ESTIMATING THE GREATEST COMMON DIVISOR OF THE VALUE OF TWO POLYNOMIALS

PÉTER E. FRENKEL AND GERGELY ZÁBRÁDI

Abstract. Let p be a fixed prime, and let $v(a)$ stand for the exponent of p in the prime factorization of the integer a. Let f and g be two monic polynomials with integer coefficients and nonzero resultant r. Write S for the maximum of $v(\gcd(f(n), g(n)))$ over all integers n. It is known that $S \leq v(r)$. We give various lower and upper bounds for the least possible value of $v(r) - S$ provided that a given power p^s divides both $f(n)$ and $g(n)$ for all n. In particular, the least possible value is $ps^2 - s$ for $s \leq p$ and is asymptotically $(p-1)s^2$ for large s.

Let $f, g \in \mathbb{Z}[x]$ be monic polynomials with nonzero resultant r. Our interest is in the range of the greatest common divisor of $f(n)$ and $g(n)$ as n varies in $\mathbb{Z}$. In the recent paper [1] by J. Pelikán and the first author, it was shown[1] that

(1) $\gcd(f(n), g(n))$ divides r for all n; moreover,
(2) for square-free r, its range is the set of all (positive) divisors of r;
(3) If r is allowed to have square divisors, then $|r|$ need not be in the range. For example, $f(x) = x^2 + 1$ and $g(x) = x^2 - 1$ have resultant 4 but never have gcd 4.
(4) If r has no divisors of the form p^p with p prime, then 1 appears in the range.

For statement (3), there is an even worse example with resultant 4: $f(x) = x^2 + x + 1$ and $g(x) = x^2 + x - 1$ have $f(n)$ and $g(n)$ coprime for all n. For statement (4) with the condition on r removed, there again is a counterexample with resultant 4: $f(x) = x^2 + x + 2$ and $g(x) = x^2 + x$ have $\gcd(f(n), g(n)) = 2$ for all n. On the other hand, it will turn out that if r is in the range, then so are all its divisors; see Theorem 6 below.

Date: 5th December 2017.
This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 648017), from the MTA Rényi Lendület Groups and Graphs research group, from the Hungarian National Research, Development and Innovation Office – NKFIH, OTKA grants no. K104206 and K109684, and from the János Bolyai Scholarship of the Hungarian Academy of Sciences.

[1]Statement (4) was essentially known before, cf. [2, 6]

In the present paper, we undertake a refined study of the case when r can have prime power divisors with high exponents. Fix a prime p, and let $v(a)$ stand for the exponent of p in the prime factorization of the integer a. It suffices to study the range of $v(\gcd(f(n), g(n)))$, since if we understand this for all p, then the Chinese remainder theorem allows us to read off the range of $\gcd(f(n), g(n))$.

Write S for the maximum of $v(\gcd(f(n), g(n)))$ as n varies in $\mathbb{Z}$. By [1, Proposition 2(a)], we have $S \le v(r)$. Our main goal is to estimate the least possible value of $v(r)-S$ provided that $v(\gcd(f(n), g(n))) \ge s$ for all n. We develop two different methods. Up to Theorem 3, we use the definition of the resultant in terms of the coefficients of f and g, while from Construction 4 on, we use the equivalent definition in terms of the roots of f and g.

Let

$$f(x) = a_0x^k + a_1x^{k-1} + \cdots + a_k \tag{1}$$

and

$$g(x) = b_0x^l + b_1x^{l-1} + \cdots + b_l, \tag{2}$$

where $a_0 = b_0 = 1$. Recall that, by definition, r is the determinant of the *Sylvester matrix*

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

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.

We shall need the following interpretation of the resultant.

Lemma 1. *If f and g are monic polynomials with integer coefficients and nonzero resultant r, then $|r| = |\mathbb{Z}[x]/(f, g)|$, where (f, g) stands for the ideal generated by f and g.*

Note that for $r = 0$ (which is excluded throughout this paper), we would have $|\mathbb{Z}/(f, g)| = \infty$ because f and g would have a nonconstant common divisor in $\mathbb{Z}[x]$.

Note also that Lemma 1 implies [1, Proposition 2(a)]: the greatest common divisor $(f(n), g(n))$ divides the resultant r. Indeed, there is a surjective ring homomorphism from $\mathbb{Z}[x]/(f, g)$ onto $\mathbb{Z}/(f(n), g(n))$.

The statement and proof of Lemma 1 are reminiscent of [3, Theorem 1.19], which was reproved as [1, Theorem 5]. In that theorem, the coefficients come from a field F, and the claim is that the corank of the Sylvester matrix M is the dimension over F of the quotient ring $F[x]/(f,g)$, i.e., the degree of the polynomial $\gcd(f,g)$.

Proof. Let us identify the free Abelian group $\mathbb{Z}^{k+l}$ with the additive group $\mathbb{Z}[x]_{<k+l}$ of polynomials of degree less than $k+l$ with integer coefficients. 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 subgroup generated by the rows of the Sylvester matrix M is identified with the set of polynomials of the form $\phi f + \psi g$, where $\phi, \psi \in \mathbb{Z}[x]$ have degree less than l and k, respectively. Any polynomial of this form is in (f,g). Conversely, any element of (f,g) of degree less than $k+l$ is an integral linear combination of the rows. To see this, we first write such a polynomial as $\phi_0 f + \psi_0 g$, where we know nothing about the degree of $\phi_0, \psi_0 \in \mathbb{Z}[x]$, 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.

Thus, the subgroup of $\mathbb{Z}^{k+l}$ generated by the rows of M is identified with the degree $< k+l$ part $(f,g)_{<k+l}$ of the ideal (f,g) of $\mathbb{Z}[x]$. The determinant r of M is the signed volume of the parallelotope spanned by the rows, therefore $|r|$ is the volume of this parallelotope, which is the cardinality of the quotient

$$\mathbb{Z}^{k+l}/\langle \text{rows of } M \rangle \simeq \mathbb{Z}[x]_{<k+l}/(f,g)_{<k+l} \simeq$$
$$\simeq ((f,g) + \mathbb{Z}[x]_{<k+l})/(f,g) = \mathbb{Z}[x]/(f,g).$$

□

For integers $S \geq s \geq 0$, let

$$I_{S,s} = \left\{ f \in \mathbb{Z}[x] : p^s | f(n) \text{ for all } n, \text{ and } p^S | f(0) \right\}.$$

This is an ideal of $\mathbb{Z}[x]$. Put $R_{S,s} = \mathbb{Z}[x]/I_{S,s}$. The cardinality of this quotient ring will play a central role in our computations. The cardinality can be expressed in terms of the functions

$$\alpha(j) = v(j!) = \left\lfloor \frac{j}{p} \right\rfloor + \left\lfloor \frac{j}{p^2} \right\rfloor + \left\lfloor \frac{j}{p^3} \right\rfloor + \dots$$

and $\beta(m) = \min\{j : \alpha(j) \geq m\}$. Put $B(s) = \sum_{m=1}^{s} \beta(m)$.

Note that α is superadditive:

$$\alpha(j_1 + j_2) \geq \alpha(j_1) + \alpha(j_2)$$

for all nonnegative integers j_1 and j_2. It follows that β is subadditive:

$$\beta(m_1 + m_2) \leq \beta(m_1) + \beta(m_2)$$

for all nonnegative integers m_1 and m_2.

Note also that $\alpha(j) = \lfloor j/p \rfloor$ for $0 \leq j < p^2$, and $\alpha(p^2) = p+1$, whence $\beta(m) = pm$ for $1 \leq m \leq p$ and $B(s) = p\binom{s+1}{2}$ for $1 \leq s \leq p$. On the other hand, $\alpha(j) \sim j/(p-1)$ for large j, whence $\beta(m) \sim (p-1)m$ for large m and $B(s) \sim (p-1)s^2/2$ for large s.

Lemma 2. *We have*

$$|R_{S,s}| = p^{S-s+B(s)}.$$

Proof. For $S = s$, the ring $R_{S,s} = R_{s,s}$ is the ring of polynomial functions $\mathbb{Z}/(p^s) \to \mathbb{Z}/(p^s)$. By a classical result of Kempner [5], reproved by Keller and Olson [4, Corollary 2.2], this ring has cardinality $p^{B(s)}$.

For $S \geq s$, observe that $I_{S,s}$ is the kernel of the map $I_{s,s} \to \mathbb{Z}/(p^S)$, $f \mapsto f(0)$. The image of this map is $(p^s)/(p^S)$, whence $|I_{s,s}/I_{S,s}| = p^{S-s}$. But $I_{s,s}/I_{S,s}$ is the kernel of the surjective map $R_{S,s} \to R_{s,s}$, therefore $|R_{S,s}|/|R_{s,s}| = p^{S-s}$ and the Lemma follows. □

The first main result of this paper is the following refinement of [1, Proposition 8(a)].

Theorem 3. *Let f and g be monic polynomials with integer coefficients and nonzero resultant r. Assume that a fixed prime power p^s divides both $f(n)$ and $g(n)$ for all n. Let*

$$S = \max_{n \in \mathbb{Z}} v(\gcd(f(n), g(n))).$$

Then $v(r) - S \geq B(s+t) - 2B(t) - s$ for all nonnegative integers t.

Proof. The resultant being translation invariant, we may and do assume that p^S divides $\gcd(f(0), g(0))$. Using Lemma 1, we have

$$\begin{aligned} v(r) =& v\left(|\mathbb{Z}[x]/(f,g)|\right) \geq \\ &\geq v\left(|\mathbb{Z}[x]/((f,g) + I_{S+t,s+t})|\right) = v\left(\left|R_{S+t,s+t}/\left(\bar{f}, \bar{g}\right)\right|\right), \end{aligned}$$

where $\bar{f}$ and $\bar{g}$ are the natural images in $R_{S+t,s+t}$ of f and g, respectively. Now observe that in the $\mathbb{Z}[x]$-module $R_{S+t,s+t}$, both elements $\bar{f}$ and $\bar{g}$ are annihilated by the ideal $I_{t,t}$. Hence $v\left(\left|\left(\bar{f}\right)\right|\right) \leq v(|R_{t,t}|) = B(t)$ by Lemma 2, and similarly for $\bar{g}$. Now

$$v\left(\left|\left(\bar{f}, \bar{g}\right)\right|\right) = v\left(\left|\left(\bar{f}\right)\right|\right) + v(|(\bar{g})|) - v\left(\left|\left(\bar{f}\right) \cap (\bar{g})\right|\right) \leq 2B(t),$$

whence

$$v(r) \geq v(|R_{S+t,s+t}|) - v\left(\left|\left(\bar{f}, \bar{g}\right)\right|\right) \geq (S+t) - (s+t) + B(s+t) - 2B(t)$$

and the Theorem follows. □

For $s = 1$, we may choose $t = 0$ in Theorem 3 to get $v(r) \geq S+p-1 \geq p$, which recovers [1, Proposition 8(a)]. For general $s \geq 0$, choosing $t = s$, we get $v(r) - S \geq B(2s) - 2B(s) - s$. When $s \leq p/2$, we have $B(s) = p\binom{s+1}{2}$ and $B(2s) = p\binom{2s+1}{2}$, whence $v(r) - S \geq ps^2 - s$. It shall follow from Theorem 6 and Construction 8 that this lower bound holds true, and is sharp, even under the weaker assumption that $s \le p$. On the other hand, for large s, we have $B(s) \sim (p-1)s^2/2$ and $B(2s) \sim 2(p-1)s^2$, whence $v(r) - S \gtrsim (p-1)s^2$. We now present a construction showing that this is asymptotically sharp for any fixed p.

Construction 4. *Consider the polynomials*

$$f(x) := \prod_{j=0}^{\beta(s)-1} (x-j) \ ;$$

$$g(x) := p^s + \prod_{i=0}^{p-1} (x-i)^{s+1}$$

for an integer $s \ge 0$. Then $v(\gcd(f(n), g(n))) = s$ for all integers n. For the resultant r, we have $v(r) = s\beta(s)$, whence $v(r) - s = s(\beta(s)-1) \sim (p-1)s^2$ when $s \gg p$.

Proof. Firstly, note that $f(\beta(s)) = \beta(s)!$ divides $f(n)$ for any integer n since the binomial coefficient $\binom{n}{\beta(s)} = f(n)/\beta(s)!$ is an integer. Therefore, we have $s \le \alpha(\beta(s)) = v(\beta(s)!) \le v(f(n))$. On the other hand, we have $v(g(n)) = s$ for all n since p^{s+1} divides $\prod_{i=0}^{p-1}(n-i)^{s+1}$ for any integer n. Hence the statement on $v(\gcd(f(n), g(n)))$. Further, we compute

$$v(r) = v\left(\prod_{j=0}^{\beta(s)-1} g(j) \right) = \sum_{j=0}^{\beta(s)-1} v(g(j)) = s\beta(s) \ .$$

□

Let us return to the notations and conditions of Theorem 3. In the rest of this paper, our main goal is to obtain a sharp lower bound for $v(r) - S$ when $s \le p$. For this, we recall a bit of p-adic number theory. Let K be the splitting field of the product fg over the field $\mathbb{Q}_p$ of p-adic numbers for the fixed prime p. So we may write $f(x) = \prod_{i=1}^{k}(x-\gamma_i)$ and $g(x) = \prod_{j=1}^{l}(x-\delta_j)$ with $\gamma_i, \delta_j \in \mathcal{O}$ ($i = 1, \dots, k$; $j = 1, \dots, l$), where $\mathcal{O}$ denotes the valuation ring in K with uniformizer π and residue field $\mathbb{F} = \mathcal{O}/(\pi)$. We put $e = v_\pi(p)$ for the absolute ramification index of K, where v_π stands for the π-adic valuation. We extend the p-adic valuation v to K by putting $v = v_\pi/e$. In particular, we have $v(\pi) = 1/e$, and the v-value of any element of $\mathcal{O}$ is a nonnegative integer multiple of $1/e$. We have $e \cdot |\mathbb{F} : \mathbb{F}_p| = |K : \mathbb{Q}_p|$, but this will not be used in the sequel.

For integers $n \in \mathbb{Z}$ and $0 \le s \in \mathbb{Z}$, the value $f(n) \in \mathbb{Z}$ is divisible by p^s if and only if $\sum_{i=1}^{k} v(n-\gamma_i) \ge s$. On the other hand, the resultant of f and g equals

$$r = \prod_{i,j}(\gamma_i - \delta_j) \in \mathbb{Z}.$$

For any fixed $n \in \mathbb{Z}$, we have the following trivial estimate for the p-adic valuation of r:

$$v(r) = \sum_{i,j} v(\gamma_i - \delta_j) \geq \sum_{i,j} \min(v(n-\gamma_i), v(n-\delta_j)) \ . \tag{4}$$

Note that the above trivial estimate again implies [1, Proposition 2(a)]: the greatest common divisor $(f(n), g(n))$ divides the resultant r. Indeed, it suffices to check this locally, i.e.,

$$v(\gcd(f(n), g(n))) = \min(v(f(n)), v(g(n))) =$$
$$= \min\left(\sum_i v(n-\gamma_i), \sum_j v(n-\delta_j)\right) \leq v(r)$$

for all primes p. The latter inequality follows easily from (4) by choosing a maximum among the multiset

$$\{v(n-\gamma_i), v(n-\delta_j) \mid 1 \leq i \leq k, 1 \leq j \leq l\}.$$

In order to estimate this further from below, we need the following lemma stating (in the special case of $I = \emptyset$) that whenever $s \leq p$ and $f(n)$ is divisible by p^s for all n, then there are at least s roots of f in $\overline{\mathbb{Q}_p}$ congruent to each integer modulo p.

Lemma 5. *Let $m \in \mathbb{Z}$ be a fixed integer, and let $I \subseteq \{1, \ldots, k\}$ be an arbitrary subset such that for all $i \in I$ we have $v(m-\gamma_i) \notin \mathbb{Z}$. Further, let $0 \leq t_I < p$ be the number of indices $i \in \{1, \ldots, k\} \setminus I$ with $v(m-\gamma_i) > 0$. Then there exists an integer $n \in \mathbb{Z}$ such that $n \equiv m \pmod p$ and $v(f(n)) \leq \sum_{i \in I} v(m-\gamma_i) + t_I$.*

Proof. First of all, note that

$$v(f(n)) = \sum_{i=1}^{k} v(n-\gamma_i) = \sum_{i \in I} v(n-\gamma_i) + \sum_{i \in \{1,\ldots,k\} \setminus I} v(n-\gamma_i).$$

On the one hand, for any integer $n \in \mathbb{Z}$ and $i \in I$, we have $v(n-m) \in \mathbb{Z}$, whence $v(n-m) \neq v(m-\gamma_i)$, as the latter is not an integer by assumption. So we compute

$$v(n-\gamma_i) = v((n-m)+(m-\gamma_i)) = \min(v(n-m), v(m-\gamma_i)) \leq v(m-\gamma_i).$$

On the other hand, we want to pick $n \in \mathbb{Z}$ in such a way that we can estimate

$$\sum_{i \in \{1,\ldots,k\} \setminus I} v(n-\gamma_i)$$

efficiently. We have to have $n \equiv m \pmod p$, and we choose n modulo p^2 so that all indices $i \in \{1, \ldots, k\} \setminus I$ satisfy $v(n-\gamma_i) \leq 1$ (equivalently, $< 1 + 1/e$). Indeed, we can achieve this by the pigeonhole principle: there are p choices for n mod p^2 and these are pairwise incongruent mod π^{e+1}, so any element $\gamma \in \mathcal{O}$ can only be congruent to one of these choices modulo π^{e+1}.

This way we obtain an integer $n \equiv m \pmod p$ such that

$$\begin{aligned} v(f(n)) &= \sum_{i=1}^{k} v(n-\gamma_i) \leq \\ &\leq \sum_{i\in I} v(m-\gamma_i) + \sum_{i\notin I, v(m-\gamma_i)>0} 1 = \sum_{i\in I} v(m-\gamma_i) + t_I \end{aligned}$$

as desired. □

The second main result of this paper is the following refinement of [1, Proposition 8(a)].

Theorem 6. *Let f and g be monic polynomials with integer coefficients and nonzero resultant r. Assume that $s \leq p$ and that the power p^s divides both $f(n)$ and $g(n)$ for all n. Let*

$$S = \max_{n\in\mathbb{Z}} v(\gcd(f(n), g(n))).$$

(a) We have

$$v(r) - S \geq ps^2 - s\ .$$

(b) If equality holds here, then $v(\gcd(f(n), g(n)))$ takes all the integer values in the interval $[s, S]$.

Proof. We may assume without loss of generality that

$$v(\gcd(f(0), g(0))) = S.$$

Fix an integer $m \in \mathbb{Z}$, and set $a_i = v(m-\gamma_i)$ and $b_j = v(m-\delta_j)$ $(i = 1, \ldots, k; j = 1, \ldots, l)$. By assumption, p^s divides $\gcd(f(m), g(m))$, so we have $\sum_{i=1}^{k} a_i \geq s$ and $\sum_{j=1}^{l} b_j \geq s$.

We may assume without loss of generality (possibly swapping f and g and permuting their roots) that the maximum of

$$\{a_i, b_j \mid 1 \leq i \leq k, 1 \leq j \leq l\}$$

is achieved at b_l.

Lemma 7. *(a) We have*

$$\sum_{i,j\colon \gamma_i \equiv m \equiv \delta_j \pmod \pi} v(\gamma_i - \delta_j) \geq \begin{cases} s^2 & (m \in \mathbb{Z}) \\ s^2 - s + S & (m = 0). \end{cases}$$

(b) If equality holds for $m = 0$, then either $S = s$, or all of the following hold:

$$b_l \geq S - s + \operatorname{sgn} s,$$

$$b_j \leq \operatorname{sgn} s \textit{ for all } j < l,$$

and

$$\sum_{j=1}^{l-1} b_j = s - \operatorname{sgn} s.$$

Here $\operatorname{sgn} 0 = 0$ and $\operatorname{sgn} s = 1$ for $s \geq 1$.

Proof. (a) We have $v(\gamma_i - \delta_j) \geq \min(a_i, b_j)$ as before. Note that whenever $m \not\equiv \gamma_i \pmod{\pi}$ or $m \not\equiv \delta_j \pmod{\pi}$, then $\min(a_i, b_j)$ vanishes. Hence we obtain

$$\sum_{i,j\colon \gamma_i \equiv m \equiv \delta_j \pmod{\pi}} v(\gamma_i - \delta_j) \geq \sum_{j=1}^{l} \sum_{i=1}^{k} \min(a_i, b_j) \tag{5}$$

by adding these together. Fix $j \in \{1, \dots, l\}$ for now, and put

$$I_j := \{i \in \{1, \dots, k\} \mid a_i \leq \min(1, b_j) \text{ and } a_i \notin \mathbb{Z}\} \ .$$

Let t_j be the number of indices $i \in \{1, \dots, k\} \setminus I_j$ such that $a_i \neq 0$. Applying Lemma 5 to the subset $I := I_j$, we find

$$s \leq \sum_{i \in I_j} a_i + t_j \ .$$

On the other hand, for any $i \in \{1, \dots, k\} \setminus I_j$ with $a_i \neq 0$, we have $a_i \geq \min(1, b_j)$, so

$$\begin{aligned} &\sum_{i=1}^{k} \min(a_i, b_j) \geq \sum_{i \in I_j} a_i + t_j \min(1, b_j) \geq \\ &\geq \left(\sum_{i \in I_j} a_i + t_j \right) \min(1, b_j) \geq s \min(1, b_j) \ . \end{aligned} \tag{6}$$

Now Lemma 5 applied to the polynomial g and to the subset

$$I := \{j \in \{1, \dots, n\} \mid 0 < b_j < 1\}$$

yields

$$s \leq \sum_{j \in I} b_j + t_I \leq \sum_{j=1}^{l} \min(1, b_j). \tag{7}$$

The first statement in (a) is a combination of (5), (6), and (7).

Let $m = 0$. By the maximality of b_l, we have

$$\sum_{i=1}^{k} \min(a_i, b_l) = \sum_{i=1}^{k} a_i = v(f(0)) \geq S \ .$$

Also,

$$1 + \sum_{j=1}^{l-1} \min(1, b_j) \geq \sum_{j=1}^{l} \min(1, b_j) \geq s \ .$$

This yields

$$\sum_{j=1}^{l}\sum_{i=1}^{k}\min(a_i,b_j)=\sum_{j=1}^{l-1}\sum_{i=1}^{k}\min(a_i,b_j)+\sum_{i=1}^{k}\min(a_i,b_l)\geq$$
$$\geq s\sum_{j=1}^{l-1}\min(1,b_j)+S\geq s(s-1)+S$$

as desired.

(b) Fix $j<l$. To have equality in the last chain of inequalities, we must have equality in (6), whence $\min(a_i,b_j)=\min(1,b_j)$ for all i such that $i\notin I_j$ and $a_i>0$. We must also have $\sum_{i=1}^{k}a_i=S$ and, in case $s\geq 1$, we must have $b_l\geq 1$ and $\sum_{j=1}^{l}\min(1,b_j)=s$.

If $b_j>1$ for some $j<l$, then $a_i=1$ for all i such that $i\notin I_j$ and $a_i>0$, which means that $a_i\leq 1$ for all i. But (6) holds with equality, so we have $\sum_{i=1}^{k}a_i=s$, whence $S=s$.

If $b_j\leq 1$ for all $j<l$, then $\min(1,b_j)=b_j$ for all $j<l$, hence

$$S\leq v(g(0))=\sum_{j=1}^{l}b_j=b_l+\sum_{j=1}^{l-1}\min(1,b_j).$$

If $s\geq 1$, then this is b_l-1+s, and $b_l\geq S-s+1$ follows. If $s=0$, then, since (6) holds with equality, we deduce either $a_1=\cdots=a_k=0$ and therefore $S=0=s$, or $b_1=\cdots=b_{l-1}=0$ and therefore $b_l\geq S$. □

Adding up the estimates of Lemma 7(a) for $m=0,1,\ldots,p-1$, we deduce Theorem 6(a). For (b), observe that the value S is obviously taken. Observe also that if $v(r)-S=ps^2-s$, then the value s is also taken, for otherwise Theorem 6(a) yields

$$v(r)-S\geq p(s+1)^2-(s+1),$$

a contradiction. Moreover, equality holds in Lemma 7(a) for all m, in particular, for $m=0$. Thus, Lemma 7(b) applies. If $S=s$, then Theorem 6(b) obviously holds. We treat the other case given in Lemma 7(b). Let $\operatorname{sgn}s<u<S-s+\operatorname{sgn}s$.

We have $v(p^u-\delta_l)=u$ and $v(p^u-\delta_j)=b_j$ for all $1\leq j\leq l-1$. So we compute

$$v(g(p^u))=\sum_{j=1}^{l}v(p^u-\delta_j)=u+\sum_{j=1}^{l-1}b_j=u+s-\operatorname{sgn}s.$$

We have $v(f(p^u))\geq u$, but also $v(f(p^u))\geq s+u-1$. To prove the latter, we distinguish two cases. If $a_i\leq u$ for all $1\leq i\leq k$, then $v(p^u-\gamma_i)\geq a_i$, which yields

$$v(f(p^u))=\sum_{i=1}^{k}v(p^u-\gamma_i)\geq\sum_{i=1}^{k}a_i\geq S>s+u-1.$$

So assume that there exists an index $1 \le i \le k$ with $a_i > u$, say $a_k > u$. Put

$$I := \{1 \le i \le k \mid 0 < a_i < 1\}$$

and let t_I be the number of indices i with $a_i \ge 1$. By Lemma 5, we find $s \le \sum_{i \in I} a_i + t_I$. On the other hand, we have $v(p^u - \gamma_i) = a_i$ for all $i \in I$. Summing yields

$$v(f(p^u)) = \sum_{i=1}^{k} v(p^u - \gamma_i) = u + \sum_{i=1}^{k-1} v(p^u - \gamma_i) =$$

$$= u + \sum_{i \in I} a_i + \sum_{i \in \{1,\dots,k-1\} \setminus I} v(p^u - \gamma_i) \ge u + \sum_{i \in I} a_i + t_I - 1 \ge u + s - 1.$$

We deduce that

$$v(\gcd(f(p^u), g(p^u))) = u + s - \operatorname{sgn} s,$$

which takes all integer values in the open interval (s, S) when u runs over integers in $(\operatorname{sgn} s, S - s + \operatorname{sgn} s)$. ☐

Remark. Assuming $s \ge 1$ and noting $S \ge s$ in Theorem 6(a) yields $v(r) \ge p$, which is the statement of [1, Proposition 8(a)].

Remark. The above proof shows that one can weaken the assumption in Theorem 6(b): it suffices to assume that the estimate in case $m = 0$ of Lemma 7(a) is sharp for the choice of f and g.

Construction 8. *Let p be a prime and assume that $0 \le s \le S$ and, in case $p = 2 \le s$, also that $2s + 1 \le S$. Then there exists a pair $f, g \in \mathbb{Z}[x]$ of monic polynomials such that $\min_{n \in \mathbb{Z}} v(\gcd(f(n), g(n))) = s$, $\max_{n \in \mathbb{Z}} v(\gcd(f(n), g(n))) = S$, and $v(r) - S = ps^2 - s$ holds for the resultant r. In particular, the estimate in Theorem 6(a) is sharp for any prime $p \ge 2$ and any $0 \le s \le p$.*

Proof. If $s = S = 0$ we simply take $f(x) = 1$ and $g(x)$ arbitrary. In case $s = 0 < S$ (resp. $s = 1 \le S$) we pick $f(x) = x$ (resp. $f(x) = x(x-1)$) and $g(x) = x - p^S$ (resp. $g(x) = (x - p^S)(x - 1 - p)$).

For $s \ge 2$ and p odd, the example is

$$f(x) = x(x - 2p)^{s-1} \prod_{j=1}^{p-1} (x - j)^s$$

and

$$g(x) = (x - p^{S-s+1})(x - p)^{s-1} \prod_{j=1}^{p-1} (x - j - p)^s \ .$$

Under this choice, we clearly have $s = \min_{n \in \mathbb{Z}} v(\gcd(f(n), g(n)))$. On the other hand, $f(0) = 0$ and $v(g(0)) = S$, whence

$$\max_{n \in \mathbb{Z}} v(\gcd(f(n), g(n))) \le S.$$

Moreover, if $n \equiv j \neq 0 \pmod p$ $(j = 1, \dots, p-1)$, then n cannot be congruent to both j and $j+p$ modulo p^2, whence

$$v(\gcd(f(n), g(n))) = s.$$

Further, if $p \mid n$, then we distinguish three cases:

(i) $n \equiv 0 \pmod{p^{S-s+2}}$. Then

$$v(n - p^{S-s+1}) = S - s + 1 \text{ and } v(n-p) = 1,$$

whence $v(g(n)) = S$.

(ii) $n \equiv p^{S-s+1} \pmod{p^{S-s+2}}$. Then

$$v(n) = S - s + 1 \text{ and } v(n - 2p) = 1,$$

showing that $v(f(n)) = S$.

(iii) $0 \not\equiv n \not\equiv p^{S-s+1} \pmod{p^{S-s+2}}$. In this case, we have

$$v(n) = v(n - p^{S-s+1}) \leq S - s + 1,$$

and n cannot be congruent to both p and $2p$ modulo p^2, showing that $v(\gcd(f(n), g(n))) \leq S$.

In all cases, we obtained $v(\gcd(f(n), g(n))) \leq S$, showing that S is the maximum. Finally, we compute

$$v(r) = v\left(g(0)g(2p)^{s-1}\prod_{j=1}^{p-1} g(j)^s\right) =$$

$$= v(g(0)) + (s-1)v(g(2p)) + s\sum_{j=1}^{p-1} v(g(j)) =$$

$$= S + (s-1)s + s(p-1)s = ps^2 - s + S$$

as claimed.

Finally, if $p = 2 \leq s \leq (S-1)/2$, then we take

$$f(x) = x(x-2)^{s-1}(x-1)^s$$

and

$$g(x) = (x - 2^{S-2s+2})(x-4)^{s-1}(x-3)^s.$$

A simple computation similar to the one above shows the statement. □

References

[1] Frenkel P. E., Pelikán J., On the Greatest Common Divisor of the Value of Two Polynomials, *The American Mathematical Monthly* **124**(5) (May 2017), 446–450.

[2] D. Gomez, J. Gutierrez, Á. Ibeas, D. Sevilla, Common factors of resultants modulo p, *Bull. Aust. Math. Soc.* **79** (2009), 299–302.

[3] S. Janson, Resultant and discriminant of polynomials, `https://www.semanticscholar.org`, 2010

[4] Keller G., Olson F. R., Counting polynomial functions (mod p^n), *Duke Math. J.* **35** (1968), 835–838.

[5] Kempner A. J., Polynomials and their residue systems, *Amer. Math. Soc. Trans.* **22** (1921), 240–288.
[6] D. I. Khomovsky, On the relationship between the number of solutions of congruence systems and the resultant of two polynomials, *INTEGERS – Electronic Journal of Combinatorial Number Theory* **16**, A41

ELTE Eötvös Loránd University, Faculty of Science, Institute of Mathematics, 1117 Budapest, Hungary, Pázmány Péter sétány 1/C & Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, 1053 Budapest, Hungary, Reáltanoda u. 13-15. ORCID ID: 0000-0003-2672-8772 and 0000-0002-7293-3569

E-mail address: frenkelp@cs.elte.hu, zger@cs.elte.hu