Elemente der Mathematik, Aufgabe 1414: ggTs rekursiver Folgen

Darij Grinberg*

9. Dezember 2020

1. Aufgabe

Sei n eine positive ganze Zahl. Sei A eine $n \times n$-Matrix mit ganzzahligen Einträgen. Sei v ein Spaltenvektor der Höhe n mit ganzzahligen Einträgen.

Für jede ganze Zahl $m \geq 0$ sei g_m der größte gemeinsame Teiler der n Einträge des Vektors $A^m v$.

Man beweise folgendes: Wenn $g_m = 1$ für mindestens eine ganze Zahl $m \geq n$ gilt, dann gilt $g_m = 1$ für jede ganze Zahl $m \geq 0$.

2. Anmerkungen

Vor langer Zeit habe ich eine schwächere Version eines Spezialfalls ($n = 2$ und $A = \begin{pmatrix} p & q \\ q & p \end{pmatrix}$) der Aufgabe in einem Wettbewerb (5te QEDMO 2007, Aufgabe 1) gestellt.

Es mag natürlich erscheinen, die Aufgabe weiter zu verstärken, indem man vermutet, dass vielleicht $g_{kn} \mid g_n^k$ für jede ganze Zahl $k \geq 1$ gilt. Dies ist aber im Allgemeinen falsch, wie man unschwer einsieht.

3. Lösung

Wir werden zwei Lemmas gebrauchen:[1]

*Drexel University, Korman Center, 15 S 33rd Street, Philadelphia PA, 19104, USA

[1]Wir werden das Symbol 0 freizügig für Nullmatrizen und für Nullvektoren verwenden.

Lemma 3.1. Sei $\mathbb{F}$ ein Körper. Sei A eine $n \times n$-Matrix über $\mathbb{F}$. Sei v ein Spaltenvektor der Höhe n mit Einträgen in $\mathbb{F}$.

Sei $k \geq 0$ eine ganze Zahl. Angenommen, es gilt $A^k v = 0$. Dann ist $A^n v = 0$.

Beweis von Lemma 3.1. Dies ist eine Standardübung in linearer Algebra; der folgende Beweis ist einer der kürzesten:

Sei $\chi_A = \det(tI_n - A) \in \mathbb{F}[t]$ das charakteristische Polynom der Matrix A (wobei I_n die $n \times n$-Einheitsmatrix bezeichnet). Der Satz von Cayley–Hamilton ergibt dann $\chi_A(A) = 0$.

Bekanntlich ist der Polynomring $\mathbb{F}[t]$ ein Hauptidealring. Folglich haben die Polynome χ_A und t^k in $\mathbb{F}[t]$ einen größten gemeinsamen Teiler. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass dieser größte gemeinsame Teiler monisch ist (denn sonst können wir ihn so skalieren, dass er monisch wird). Dieser größte gemeinsame Teiler ist dann ein monischer Teiler des Polynoms t^k, und hat daher die Form t^j für ein $j \in \{0, 1, \ldots, k\}$ (denn jeder monische Teiler des Polynoms t^k hat diese Form). Betrachten wir dieses j. Also ist t^j der größte gemeinsame Teiler der Polynome χ_A und t^k. Somit ist t^j ein Teiler von χ_A; wir haben also $t^j \mid \chi_A$, und damit $\deg\left(t^j\right) \leq \deg(\chi_A) = n$ (denn das charakteristische Polynom einer $n \times n$-Matrix hat immer Grad n). Mit anderen Worten: $n \geq \deg\left(t^j\right) = j$.

Laut dem Satz von Bezout läßt sich der größte gemeinsame Teiler von zwei Polynomen $f, g \in \mathbb{F}[t]$ stets in der Form $xf + yg$ für gewisse $x, y \in \mathbb{F}[t]$ ausdrücken. Wenden wir dies auf $f = \chi_A$ und $g = t^k$ an, so erhalten wir, dass sich t^j in der Form $x\chi_A + yt^k$ für gewisse $x, y \in \mathbb{F}[t]$ ausdrücken läßt (denn t^j ist der größte gemeinsame Teiler von χ_A und t^k). Betrachte diese x, y. Dann gilt also $t^j = x\chi_A + yt^k$. Setzen wir A für t auf beiden Seiten dieser Gleichung ein, so erhalten wir

$$A^j = \left(x\chi_A + yt^k\right)(A) = x(A)\,\chi_A(A) + y(A)\,A^k.$$

Also ist

$$A^j v = \left(x(A)\,\chi_A(A) + y(A)\,A^k\right) v = x(A)\,\underbrace{\chi_A(A)}_{=0} v + y(A)\,\underbrace{A^k v}_{=0} = 0 + 0 = 0.$$

Aber wir haben $n \geq j$, daher $A^n = A^{n-j} A^j$ und somit $A^n v = A^{n-j}\,\underbrace{A^j v}_{=0} = A^{n-j} 0 = 0$. Dies beweist Lemma 3.1. □

Lemma 3.2. Sei p eine Primzahl. Angenommen, $p \nmid g_m$ gilt für mindestens eine ganze Zahl $m \geq n$. Dann gilt $p \nmid g_k$ für jede ganze Zahl $k \geq 0$.

Beweis von Lemma 3.2. Betrachte den endlichen Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit p Elementen. Ist i eine ganze Zahl, dann bezeichne $[i]$ die Projektion von $i \in \mathbb{Z}$ auf diesen endlichen Körper $\mathbb{F}_p$ (das heißt, die Kongruenzklasse von i modulo p). Ist B eine Matrix mit ganzzahligen Einträgen, dann bezeichne $[B]$ die Matrix, die entsteht, wenn wir jeden Eintrag von B auf $\mathbb{F}_p$ projizieren (das heißt: wenn $B =$

$\left(b_{i,j}\right)_{1\leq i\leq k,\ 1\leq j\leq \ell} \in \mathbb{Z}^{k\times \ell}$, dann sei $[B] = \left(\left[b_{i,j}\right]\right)_{1\leq i\leq k,\ 1\leq j\leq \ell} \in \mathbb{F}_p^{k\times \ell}$). Wir betrachten Spaltenvektoren der Höhe n als $n \times 1$-Matrizen; daher ist v eine $n \times 1$-Matrix.

Die Projektion von $\mathbb{Z}$ nach $\mathbb{F}_p$ ist ein Ringhomomorphismus. Für jede ganze Zahl $m \geq 0$ gilt also

$$[A^m v] = [A]^m [v]. \tag{1}$$

Sei nun $k \geq 0$ eine ganze Zahl. Wir werden zeigen, dass $p \nmid g_k$ gilt.

In der Tat nehmen wir das Gegenteil an. Dann ist also $p \mid g_k$. Doch g_k war definiert als der größte gemeinsame Teiler der n Einträge des Vektors $A^k v$. Aus $p \mid g_k$ folgt somit, dass alle n Einträge des Vektors $A^k v$ durch p teilbar sind. Die Projektionen dieser n Einträge auf $\mathbb{F}_p$ sind also alle 0. Mit anderen Worten: Wir haben $\left[A^k v\right] = 0$ (denn die Einträge des Vektors $\left[A^k v\right]$ sind die Projektionen der Einträge des Vektors $A^k v$ auf $\mathbb{F}_p$). Doch laut (1) gilt $\left[A^k v\right] = [A]^k [v]$. Somit ist $[A]^k [v] = \left[A^k v\right] = 0$. Lemma 3.1 (angewandt auf $\mathbb{F}_p$, $[A]$ und $[v]$ statt $\mathbb{F}$, A und v) ergibt also $[A]^n [v] = 0$.

Wir haben angenommen, dass $p \nmid g_m$ für mindestens eine ganze Zahl $m \geq n$ gilt. Betrachte diese Zahl m. Wegen $m \geq n$ ist $[A]^m = [A]^{m-n} [A]^n$, und folglich $[A]^m [v] = [A]^{m-n} \underbrace{[A]^n [v]}_{=0} = [A]^{m-n} 0 = 0$.

Nun folgt aus (1) aber $[A^m v] = [A]^m [v] = 0$. Mit anderen Worten: Alle n Einträge des Vektors $[A^m v]$ sind 0. Mit anderen Worten: Alle n Einträge des Vektors $A^m v$ sind durch p teilbar (denn die Einträge des Vektors $[A^m v]$ sind die Projektionen der Einträge des Vektors $A^m v$ auf $\mathbb{F}_p$). Folglich muss der größte gemeinsame Teiler dieser n Einträge auch durch p teilbar. Da wir diesen größten gemeinsamen Teiler mit g_m bezeichnet haben, folgern wir also, dass g_m durch p teilbar ist. Das heißt, $p \mid g_m$. Dies widerspricht $p \nmid g_m$. Dieser Widerspruch zeigt, dass unsere Annahme falsch war. Somit ist $p \nmid g_k$ bewiesen. Damit ist Lemma 3.2 gezeigt. □

Nun läßt sich die Aufgabe einfach lösen: Nehmen wir an, dass $g_m = 1$ für mindestens eine ganze Zahl $m \geq n$ gilt. Sei $k \geq 0$ eine ganze Zahl. Wir werden zeigen, dass $g_k = 1$ gilt.

In der Tat nehmen wir das Gegenteil an. Also gilt $g_k \neq 1$. Da g_k eine nichtnegative ganze Zahl ist (denn g_k war definiert als größter gemeinsamer Teiler von n ganzen Zahlen), ist mithin $g_k \in \{0\} \cup \{2, 3, 4, 5, \ldots\}$. Also existiert eine Primzahl p mit $p \mid g_k$. Betrachte diese Primzahl p. Wir haben angenommen, dass $g_m = 1$ für mindestens eine ganze Zahl $m \geq n$ gilt. Daher gilt $p \nmid g_m$ für mindestens eine ganze Zahl $m \geq n$ (denn aus $g_m = 1$ folgt offensichtlich $p \nmid g_m$). Lemma 3.2 zeigt daher, dass $p \nmid g_k$ ist. Dies widerspricht aber $p \mid g_k$. Dieser Widerspruch zeigt, dass unsere Annahme falsch war. Also ist $g_k = 1$ bewiesen.

Vergessen wir, dass wir k fixiert haben. Wir haben also gezeigt, dass $g_k = 1$ für jede ganze Zahl $k \geq 0$ gilt. Mit anderen Worten: Wir haben gezeigt, dass $g_m = 1$ für jede ganze Zahl $m \geq 0$ gilt. Die Aufgabe ist damit gelöst.