5. Ein paar Anwendungen

Berechnung des Wochentags zu gegebenem Datum

Aus $365 \equiv 1 (7)$ (bzw. $366 \equiv 2 (7)$) folgt, dass sich der Wochentag zu einem gegebenen Datum von einem Jahr zum nächsten um einen Tag verschiebt (bzw. um zwei Tage, wenn wegen eines Schaltjahrs ein 29. Februar dazwischen liegt).
Der 16. Juni 2025 ist ein Montag. Der 16. Juni wird daher 2026 ein Dienstag, 2027 ein Mittwoch und 2028 ein Freitag sein (da 2028 ein Schaltjahr ist).
Dabei muss man berücksichtigen:

- Ein Jahr ist ein Schaltjahr, wenn die Jahreszahl durch 4 teilbar ist.
  Ausgenommen sind davon Jahreszahlen, die durch 100 teilbar sind.
  Ausnahmen von der Ausnahme sind Jahreszahlen, durch 400 teilbar sind.
  (z.B. war 2000 ein Schaltjahr, aber 2100 wird kein Schaltjahr sein.)
- Diese Berechnung ist nur sinnvoll für Daten nach der Einführung des Gregorianischen Kalenders. Dieser wurde 1582 von Papst GREGOR XIII veranlasst, in verschiedenen Ländern aber erst später eingeführt (z.B. in England erst 1752).

Beispiel: Welcher Wochentag war der 1. April 2000? Der 1. April 2025 war ein Dienstag. Das Jahr 2000 war 25 Jahre früher, darunter die sechs Schaltjahre 2004, 2008, 2012, 2016, 2020 und 2024. (Das Jahr 2000 war ein Schaltjahr, muss aber nicht berücksichtigt werden, da der 29.2.2000 nicht in den Zeitraum zwischen 1.4.2000 und 1.4.2025 fällt.) Der Wochentag muss daher um $25+6=31$ Tage (zurück) verschoben werden. Wegen $-31 \equiv 4 (7)$ war der 1. April 2000 ein Samstag.

Prüfziffern

Prüfziffern werden verwendet, um die Korrektheit von Daten zu gewährleisten (wie z.B. Kontonummern, Kreditkartennummern, Sozialversicherungsnummern, ISBN, Seriennummern von Geldscheinen). Ziel ist es Fehler zu erkennen, wie z.B. Vertipen oder Verschreiben bei einer einzelnen Ziffer oder Zahlendrehen (d.h. Vertauschen von zwei benachbarten Ziffern).
Eine Möglichkeit ist die Verwendung von Quersummen. Man kann einer Zahl z.B. eine Ziffer hinzufügen, derart dass die Quersumme durch 10 teilbar ist. Z.B. hat die Zahl 2347 Quersumme $2+3+4+7=16$. Fügt man die Prüfziffer 4 hinzu, so hat 23474 Quersumme $2+3+4+7+4=20 \equiv 0 (10)$
Einzelne falsche Ziffern werden dadurch erkannt. Schreibt man versehentlich 25474, so ist $2+5+4+7+4 = 22 \equiv 2 \not\equiv 0 (10)$. Zahlendrehen werden aber nicht entdeckt, da die Quersumme gleich bleibt.

Es ist darum besser, gewichtete Quersummen zu verwenden. Ein Bsp. dafür ist ISBN (International Standard Book Number), die zur eindeutigen Kennzeichnung von Büchern verwendet wird. Seit 2007 wird nur noch das ISBN-13-System verwendet. Jeder ISBN-13-Code besteht aus 13 Ziffern. Die ersten 3 Ziffern sind ein Präfix (978 oder 979), gefolgt von Informationen über Sprache oder Land (1 bis 5 Ziffern, z.B. „3" für deutschsprachige Bücher mit Präfix 978 und „0" oder „1" für englischsprachige Bücher mit Präfix 978), Verlag und Titel (zusammen 8 Ziffern für deutschsprachige Bücher). Die 13. Ziffer ist die Prüfziffer und wird folgendermaßen bestimmt: Ist der ISBN-Code $a_1 a_2 \dots a_{13}$ (mit $a_j \in \{0,1,\dots,9\}$ für $1 \le j \le 13$), so ist

$$a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + a_{13} \equiv 0 \ (13)$$

oder kurz

$$\sum_{\substack{1 \le j \le 13 \\ 2 \nmid j}} a_j + 3 \sum_{\substack{1 \le j \le 13 \\ 2 \mid j}} a_j \equiv 0 \ (3),$$

d.h. jede zweite Ziffer wird mit Gewicht 3 versehen. Z.B. hat das Buch „Zahlen, Formeln, Gleichungen" von A. BEUTELSPACHER den ISBN-Code 978-3-658-16105-7, den wir überprüfen:

$$9 + 3\cdot 7 + 8 + 3\cdot 3 + 6 + 3\cdot 5 + 8 + 3\cdot 1 + 6 + 3\cdot 1 + 0 + 3\cdot 5 + 7 = 110 \equiv 0 \ (10)$$

oder geschickter

$$9 + 3\cdot 7 + 8 + 3\cdot 3 + 6 + 3\cdot 5 + 8 + 3\cdot 1 + 6 + 3\cdot 1 + 0 + 3\cdot 5 + 7$$
$$\equiv -1 + 1 - 2 - 1 - 4 + 5 - 2 + 3 - 4 + 3 + 5 - 3 \equiv 0 \ (10)$$

- Einzelne falsche Ziffern werden entdeckt. Sind $a, b \in \{0,1,\dots,9\}$, so gelten $a \equiv b \ (10) \Rightarrow a = b$ bzw. $3a \equiv 3b \ (10) \xrightarrow{\text{Kor. 40 (vii)}} a \equiv b \ (10) \Rightarrow a = b$. Ist also $a \neq b$, so ist $a \not\equiv b \ (10)$ bzw. $3a \not\equiv 3b \ (10)$.
- Die meisten (aber nicht alle) Zahlendrehen werden entdeckt. Sind wieder $a, b \in \{0,1,\dots,9\}$, so ist

$$3a + b \equiv a + 3b \ (10) \iff 2a \equiv 2b \ (10) \xleftarrow{\text{Kor. 39 (v)}} a \equiv b \ (5) \iff |a-b| = 5$$

Bei der Vertauschung benachbarter Ziffern, die sich um 5 unterscheiden, wird nicht erkannt (d.h. $0 \leftrightarrow 5$, $1 \leftrightarrow 6$, $2 \leftrightarrow 7$, $3 \leftrightarrow 8$, $4 \leftrightarrow 9$). Werden z.B. im Block 16105 des ISBN-Codes des Buchs von Beutelspacher 1 und 6 vertauscht (d.h. 11605 oder 61105), so wird das nicht erkannt, da $3\cdot 1 + 6 = 9 \equiv 19 = 3\cdot 6 + 1 \ (10)$. ⊛

Tatsächlich war das zuvor verwendete ISBN-10-System in dieser Hinsicht sicherer

16.6.2025

Jeder ISBN-10-Code bestand aus 10 Ziffern, wobei die 10. Ziffer die Prüfziffer war. War der Code $a_1 a_2 \dots a_{10}$, musste die Bedingung

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10} \equiv 0 \ (11)$$

oder kurz $\sum_{j=1}^{10} (11-j)\, a_j \equiv 0 \ (11)$ erfüllt sein, d.h. jede Ziffer hatte ein anderes Gewicht.

Da es sich dabei um Kongruenzen modulo 11 handelte, war es möglich, dass $a_{10} = 10$ sein musste. In diesem Fall verwendete man X als 10. Ziffer (also „römisch 10^{N}"). Z.B. hat das Buch „Introduction to Cryptography" von J.A. BUCHMANN ISBN-Code 0-387-21156-X, den wir überprüfen:

$$10\cdot 0 + 9\cdot 3 + 8\cdot 8 + 7\cdot 7 + 6\cdot 2 + 5\cdot 1 + 4\cdot 1 + 3\cdot 5 + 2\cdot 6 + 10 = 198 = 18\cdot 11 \equiv 0 \ (11)$$

oder geschickter

$$10\cdot 0 + 9\cdot 3 + 8\cdot 8 + 7\cdot 7 + 6\cdot 2 + 5\cdot 1 + 4\cdot 1 + 3\cdot 5 + 2\cdot 6 + 10$$
$$\equiv \cancel{8} - 2 + \cancel{8} + \cancel{1} + 5 + 4 + 4 + \cancel{X} - \cancel{X} \equiv 0 \ (11)$$

- Einzelne falsche Ziffern werden entdeckt. Sind $a, b \in \{0,1,\dots,10\}$ und $g \in \{1,2,\dots,10\}$, so gilt $ga \equiv gb \ (11) \xrightarrow{\text{Kor. 4.0 (vii)}} a \equiv b \ (11) \Rightarrow a = b$. Aus $a \neq b$ folgt daher $ga \not\equiv gb \ (11)$.
- Alle Zahlendreher werden entdeckt. Sind $a, b \in \{0,1,\dots,10\}$ und $g \in \{1,2,\dots,9\}$, so ist $(g+1)a + gb \equiv (g+1)b + ga \ (11) \Rightarrow a \equiv b \ (11) \Rightarrow a = b$. Ist also $a \neq b$, so ist $(g+1)a + gb \not\equiv (g+1)b + ga \ (11)$.

RSA-Verschlüsselung

Um vertrauliche oder geheime Informationen zu schützen, werden sie verschlüsselt. Ein schon von Julius Cäsar verwendetes Verschlüsselungsverfahren verschiebt alle Buchstaben zyklisch im Alphabet, z.B.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

REVOLUTION wird so z.B. zu VIZSPYXMSR. Verschlüsselungsverfahren ist dabei die Caesar-Verschlüsselung und A→E der Schlüssel. Der Schlüssel ist derselbe für Ver- und Entschlüsselung und muss geheim gehalten werden. (Diese Verschlüsselung ist relativ leicht zu knacken, da in jeder Sprache verschiedene Buchstaben mit verschiedener Häufigkeit auftreten. Im Deutschen sind die fünf häufigsten Buchstaben z.B.: E: 17,40%, N: 9,78%, I: 7,55%, S: 7,27% und R: 7,00% und machen daher knapp die Hälfte aller Buchstaben in deutschen Texten aus.)

Im Jahr 1978 publizierten R. RIVEST, A. SHAMIR und L. ADLEMAN ein Verschlüsselungsverfahren mit verschiedenen Schlüsseln für Ver- und Entschlüsselung. Der Schlüssel für die Verschlüsselung braucht nicht geheim gehalten werden. Das Verfahren wird - nach den Anfangsbuchstaben ihrer Namen - RSA-Verschlüsselung genannt. Seine Sicherheit beruht darauf, dass es viel einfacher ist, zwei (große) Primzahlen (mit dem Computer) zu multiplizieren, als die Primfaktorzerlegung des Produkts zu finden.

Alice will eine verschlüsselte Nachricht an Bob schicken. Bob stellt den Schlüssel für die Verschlüsselung folgendermaßen bereit:

- Bob wählt zwei (große) Primzahlen p und q und berechnet $n = pq$
- Bob wählt eine Zahl e mit den Eigenschaften $1 < e < \varphi(n) = (p-1)(q-1)$ und $ggT(e, \varphi(n)) = ggT(e, (p-1)(q-1)) = 1$. (Da $2 | (p-1)$ und $2 | (q-1)$, muss $2 \nmid e$ gelten.)
- Bob berechnet eine Zahl d mit den Eigenschaften $1 < d < \varphi(n) = (p-1)(q-1)$ und $de \equiv 1 \pmod{(p-1)(q-1)}$. (Ein solches d existiert wegen Satz 46 und kann z.B. mit Hilfe des Euklidischen Algorithmus gefunden werden.)
- Bobs öffentlicher Schlüssel ist das Paar (n, e), das er nicht geheimhalten muss. Sein privater Schlüssel ist d, das er (ebenso wie p und q) geheim hält.

Alice geht bei der Verschlüsselung folgendermaßen vor:

- Alice verwandelt ihren zu verschlüsselnden Text in eine Zahl m. (z.B. durch ersetzen $A \to 01$, $B \to 02, \ldots, Z \to 26$). Ist dabei $m \geq n$, so wird die Zahl in Blöcke zerlegt, die einzeln verschlüsselt werden. Ist $m < n$, so kann dieser Schritt entfallen (wovon wir ab jetzt ausgehen).
- Um den Klartext m zu verschlüsseln, berechnet Alice $c \equiv m^e \pmod{n}$ mit $0 \leq c < n$. (Das kann sie, da sie (n, e) kennt.)

Um die verschlüsselte Nachricht zu entschlüsseln, berechnet Bob c^d modulo n. Wir behaupten, dass er so m zurück erhält, d.h. dass $c^d \equiv (m^e)^d \equiv m \pmod{n}$ gilt.

Beweis: Da $de \equiv 1 \pmod{(p-1)(q-1)}$ gibt es ein $\ell \in \mathbb{Z}$, sodass $de = 1 + \ell(p-1)(q-1)$ und daher $(m^e)^d = m^{de} = m^{1+\ell(p-1)(q-1)} = m \left(m^{(p-1)(q-1)}\right)^\ell$.

Wir zeigen zunächst $(m^e)^d \equiv m \pmod{p}$:

Falls $p \nmid m$, so $m^{p-1} \equiv 1 \pmod{p}$ nach Kor. 55 (i) und daher

$$(m^e)^d = m \left((m^{p-1})^{q-1}\right)^\ell \equiv m \cdot (1^{q-1})^\ell = m \pmod{p}$$

Falls $p \mid m$, so $(m^e)^d \equiv 0 \equiv m \pmod{p}$.

Völlig analog zeigt man $(m^e)^d \equiv m \pmod{q}$. Daher ist $(m^e)^d - m$ gemeinsames Vielfaches von p und q. Nach Satz 27 gilt $kgV(p,q) \mid ((m^e)^d - m)$, d.h. $pq \mid ((m^e)^d - m)$ wegen Korollar 34. Also gilt $n \mid ((m^e)^d - m)$ und daher $c^d \equiv (m^e)^d \equiv m \pmod{n}$.

Beispiel: Bob wählt $p = 11$, $q = 23$ $\Rightarrow n = pq = 253$ und $\varphi(n) = (p-1)(q-1) = 10 \cdot 22 = 220$
Weiters wählt er $e = 3$ (was die Bedingung $ggT(e, \varphi(n)) = 1$ erfüllt). Um d zu finden, kann man folgendermaßen vorgehen: $220 = 73 \cdot 3 + 1 \Rightarrow 1 \cdot 220 + (-73) \cdot 3 = 1$
$\Rightarrow (1-3) \cdot 220 + (220-73) \cdot 3 = 1 \Rightarrow (-2)\,220 + 147 \cdot 3 = 1 \Rightarrow 147\,3 \equiv 1\ (220)$, also $d = 147$
Um den Klartext $m = 165$ zu verschlüsseln, berechnet Alice $m^e = 165^3 \equiv 110 = c\ (253)$.
Um den Klartext zu finden, berechnet Bob $c^d = 110^{147} \equiv 165\ (253)$.

Bemerkungen: 1) Die Primzahlen p und q müssen so groß sein, dass es sehr zeitaufwendig ist $n = pq$ in Primfaktoren zu zerlegen. Da p und q müssen hunderte Stellen lang sein. (Die Primzahlen in unserem Beispiel sind viel zu klein.)
2) Die Wahl der Primzahlen p und q und der Zahl e kann nicht völlig beliebig erfolgen, da eine ungeschickte Wahl Möglichkeiten eröffnet, die Verschlüsselung zu knacken.
3) Die im Verfahren auftretenden Ausdrücke wie m^e und c^d modulo n sind auch für große Zahlen schnell zu berechnen, da man nur ihren Rest modulo n benötigt, wofür es effiziente Algorithmen gibt.

23.6.2025