ON THE GREATEST COMMON DIVISOR OF THE VALUE OF TWO POLYNOMIALS

PÉTER E. FRENKEL AND JÓZSEF PELIKÁN

Abstract. We show that if two monic polynomials with integer coefficients have square-free resultant, then all positive divisors of the resultant arise as the greatest common divisor of the values of the two polynomials at a suitable integer.

Throughout this paper, $f, g \in \mathbb{Z}[x]$ are monic polynomials with integer coefficients:

$$f(x) = a_0 x^k + a_1 x^{k-1} + \cdots + a_k \tag{1}$$

and

$$g(x) = b_0 x^l + b_1 x^{l-1} + \cdots + b_l, \tag{2}$$

where $a_0 = b_0 = 1$. Our interest is in the range of the greatest common divisor $\gcd(f(n), g(n))$ as n varies in the ring $\mathbb{Z}$ of integers. Such gcd's can behave in intriguing ways.

Example 1. (a) A problem in a Hungarian mathematics competition in 2015 asked for the range of $\gcd\left(n^2+3, (n+1)^2+3\right)$. The answer is $\{1, 13\}$. The gcd is 1 for $n = 1, \ldots, 5$ but is 13 for $n = 6$.

(b) The Prime Glossary page [4] explaining the "law of small numbers" of R. K. Guy [2] points out that the $\gcd\left(n^{17}+9, (n+1)^{17}+9\right)$ is 1 for $n = 1, \ldots, N-1$, but is greater than 1 for $n = N$, where

$$N = 8424432925592889329288197322308900672459420460792433.$$

This number N has 52 digits, and the gcd for $n = N$ is the 52-digit prime

$$p = 8936582237915716659950962253358945635793453256935559.$$

Turning to the general case, let $r = R(f, g) \in \mathbb{Z}$ be the *resultant* of the two polynomials. Recall that, by definition, r is the determinant

Research of the first author is partially supported by ERC Consolidator Grant 648017, by MTA Rényi Lendület Groups and Graphs research group, and by the Hungarian National Research, Development and Innovation Office – NKFIH, OTKA grants no. K109684 and K104206.

of the *Sylvester matrix*

$$M = \begin{pmatrix} a_0 & a_1 & \dots & a_k & & & \\ & a_0 & a_1 & \dots & a_k & & \\ & & \dots & \dots & \dots & \dots & \\ & & & a_0 & a_1 & \dots & a_k \\ b_0 & b_1 & \dots & b_l & & & \\ & b_0 & b_1 & \dots & b_l & & \\ & & \dots & \dots & \dots & \dots & \\ & & & b_0 & b_1 & \dots & b_l \end{pmatrix} \tag{3}$$

of the two polynomials. Note that M is an $(l+k)$-square matrix; the first l rows are built from the coefficients of f, and the last k rows are built from the coefficients of g, padded with zeros.

The most widely applied fact about the resultant is that it is zero if and only if the two polynomials have a common complex root, or, equivalently, a non-constant common divisor in $\mathbb{C}[x]$. This holds true even if the coefficients are arbitrary complex numbers. In our case, however, the coefficients are integers. In this setting, the resultant is zero if and only if the two polynomials have a non-constant common divisor in $\mathbb{Z}[x]$.

We start with two easy observations relating the resultant r to the gcd of the polynomial values.

Proposition 2. *(a) For any integer n, $\gcd(f(n), g(n))$ divides r.*

(b) As a function of n, the value $\gcd(f(n), g(n))$ is periodic with period r.

Note that r can be zero. By definition, any function is periodic with period 0.

Proof. (a) Let $d = \gcd(f(n), g(n))$. Each coordinate of the column vector

$$M \cdot (n^{k+l-1}, n^{k+l-2}, \dots, n, 1)^\top$$

is divisible by either $f(n)$ or $g(n)$, and therefore by d. Thus, the last column of M is congruent modulo d to a linear combination, with integral coefficients, of the previous columns. It follows that $r = \det M \equiv 0 \mod d$, as claimed.

(b) We have $f(n+r) \equiv f(n)$ and $g(n+r) \equiv g(n) \mod r$. It follows that

$$\gcd(f(n+r), g(n+r), r) = \gcd(f(n), g(n), r).$$

In view of statement (a), the third argument can be omitted from the gcd on both sides, proving statement (b). □

Recall that $r = 0$ if and only if f and g have a non-constant common divisor h in the ring $\mathbb{Z}[x]$. In this case, $\gcd(f(n), g(n))$ is divisible by $h(n)$ for all n and therefore has an infinite range and no nonzero period.

Do all nonnegative divisors of r arise as $\gcd(f(n), g(n))$ with suitable integral n? In particular, does $|r|$ itself arise as such a gcd? Not necessarily.

Example 3. Let $f(x) = g(x) = x^2 + x + 1$. Then $r = 0$, so all integers divide r, but not all nonnegative integers arise as $\gcd(f(n), g(n)) = n^2 + n + 1$. In fact, no even numbers arise. In particular, 0 itself does not arise.

What if we assume $r \neq 0$? The answer is still no.

Example 4. Let $f(x) = x^2 - 1$ and $g(x) = x^2 + 1$. Then $r = 4$, but the range of $\gcd(f(n), g(n))$ is $\{1, 2\}$.

This example also shows that when $r \neq 0$, $|r|$ need not be the smallest positive period of $\gcd(f(n), g(n))$. In Example 4, we have $r = 4$, but the smallest positive period is 2.

Our main result, Theorem 6 below, says that when r is square-free, Proposition 2(a) is the only restriction on the values attained by the gcd, and the smallest positive period of the gcd is $|r|$.

For this, we shall need a basic fact about integer matrices: they can be brought to *Smith normal form.* For any matrix M with integral entries, there exist matrices U and V, also with integral entries and invertible over $\mathbb{Z}$, such that UMV is a diagonal matrix with diagonal entries $d_1, d_2, \ldots$, where the so-called *invariant factors* d_i satisfy $d_i | d_{i+1}$ for all i. See Smith's original paper [5], or see, e.g., [1, Section 5.3] for a textbook presentation. Note that U and V, being invertible over $\mathbb{Z}$, are necessarily square matrices with determinant ± 1. If M is also square, it follows that

$$\prod d_i = \det(UMV) = \pm \det M. \tag{4}$$

In the proof of our main result, we shall have to leave the realm of polynomials with integer coefficients and consider polynomials over the field $\mathbb{F}_p$ of prime cardinality p. Given two polynomials f and g over any field F, of degree k and l respectively, with coefficients as in (1) and (2), their Sylvester matrix M is defined by the formula (3). We shall need

Theorem 5. [3, Theorem 1.19] *The* corank *(or* kernel dimension*)* $k + l - \operatorname{rank} M$ *of* M *over* F *equals the degree of the gcd of the two polynomials* f *and* g *as elements of the polynomial ring* $F[x]$.

For two proofs of this well-known fact, the reader may consult [3]. As this is an Internet reference, and we were unable to find a textbook or journal reference, we include a third proof.

Proof. Let us identify the vector space F^{k+l} with the vector space of polynomials of degree less than $k + l$. Let any such polynomial correspond to the list of its coefficients, starting with the coefficient of x^{k+l-1} and ending with the constant term.

Under this correspondence, the row space of the Sylvester matrix M is identified with the set of polynomials of the form $\phi f + \psi g$, where $\phi, \psi \in F[x]$ have degree less than l and k, respectively. Any polynomial of this form is divisible by $\gcd(f, g)$. Conversely, any polynomial that is divisible by $\gcd(f, g)$ and has degree less than $k+l$ is in the row space. To see this, we first write such a polynomial as $\phi_0 f + \psi_0 g$, where we know nothing about the degree of $\phi_0, \psi_0 \in F[x]$, but then we write $\phi_0 = qg + \phi$ with ϕ of degree less than l, and we define $\psi = qf + \psi_0$. Then $\phi_0 f + \psi_0 g = \phi f + \psi g$; moreover, this polynomial and ϕf both have degree less than $k + l$, whence so does ψg, showing that ψ has degree less than k.

The rank of M is the dimension of the row space. The theorem follows. □

We are now ready for the main result of this paper.

Theorem 6. *Let f and g be monic polynomials with integer coefficients. Assume that their resultant r is square-free. Then all positive divisors of r arise as $\gcd(f(n), g(n))$ with suitable integral n. Moreover, any $d|r$ arises exactly $\prod(p-1)$ times in each period of length $|r|$, where the product is taken over all (positive) prime divisors p of r/d. In particular, $|r|$ itself arises once.*

Proof. Let $\mathcal{P}$ be the set of all prime divisors of r, so that

$$r = \pm \prod_{p \in \mathcal{P}} p.$$

We shall prove that for all subsets $\mathcal{S}$ of $\mathcal{P}$, the product $d = \prod_{p\in\mathcal{S}} p$ arises as $\gcd(f(n), g(n))$ for a suitable integer n; moreover, in each period of length $|r|$, it arises exactly $\prod_{p\in\mathcal{P}-\mathcal{S}}(p-1)$ times.

For each $p \in \mathcal{P}$, the $\gcd(f(n), g(n), p)$ is periodic with period p. It suffices to prove that in each period of length p, this gcd is p exactly once. Indeed, the Chinese remainder theorem will then finish the proof: in each period of length $|r|$, the integers n such that $\gcd(f(n), g(n)) = d$ can be found by specifying their value mod p for each $p \in \mathcal{P}$. For each $p \in \mathcal{S}$, there is a unique possibility for n mod p, and for each $p \in \mathcal{P} - \mathcal{S}$, there are $p - 1$ possibilities.

It suffices to prove that for any prime $p \in \mathcal{P}$, the polynomials f and g, when viewed mod p, have a unique common root in $\mathbb{F}_p$; equivalently, the gcd of f and g as elements of $\mathbb{F}_p[x]$ has a unique root in $\mathbb{F}_p$. In fact, we shall prove that this gcd is a polynomial of degree exactly 1.

It suffices to prove that the mod p corank of the Sylvester matrix M of f and g is 1. But the determinant of M over $\mathbb{Z}$ is r, which is divisible by p but not by p^2. Now M can be brought to Smith normal form, and from (4), we see that the last invariant factor d_{k+l} is divisible by p, but the previous one is not. The mod p corank of the diagonal matrix UMV, and therefore also of M, is 1, as claimed. □

Remark 7. When $|r|$ is prime, the gcd is $|r|$ for n in a unique residue class mod r and is 1 for all other n. This sheds some light on the seemingly peculiar behavior in Example 1, since $r = 13$ for (a) and $r = p$ for (b).

When r is not square-free, we know very little about the range of the gcd. At least, we can give a sufficient condition for 1 to appear in the range. This condition, however, is not necessary; see Example 4.

Proposition 8. *Let f and g be monic polynomials with integer coefficients and resultant r.*

(a) Suppose that p is prime and r is not divisible by p^p. Then there exists an integer n such that $\gcd(f(n), g(n))$ *is not divisible by p.*

(b) If r has no divisor of the form p^p with p prime, then there exists an integer n such that $f(n)$ and $g(n)$ are coprime.

Proof. (a) Again we exploit the fact that $r = \pm d_1 \cdots d_{k+l}$, where the d_i are the invariant factors of the Sylvester matrix M. Since $d_i | d_{i+1}$ for all i, and $p^p \not| r$, it follows that at most the last $p - 1$ invariant factors d_i can be divisible by p. In other words, the mod p corank of M is less than p, so the degree of the gcd of f and g as elements of $\mathbb{F}_p[x]$ is less than p, and therefore this gcd cannot vanish as a function $\mathbb{F}_p \to \mathbb{F}_p$. But this gcd can be written as $\phi f + \psi g$ with $\phi, \psi \in \mathbb{F}_p[x]$, so it follows that f and g cannot both vanish as functions $\mathbb{F}_p \to \mathbb{F}_p$.

(b) For all prime divisors p of r, we can use statement (a) to get an integer n_p such that $\gcd(f(n_p), g(n_p))$ is not divisible by p. The Chinese remainder theorem gives us an integer n such that $n \equiv n_p \mod p$ for all p. This n will have the desired property. □

Remark 9. Throughout this paper, we have studied two monic polynomials over the ring $\mathbb{Z}$ of integers. However, $\mathbb{Z}$ can be replaced by an arbitrary principal ideal domain A. Our results and their proofs remain valid, with trivial modifications.

For example, Proposition 2(b) should be interpreted as saying that $(f(n), g(n)) = (f(n'), g(n'))$ whenever $n, n' \in A$ and $r | n - n'$ in A. Note that this is an equality of ideals of A.

In this general setting, the conclusion of Theorem 6 is replaced by the following. There exist constants $c_P \in A$, one for each prime ideal P containing r, such that for any divisor d of r, and any $n \in A$, we have $(f(n), g(n)) = (d)$ if and only if $n - c_P \in P$ for each P containing d but $n - c_P \notin P$ for each P that does not contain d. Such elements n exist for any divisor d of r. When $d = r$, they form a coset $c + (r)$.

The p^p in Proposition 8 should be interpreted as $p^{|A/(p)|}$. This can be p^∞, which, by definition, divides only 0.

Acknowledgements

We are grateful to the Editorial Board of the Monthly and to the two unnamed referees of this paper for many useful comments.

References

[1] W. A. Adkins, S. H. Weintraub, *Algebra: an approach via module theory,* Springer, 1992.

[2] R. K. Guy, The Strong Law of Small Numbers, *Amer. Math. Monthly* **95** no. 8 (Oct 1988), 697–712.

[3] S. Janson, Resultant and discriminant of polynomials, `http://www2.math.uu.se/~svante/papers/sjN5.pdf`

[4] The Prime Glossary, `http://primes.utm.edu/glossary/page.php?sort=LawOfSmall`

[5] H. J. S. Smith, On systems of linear indeterminate equations and congruences, *Phil. Trans. R. Soc. Lond.* **151** (1), 293–326. Reprinted in *The Collected Mathematical Papers of Henry John Stephen Smith I,* Ed. J.W.L. Glaisher. Oxford, Clarendon Press (1894), 367–409.

Eötvös University, Department of Algebra and Number Theory, Pázmány Péter sétány 1/c, H-1117 Budapest, Hungary, and Rényi Institute of Mathematics, Hungarian Academy of Sciences, 13-15 Reáltanoda utca, H-1053 Budapest, Hungary

E-mail address: `frenkelp265@gmail.com`

Eötvös University, Department of Algebra and Number Theory, Pázmány Péter sétány 1/c, H-1117 Budapest, Hungary

E-mail address: `pelikan@cs.elte.hu`