Elemente der Mathematik, Problem 1414: gcds of recursively defined sequences

Darij Grinberg*

December 9, 2020

1. Problem

Let n be a positive integer. Let A be an $n \times n$-matrix with integer entries. Let v be a column vector of size n with integer entries.

For each integer $m \geq 0$, define g_m to be the greatest common divisor of the n entries of the vector $A^m v$.

Prove the following: If $g_m = 1$ holds for at least one integer $m \geq n$, then $g_m = 1$ holds for every integer $m \geq 0$.

2. Remarks

Long ago, I posed a weaker version of a particular case ($n = 2$ and $A = \begin{pmatrix} p & q \\ q & p \end{pmatrix}$) as a contest problem (5th QEDMO 2007, problem 1).

It appears natural to try strengthening the problem further, conjecturing perhaps that $g_{kn} \mid g_n^k$ for any integer $k \geq 1$. However, this is easily seen to be false in general.

3. Solution

We shall use two lemmas:[1]

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

[1]We shall liberally use the notation 0 for zero matrices and zero vectors.

Lemma 3.1. Let $\mathbb{F}$ be a field. Let A be an $n \times n$-matrix over $\mathbb{F}$. Let v be a column vector of size n with entries in $\mathbb{F}$.

Let $k \geq 0$ be an integer. Assume that $A^k v = 0$. Then, $A^n v = 0$.

Proof of Lemma 3.1. This is a standard exercise in linear algebra; here is one of the shortest proofs:

Let $\chi_A = \det(tI_n - A) \in \mathbb{F}[t]$ be the characteristic polynomial of the matrix A (where I_n denotes the $n \times n$ identity matrix). The Cayley–Hamilton theorem yields $\chi_A(A) = 0$.

Recall that the polynomial ring $\mathbb{F}[t]$ is a principal ideal domain. Thus, the polynomials χ_A and t^k in $\mathbb{F}[t]$ have a greatest common divisor. Without loss of generality, we can assume that this greatest common divisor is monic (otherwise, we can scale it so it becomes monic). This greatest common divisor is then a monic divisor of t^k, and thus has the form t^j for some $j \in \{0, 1, \ldots, k\}$ (since any monic divisor of t^k has this form). Consider this j. Thus, t^j is the greatest common divisor of the polynomials χ_A and t^k. Hence, t^j is a divisor of χ_A; therefore, $t^j \mid \chi_A$, so that $\deg\left(t^j\right) \leq \deg(\chi_A) = n$ (since the characteristic polynomial of an $n \times n$-matrix always has degree n). In other words, $n \geq \deg\left(t^j\right) = j$.

Bezout's theorem shows that the greatest common divisor of any two polynomials $f, g \in \mathbb{F}[t]$ can be written in the form $xf + yg$ for some $x, y \in \mathbb{F}[t]$. Applying this to $f = \chi_A$ and $g = t^k$, we thus conclude that t^j can be written in the form $x\chi_A + yt^k$ for some $x, y \in \mathbb{F}[t]$ (since t^j is the greatest common divisor of χ_A and t^k). Consider these x, y. Thus, $t^j = x\chi_A + yt^k$. Substituting A for t on both sides of this equality, we obtain

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

Thus,

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

However, $n \geq j$, so that $A^n = A^{n-j}A^j$ and thus $A^n v = A^{n-j}\,\underbrace{A^j v}_{=0} = A^{n-j}0 = 0$. This proves Lemma 3.1. □

Lemma 3.2. Let p be a prime number. Assume that $p \nmid g_m$ holds for at least one integer $m \geq n$. Then, $p \nmid g_k$ holds for every integer $k \geq 0$.

Proof of Lemma 3.2. Consider the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p elements. If i is an integer, then $[i]$ shall denote the projection of $i \in \mathbb{Z}$ onto this finite field $\mathbb{F}_p$ (that is, the congruence class of i modulo p). Likewise, if B is any matrix with integer entries, then $[B]$ shall denote the matrix obtained by projecting each entry of B onto $\mathbb{F}_p$ (that is: if $B = \left(b_{i,j}\right)_{1 \leq i \leq k,\, 1 \leq j \leq \ell} \in \mathbb{Z}^{k \times \ell}$, then $[B] = \left(\left[b_{i,j}\right]\right)_{1 \leq i \leq k,\, 1 \leq j \leq \ell} \in \mathbb{F}_p^{k \times \ell}$). We treat column vectors of size n as $n \times 1$-matrices; thus, v is an $n \times 1$-matrix.

The projection from $\mathbb{Z}$ onto $\mathbb{F}_p$ is a ring homomorphism. Thus, for each integer $m \geq 0$, we have

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

Now, let $k \geq 0$ be an integer. We shall show that $p \nmid g_k$.

Indeed, assume the contrary. Thus, $p \mid g_k$. Recall that g_k was defined as the greatest common divisor of the n entries of the vector $A^k v$. Hence, $p \mid g_k$ entails that all n entries of the vector $A^k v$ are divisible by p. Thus, the projections of these n entries onto $\mathbb{F}_p$ are all 0. In other words, we have $\left[A^k v\right] = 0$ (since the entries of the vector $\left[A^k v\right]$ are the projections of the entries of $A^k v$ onto $\mathbb{F}_p$). But (1) shows that $\left[A^k v\right] = [A]^k [v]$. Hence, $[A]^k [v] = \left[A^k v\right] = 0$. Thus, Lemma 3.1 (applied to $\mathbb{F}_p$, $[A]$ and $[v]$ instead of $\mathbb{F}$, A and v) yields $[A]^n [v] = 0$.

We have assumed that $p \nmid g_m$ holds for at least one integer $m \geq n$. Consider this m. From $m \geq n$, we obtain $[A]^m = [A]^{m-n} [A]^n$, thus $[A]^m [v] = [A]^{m-n} \underbrace{[A]^n [v]}_{=0} = [A]^{m-n} 0 = 0$.

Now, (1) shows that $[A^m v] = [A]^m [v] = 0$. In other words, all n entries of the vector $[A^m v]$ are 0. In other words, all n entries of the vector $A^m v$ are divisible by p (since the entries of the vector $[A^m v]$ are the projections of the entries of the vector $A^m v$ onto $\mathbb{F}_p$). Hence, the greatest common divisor of these n entries must also be divisible by p. Since we have denoted this greatest common divisor by g_m, we thus conclude that g_m is divisible by p. In other words, $p \mid g_m$. This contradicts $p \nmid g_m$. This contradiction shows that our assumption was false. Hence, $p \nmid g_k$ is proved. Thus, we have proved Lemma 3.2. □

Now, it is easy to solve the exercise: Assume that $g_m = 1$ holds for at least one integer $m \geq n$. Let $k \geq 0$ be an integer. We shall show that $g_k = 1$.

Indeed, assume the contrary. Thus, $g_k \neq 1$. Since g_k is a nonnegative integer (being defined as a greatest common divisor of n integers), we thus conclude that $g_k \in \{0\} \cup \{2, 3, 4, 5, \ldots\}$. Hence, there exists a prime p such that $p \mid g_k$. Consider this p. We have assumed that $g_m = 1$ holds for at least one integer $m \geq n$. Thus, $p \nmid g_m$ holds for at least one integer $m \geq n$ (since $g_m = 1$ clearly implies $p \nmid g_m$). Lemma 3.2 thus shows that $p \nmid g_k$. This contradicts $p \mid g_k$. This contradiction shows that our assumption was wrong. Hence, $g_k = 1$ is proved.

Forget that we fixed k. We thus have shown that $g_k = 1$ holds for every integer $k \geq 0$. In other words, $g_m = 1$ holds for every integer $m \geq 0$. This solves the exercise.