Österreichische Mathematische Gesellschaft

MATHE-BRIEF

Juni 2016 — Nr. 70

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

VERBLÜFFENDE MATHEMATIK

„Denke Dir eine beliebige ganze Zahl, ohne sie mir bekanntzugeben. Subtrahiere 1*, verdopple das Resultat, addiere dazu die gedachte Zahl und sage mir nun das Ergebnis. Die gedachte Zahl war…“*

Mit solchen und ähnlichen Tricks lassen sich vielleicht Volksschüler beeindrucken, aber jeder, der mit Unbekannten zu rechnen versteht, wird wissen, dass dahinter nur elementare Umformungen von Gleichungen stecken. Bezeichnet man in obigem Beispiel die gedachte Zahl mit x, so liefern die befohlenen Umformungen schrittweise

$$x \quad\longrightarrow\quad x-1 \quad\longrightarrow\quad 2(x-1) \quad\longrightarrow\quad 2(x-1)+x=3x-2,$$

und Auflösen der Gleichung nach der bekanntgegebenen Zahl $y=3x-2$ nach x liefert

$$x=(y+2)/3.$$

Ein wenig spannender ist da schon folgendes:

> *„Denke an eine ganze Zahl zwischen* 1 *und* 60*. Teile sie durch* 3,4 *und* 5 *und gib mir jeweils den dabei übrig bleibenden Rest mit. Du hast an … gedacht.“*

Hier findet man nicht mit dem Umformen von Gleichungen das Auslangen: der mathematische Hintergrund ist das simultane Lösen von Kongruenzen, genauer eine Anwendung des Chinesischen Restsatzes. In der Tat sind die Moduln $3,4,5$ paarweise zueinander teilerfremd, sodass genau eine Lösung x_0 des Systems von Kongruenzen

$$\begin{aligned} x &\equiv r_1 \pmod 3,\\ x &\equiv r_2 \pmod 4,\\ x &\equiv r_3 \pmod 5 \end{aligned}$$

zwischen 1 und $3\cdot 4\cdot 5=60$ existiert. Um diese schnell im Kopf zu ermitteln, berechnet man zunächst die Größe $S=40r_1+45r_2+36r_3$ (siehe [1], um zu verstehen warum) und ermittelt dann den kleinsten positiven Repräsentanten der Restklasse von $S \mod 60$. Zugegeben, etwas Kopfrechnen muss man dabei schon!

Wer sich auch dadurch nicht beeindrucken lässt, dem imponiert vielleicht die Tatsache, dass sich nicht nur gedachte Zahlen, sondern auch Polynome erraten lassen. Dabei ist nur das Erfragen des Werts des Polynom an vom Ratenden geschickt gewählten Stellen nötig. Das erstaunt zunächst nicht, denn jedes Polynom vom Grad n ist durch seine Werte an beliebigen $n+1$ verschiedenen

Stellen eindeutig bestimmt, worauf auch die Interpolationsformel von Lagrange (siehe [2]) beruht. Doch was, wenn der Grad des gedachten Polynoms dem Ratenden nicht bekannt ist?

Ohne irgendeine weitere Information ist das Erraten dann unmöglich, aber bereits die Einschränkung auf Polynome P mit ganzen, positiven Koeffizienten bewirkt, dass es schon mit nur zwei Fragen gelingt, das gedachte Polynom zweifelsfrei angeben zu können. An welchen zwei Stellen soll man das Polynom also auswerten lassen?

Die erste Frage zielt darauf ab, sich eine Vorstellung von der Größe der Koeffizienten von P zu machen. In der Tat liefert $P(1)$ die Summe der Koeffizienten, und da diese alle positiv sind, muss jeder Koeffizient kleiner oder gleich $P(1)$ sein und daher insbesondere höchstens so viele Stellen (in der Dezimalentwicklung) haben, wie $P(1)$. Bezeichnet k die Anzahl dieser Stellen, so erkundigt man sich als nächstes nach $P(10^k)$ und kann aus dem bekanntgegebenen Wert unmittelbar die Koeffizienten des zu erratenden Polynoms ablesen.

Zur Veranschaulichung gleich ein Beispiel. Angenommen $P(x) = 34x^4 + 15x^2 + 22x + 80$. Dann entnimmt man $P(1) = 151$, dass alle Koeffizienten von P höchstens dreistellig sein können. Den Wert $P(10^3) = 34000015022080$ unterteilt man dann in Dreierblöcke 080, 022, 015, 000 sowie 034 und liest im $i-$ten Block von links den Koeffizienten von x^i in P ab. Die Ganzzahligkeit der Koeffizienten von P und die Kenntnis der maximalen Stellenzahl dieser Koeffizienten bewirkt, dass jeder Koeffizient nur einen Block beeinflusst und so eindeutig erkannt werden kann.

Schwieriger wird es, wenn auch nicht ganzzahlige Koeffizienten zugelassen sind. Dann kann man zwar keine feste Grenze für die Anzahl der nötigen Fragen angeben, aber es ist immer noch möglich aus der Kenntnis von geeignet vielen Werten des Polynoms P an geeigneten Stellen, P eindeutig anzugeben. Genauer, es sind $n+2$ Fragen nötig, wenn P den Grad n hat (den der Ratende jedoch nicht kennt!).

Dazu wählt man eine beliebige arithmetische Progression der Länge $n+2$, am einfachsten die Zahlen $0, 1, 2, \dots, n, n+1$ und beginnt damit, $P(0)$ und $P(1)$ zu erfragen. Gilt $P(1) - P(0) = 1$, so muss P, das ja positive Koeffizienten hat, konstant sein, also $P = P(0)$, fertig.

Ist $P(1) - P(0) > 0$, so fragt man weiter nach $P(2)$ und bildet die Differenzen $P(2) - P(1)$ und $P(1) - P(0)$ und anschließend die Differenz zweiter Ordnung

$$(P(2) - P(0)) - (P(1) - P(0)) = P(2) - 2P(1) + P(0).$$

Ist letztere Differenz gleich 0, so ist P linear und lässt sich durch $P(0)$ und $P(1)$ eindeutig bestimmen. In der Tat sind $P(2) - P(1)$ und $P(1) - P(0)$ Werte des Polynoms $Q(x) = P(x+1) - P(x)$ an den Stellen 0 und 1. Es ist $\deg Q = \deg P - 1$ wie man leicht nachrechnet und Q hat erneut positive Koeffizienten, also folgt aus $Q(0) = Q(1)$, dass Q konstant ist. Q ist wegen $P(1) > P(0)$ nicht identisch Null, sodass P also linear sein muss.

Dieser Prozess der iterativen Differenzenbildung lässt sich induktiv fortsetzen, da beginnend mit einem Polynom P mit $\deg P = n$, $P(x) = \sum_{k=0}^{n} a_i x^i$, mit positiven a_i auch die Koeffizienten von $Q(x) = P(x+1) - P(x)$ erneut positiv sind und $\deg Q = n - 1$. Dies sieht man anhand von

$$\sum_{k=0}^{n} a_k (x+1)^k - \sum_{k=0}^{n} a_k x^k = \sum_{k=0}^{n} a_k \sum_{j=0}^{k-1} \binom{k}{j} x^k.$$

So kommt man bei jedem Polynom vom Grad n ausgehend von $n+2$ Werten nach $n+1$ iterierten Differenzen auf Null und kann $\deg P$ und in der Folge mittels Lagrange Interpolation die Koeffizienten von P unzweifelhaft bestimmen.

Auch dazu ein kurzes Beispiel: das gedachte Polynom sei $x^2+\sqrt{2}x+1/2$. Dann ist

$$P(0)=1/2,\ P(1)=3/2+\sqrt{2},\ \text{also}\ P(1)-P(0)=1+\sqrt{2}\neq 0.$$

Weiters ist $P(2)=4+2\sqrt{2}+1/2$, sodass

$$(P(2)-P(0))-(P(1)-P(0))=2\neq 0.$$

Die Frage nach dem Wert bei 3 ist daher nötig und ergibt $P(3)=9+3\sqrt{2}+1/2$. Nun wird

$$(P(3)-P(2))-(P(2)-P(1))=(5+\sqrt{2})-3+\sqrt{2}=2$$

berechnet, sodass

$$[(P(3)-P(2))-(P(2)-P(1))]-[(P(2)-P(1))-(P(1)-P(0))]=0.$$

Damit steht fest, dass der Grad des gedachten Polynoms $4-2=2$ ist, aus $P(0),P(1),P(2)$ kann P nun ermittelt werden.

LITERATUR

[1] *http://de.wikipedia.org/wiki/Chinesischer_Restsatz*

[2] *http://de.wikipedia.org/wiki/Polynominterpolation#Lagrangesche_Interpolationsformel*

Leonhard Summerer