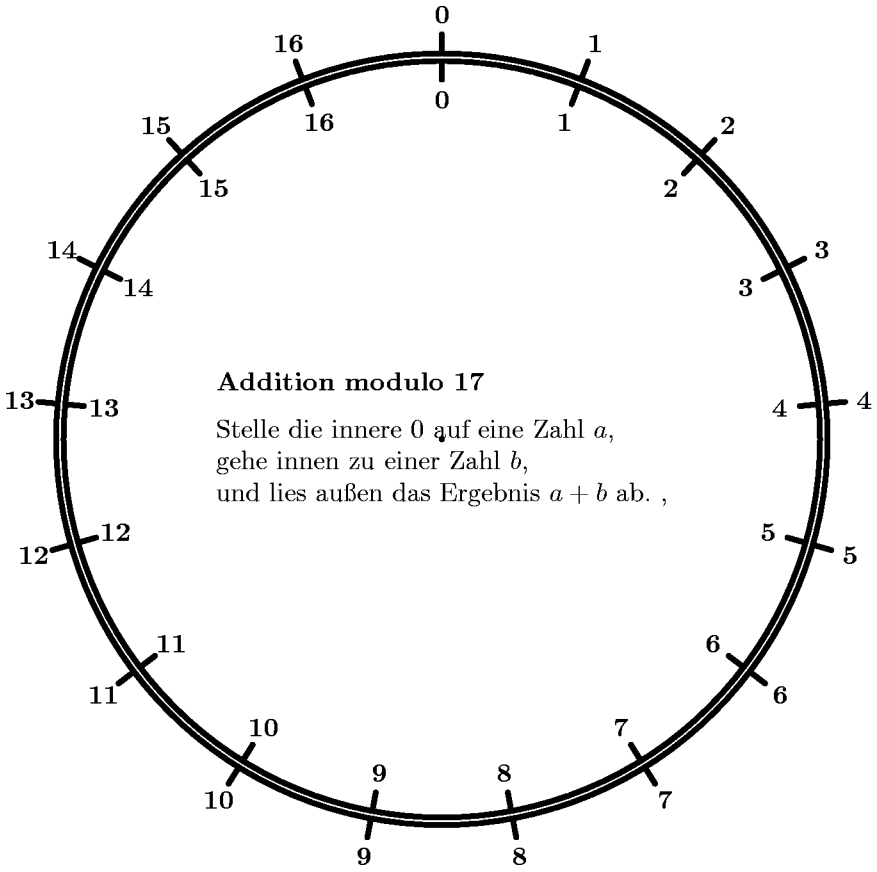
Rechnen modulo 17 – Die Uhrenarithmetik

Rechnen modulo einer Zahl N bedeutet Rechnen bis auf Vielfache dieser Zahl. Vielfache von N werden ignoriert bzw. als Null angesehen. Dies kennen Sie etwa an der Uhr, wo 12 und 0 dasselbe sind und nach 12 die 1 folgt.

Nimmt man statt der 12 eine Primzahl, so hat man eine Reihe von interessanten Besonderheiten. Wir nehmen hier einmal die Primzahl 17 als Beispiel. Man rechnet modulo 17 wie üblich, nur dass hinter der 16 die Zahlen wieder bei 0 beginnen. 17 ist also dasselbe wie 0, 18 ist 1, 19 ist 2 ...

Die folgende Rechenscheibe dient der Additon modulo 17:



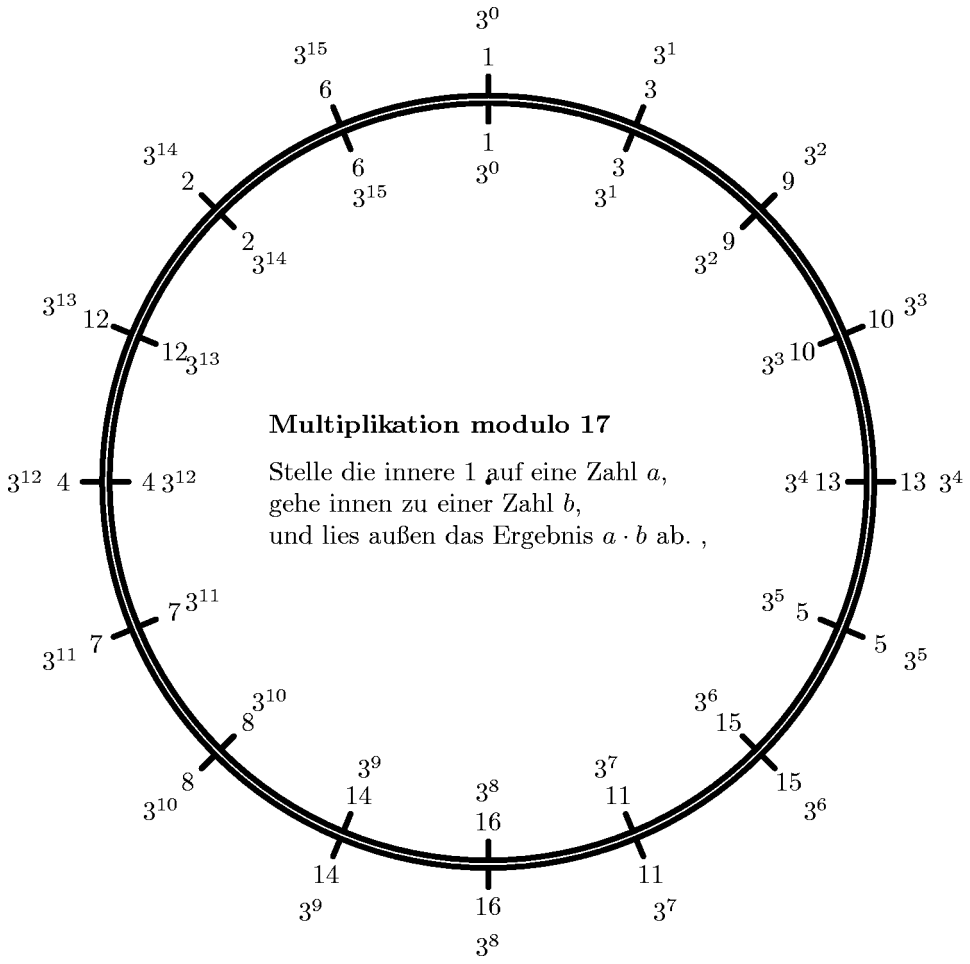
So ist etwa $13 + 8 = 21 \equiv 4 \bmod 17$, $12 + 13 = 25 \equiv 8 \bmod 17$. In gleicher Weise kann man auch subtrahieren: $4 - 9 = -5 \equiv 12 \bmod 17$.

Die Multiplikation: Wenn man addieren kann, kann man auch multiplizieren. So ist etwa $5 \cdot 4 = 20 \equiv 3 \bmod 17$, $9 \cdot 2 = 18 \equiv 1 \bmod 17$. Diese letzte Gleichung besagt, dass 9 gleich $\frac{1}{2}$ ist (modulo 17!).

Potenzen: Wir berechnen als Beispiel einmal alle Potenzen von 3 modulo 17: $3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv 10 \bmod 17$, $3^4 = 3 \cdot 10 = 30 \equiv 13 \bmod 17$, $3^5 = 3 \cdot 13 = 39 = 5 \bmod 17$ ...

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^n	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Es fällt auf, dass jede Zahl $\neq 0$ eine Potenz von 3 ist. Außerdem stellt man fest $3^{16} = 3 \cdot 3^{15} = 3 \cdot 6 = 18 \equiv 1 \bmod 17$. Daraus ergibt sich die folgende Multiplikationsscheibe:



Diese Multiplikationsscheibe funktioniert nach dem Prinzip des Rechenschiebers. Statt die Zahlen zu multiplizieren, werden diese als Potenzen von 3 dargestellt und deren Exponenten addiert. (Diese Exponenten sind gerade die Logarithmen zur Basis 3.)

Potenzen und Wurzeln: Die Tatsache, dass alle Zahlen (außer der 0) eine Potenz von 3 sind und außerdem $3^{16} = 1 \bmod 17$ ist, hat zur Folge: Jede Zahl $a \neq 0 \bmod 17$ hat als 16te Potenz den Wert 1: Denn a ist eine Potenz von 3: $a = 3^n$ und daher $a^{16} = 3^{n \cdot 16} = (3^{16})^n = 1^n = 1 \bmod 17$. Daraus folgen interessante Beziehungen:

$$\begin{aligned} a^{16} = 1 \quad &\Longrightarrow \quad a^{17} = a \quad | \quad \cdot a^{16} = 1 \\ &\Longrightarrow \quad a^{33} = a \quad | \quad \cdot a^{16} = 1 \\ &\Longrightarrow \quad a^{49} = a \quad | \quad \cdot a^{16} = 1 \\ &\Longrightarrow \quad a^{65} = a \end{aligned}$$

Etwa aus $a^{33} = a$ erhält man

$$a = a^{33} = a^{3\cdot 11} = (a^3)^{11}\,.$$

Dies bedeutet: Man zieht die dritte Wurzel, indem man mit 11 potenziert! Dies funktioniert in ähnlicher Weise für jeden ungeraden Exponenten:

$$(a^5)^{13} = a^{65} = a \bmod 17 \quad (a^7)^7 = a^{49} = a \bmod 17,$$

Kryptographie – Eine erste Idee: Diese letztgenannten Beziehungen enthalten eine der Grundideen zur Verschlüsselung mittels Zahlentheorie. Benutzt man die 16 Zahlen von 1 bis 16 als (verkürztes) Alphabet, so kann man die Potenzierung mit 3 als *Ver*schlüsselung und die Potenzierung mit 11 als *Ent*schlüsselung benutzen:

Verschlüsselung: $a \mapsto a^3$, Entschlüsselung: $b \mapsto b^{11}$.

Unterwirft man die verschlüsselte 'Nachricht' a^3 der Entschlüsselung $(a^3)^{11} = a^{33}$, so erhält man wegen $a^{33} = a \bmod 17$ wieder den Klartext a.

Ein besonders günstiger Aspekt dieses Verfahrens ist, dass man zur Ver- und Entschlüsselung dasselbe Verfahren benutzen kann (Potenzierung) und dass die Reihenfolge von Ver- und Entschlüsselung ausgetauscht werden kann. Dies eröffnet interessante Möglichkeiten in der Kryptographie.

Die Anwendbarkeit des Verfahrens hängt nun entscheidend davon ab, ob und wie leicht man zum Verschlüsselungsexponten 3 den Entschlüsselungsexponenten 11 ermitteln kann.