Österreichische Mathematische Gesellschaft

MATHE-BRIEF

Dezember 2015 — Nr. 64

Herausgegeben von der Österreichischen Mathematischen Gesellschaft
http://www.oemg.ac.at/Mathe–Brief ——— mathe–brief@oemg.ac.at

How to Share a Secret

Die Aufgabe. Stellen Sie sich vor, Sie wären in einem großen Betrieb für die Sicherheit der geheimsten Herstellungsmethoden (Rezepte, Materialmischungen, ...) verantwortlich. Es sollte nicht ein Einziger Zugang zum Tresor mit den „großen Geheimnissen“ haben, sondern es sollten nur mehrere gleichzeitig den Tresor öffnen können. Es soll ja schon vorgekommen sein, dass sich der Herr Generaldirektor persönlich am Tresor bereichert hat. Auch Generaldirektoren sind nur Menschen!

Die Grundidee der Lösung. Einer der Erfinder des wohl besten Verschlüsselungssystems für geheime Nachrichten, Adi Shamir, hat auch für diese Situation ein geniales (d.h. einfaches und wirksames) Verfahren entdeckt. Es ist tatsächlich im Einsatz, zum Beispiel bei der VOEST (bzw. deren Nachfolgeorganisationen).

Sagen wir, es sollen erst immer 4 Personen von 100 Angestellten in der Lage sein, den Tresor zu öffnen. Wir wählen zufällig ein Polynom

$$f = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

mit ganzzahligen Koeffizienten a_i. Dann berechnen wir die 100 Paare

$$(1, f(1)), \quad (2, f(2)), \ \ldots \quad (100, f(100))$$

und verteilen diese 100 Werte auf Chipkarten an die 100 Angestellten. Der geheime Schlüssel ist der Wert a_0.

Kommen nun 4 Personen zusammen und stecken ihre Chipkarten in einen Rechner, so kennt der Rechner die vier x- und die zugehörigen y-Werte, kann z.B. mit der Lagrangeschen Interpolationsformel das Polynom f eindeutig identifizieren, den Wert $a_0 = f(0)$ berechnen und nachprüfen, ob das mit dem Schlüssel übereinstimmt. Denn 2 Punkte bestimmen genau eine Gerade, 3 Punkte genau eine Parabel, 4 Punkte genau ein Polynom vom Grad 3 (immer mit verschiedenen x-Werten) u.s.f. Aber ist dies wirklich sicher? Kennt der Herr Generaldirektor vielleicht doch den geheimen Schlüssel? Wir müssen uns absichern.

Absicherung 1. Oben steht: „Wir wählen zufällig ein Polynom...“. Wer ist „wir”? Sobald es eine Person involviert, ist schon Gefahr am Dach. Das Polynom sollte ein Zufallsgenerator in einem wirklich geschützten Teil eines Computers sein, den niemand auslesen kann.

Absicherung 2. Was passiert, wenn eine Chipkarte verlorengeht? Ein Dieb müsste nur 4 Chipkarten sammeln, um den Tresor ganz alleine öffnen zu können. In diesem Fall wählt man ein anderes Polynom und erneuert alle Chipkarten. Einzelne der alten Chipkarten sind nicht gemeinsam mit den neuen Chipkarten verwendbar.

Durchführung der Interpolation. Das Auswerten und das Interpolieren von Polynomen wurde bereits im Mathe-Brief 57 besprochen. Es gibt noch andere Interpolationsverfahren; wir wollen kurz das (eher unbekannte) *Verfahren von Neville-Aitken* vorstellen. Es hat den großen Vorteil, bei Hinzunahme eines weiteren Interpolationspunktes nicht wieder von vorne beginnen zu müssen; das vorhandene Interpolationspolynom kann einfach adaptiert werden, um den neuen Punkt auch „mitzunehmen".

Gegeben seien paarweise verschiedene reelle Werte $x_1, x_2, \ldots, x_n$ sowie weitere reelle Werte $y_1, y_2, \ldots, y_n$. Wir suchen das eindeutig bestimmte Polynom f vom Grad $n-1$, das an den Stellen x_i die Funktionswerte y_i hat; i läuft dabei von 1 bis n. Es ist sehr einfach, ein Polynom $f_{1,1}$ zu finden, das die Interpolationsaufgabe an der ersten Stelle löst: wir nehmen einfach das konstante Polynom

$$f_{1,1} = y_1.$$

Um auch an der Stelle x_2 den gewünschten Wert y_2 zu erhalten, berechnen wir das Polynom

$$f_{1,2} = \frac{(x-x_1)y_2 - (x-x_2)y_1}{x_2 - x_1}.$$

Wie man durch Einsetzen sofort sieht, gilt $f_{1,2}(x_1) = y_1$ und $f_{1,2}(x_2) = y_2$. Allgemeiner löst für jedes i zwischen 1 und $n-1$ das Polynom

$$f_{i,i+1} = \frac{(x-x_i)y_{i+1} - (x-x_{i+1})y_i}{x_{i+1} - x_i}$$

die Interpolationsaufgabe an den Stellen Nummer i und $i+1$. Setzen wir $f_{k,k} = y_k$ für alle $k = 1, \ldots, n$, können wir für $i < j$ schrittweise das Polynom

$$f_{i,j} = \frac{(x-x_i)f_{i+1,j} - (x-x_j)f_{i,j-1}}{x_j - x_i}$$

berechnen. Der Grad dieses Polynoms ist j-i. Wie sieht man das ein? Für $i = j$ ist das klar, weil $f_{i,i} = y_i$ eine Konstante, also ein Polynom vom Grad 0 ist. Wenn unsere Vermutung aber für alle Indexdifferenzen kleiner als $j-i$ zutrifft, dann sind $f_{i+1,j}$ und $f_{i,j-1}$ Polynome des Grades $j-i-1$ und unsere Formel für $f_{i,j}$ liefert offenbar ein Polynom des Grades $j-i$.
Darüber hinaus nimmt das Polynom $f_{i,j}$ an den Stellen $x_i, x_{i+1}, \ldots, x_j$ der Reihe nach die Funktionswerte $y_i, y_{i+1}, \ldots, y_j$ an. Wie kann man das einsehen? Für $f_{i,i+1}$ haben wir das gerade nachgeprüft. Wenn unsere Behauptung für die Polynome $f_{i+1,j}$ und $f_{i,j-1}$ zutrifft, also

$$\begin{aligned} f_{i+1,j}(x_k) &= y_k \qquad \text{für } i+1 \le k \le j \quad \text{und} \\ f_{i,j-1}(x_k) &= y_k \qquad \text{für } i \le k \le j-1, \end{aligned}$$

dann liefert die Formel für $f_{i,j}$ tatsächlich $f_{i,j}(x_k) = y_k$, wenn $i+1 \le k \le j-1$. Dass $f_{i,j}(x_i) = f_{i,j-1}(x_i) = y_i$ und $f_{i,j}(x_j) = f_{i+1,j}(x_j) = y_j$ ist, kann man direkt nachrechnen.
Unsere gesuchte Gesamtlösung f ist dann natürlich $f = f_{1,n}$. Praktischerweise berechnet man alles nach dem Schema

$$\begin{array}{ccccccc} f_{1,1} & & & & & & \\ & \searrow & & & & & \\ f_{2,2} & \to & f_{1,2} & & & & \\ & \searrow & & \searrow & & & \\ f_{3,3} & \to & f_{2,3} & \to & f_{1,3} & & \\ & \searrow & & \searrow & & \searrow & \\ f_{4,4} & \to & f_{3,4} & \to & f_{2,4} & \to & f_{1,4}. \end{array}$$

Ein Beispiel. Das Geheimnis lautet 3081, und der Computer wählt das Polynom

$$f(x) = 3081 + 4x - 133x^2 + 2x^3.$$

Es werden nun die Schlüssel

$$\begin{array}{llllll} (1,f(1)) & (2,f(2)) & (3,f(3)) & (4,f(4)) & (5,f(5)) & \dots \quad (100,f(100)), \text{ d.h.} \\ (1,2954) & (2,2573) & (3,1950) & (4,1097) & (5,26) & \dots \quad (100,673481), \end{array}$$

an die Mitarbeiter ausgegeben. Angenommen, die Mitarbeiter Nr. 1, 2, 3 und 5 kommen zusammen und möchten Zugang zum Tresor. Man muss nun ein Polynom f finden, welches an den Stellen $x = 1, 2, 3, 5$ die Werte $y = 2954, 2573, 1950, 26$ annimmt. Im obigen Schema erhalten wir:

$$\begin{array}{lllll} f_{1,1} = 2954 & & & & \\ \qquad \searrow & & & & \\ f_{2,2} = 2573 \to & f_{1,2} = 3335 - 381x & & & \\ \qquad \searrow & \qquad \searrow & & & \\ f_{3,3} = 1950 \to & f_{2,3} = 3819 - 623x \to & f_{1,3} = 3093 - 18x - 121x^2 & & \\ \qquad \searrow & \qquad \searrow & & \qquad \searrow & \\ f_{4,4} = 26 \quad \to & f_{3,4} = 4836 - 962x \to & f_{2,4} = 3141 - 58x - 113x^2 \to & f_{1,4} = 3081 + 4x - 133x^2 + 2x^3. \end{array}$$

Und, in der Tat, $f_{1,4}$ ist das gesuchte Polynom, das vorher der Computer gewählt hat.

Absicherung 3. Das Rechnen mit reellen Zahlen oder auch mit ganzen Zahlen ist nicht praktikabel, wegen der unvermeidlichen Rundungsfehler und weil Computer keine unendlichen Zahlbereiche haben. Daher werden in de Praxis alle Rechnungen modulo einer großen Primzahl p durchgeführt. Man ersetzt alle vorkommenden Zahlen x_i und $y_i = f(x_i)$ durch deren Reste bei Division durch p. Die Interpolationsformel bleibt dadurch, wie man zeigen kann, weiterhin gültig. Hält man die Primzahl p ebenfalls geheim, so werden alle Rechnungen für Außenstehende noch weniger nachvollziehbar.*

Rechenbeispiele. Will man z.B. in einem (viel zu kleinen) Beispiel $5 \cdot 16$ berechnen, so ergibt sich als Ergebnis 12 bei $p = 17$, dagegen 4 bei $p = 19$ und 80 bei $p = 87$. Man wendet dabei also die „modulare Arithmetik“ an, der wir bereits im Mathe-Brief 57 begegnet sind. Nach der Wahl von p kann man die vier Grundrechnungsarten und auch Potenzieren ebenso ausführen wie in den ganzen Zahlen, nur dass alle Ergebnisse nach Division durch p im Bereich $0, 1, 2, \dots, p-1$ landen. Das gibt zwar „exotische“ Ergebnisse, aber wir sind dadurch vor Kommazahlen gefeit. Und das *secret*, das wir teilen wollen, bleibt noch geheimer.

Für ein paar Beispiele fixieren wir die Primzahl $p = 31$ (eigentlich viel zu klein), schreiben Zwischenergebnisse, vor Division durch 31, in runden Klammern an und erhalten

$$14 + 20 = (34) = 3 \qquad 14 - 20 = (-6) = (31 - 6) = 25 \qquad (\textit{Probe:}\ 25 + 20 = (45) = 14)$$
$$14 \cdot 20 = (280) = 1 \qquad 14/20 = 10 \qquad (\textit{Probe:}\ 20 \cdot 10 = (200) = 16)$$

*Wenn man mit den Zahlen $\{0, 1, 2, \dots, p-1\}$ auf die beschriebene Art rechnet, bleibt man stets in diesem Bereich, den man meist mit $\mathbb{Z}_p$ bezeichnet und dessen Elemente $0, 1, 2, \dots, p-1$ dann die „Restklassen modulo p“ heißen.

Die Zahl $10 = 14/20$ kann man durch Probieren finden, denn sie muss ja eine der Zahlen 0, 1, $2, \ldots 30$ sein.[**] Potenzen wie 14^{20} berechnet man am besten durch *square and multiply*:

$$14^2 = (196) = 10 \implies 14^4 = 14^2 \cdot 14^2 = 10 \cdot 10 = (100) = 7 \implies 14^8 = 7 \cdot 7 = 18$$
$$\implies 14^{16} = 18 \cdot 18 = (324) = 14 \implies 14^{20} = 14^{16} \cdot 14^4 = 14 \cdot 7 = (98) = 5.$$

G. Pilz

[**] Das ist eine ziemlich blöde Methode, wenn p zum Beispiel 100-stellig ist. Eine „rechnerische“ Methode ist die folgende: Es reicht natürlich, den Wert von $1/20$ zu wissen. Intime Kenner der Berechnung größter gemeinsamer Teiler zweier Zahlen a, b sind klar im Vorteil: Sie wissen, dass man durch Kettendivision ganze Zahlen x und y findet, sodaß $\mathrm{ggT}(a,b) = a \cdot x + b \cdot y$ gilt. Hier berechnen wir $1 = \mathrm{ggT}(20,31) = 20 \cdot 14 + 31 \cdot (-9)$. Betrachtet man dieselbe Gleichung modulo 31, so wird sie zu $1 = 20 \cdot 14$, woraus wir $1/20 = 14$ erkennen. Damit ist $14/20 = 14 \cdot \frac{1}{20} = 14 \cdot 14 = 10$. Allgemein ist bei einem gegebenen primen p und einer natürlichen Zahl $a < p$ der Wert von $1/a$ also so zu finden: $\mathrm{ggT}(a,p) = 1$, also gibt es ganzzahlige x, y mit $1 = a \cdot x + p \cdot y$. Geht man über zu Resten bei Division durch p, wird p zu 0 und wir erhalten wir $1 = a \cdot x$. Die Zahl x ist also gerade der gesuchte Kehrwert $1/a$.