Divisor Function and Bounds in Domains with Enough Primes

Haydar Göral *

Abstract

In this note, first we show that there is no uniform divisor bound for the Bézout identity using Dirichlet's theorem on arithmetic progressions. Then, we discuss for which rings the absolute value bound for the Bézout identity is not trivial and the answer depends on the number of small primes in the ring.

Keywords: divisor function, arithmetic progression, polynomials, unique factorization domain

2000 AMS Classification: 13G, 11A25, 11N13

1. Introduction and Definitions

Let $d(n)$ be the number of positive divisors of a given positive integer n. More precisely,

$$d(n) = |\{m \geq 1 : m \text{ divides } n\}| = \sum_{m|n} 1.$$

For instance for a prime number p, we have $d(p) = 2$. If $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of n, then

$$d(n) = d(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1 + 1) \cdots (\alpha_k + 1). \tag{1.1}$$

The divisor function and its extensions have been studied extensively in terms of both analytic and arithmetic properties. It is well-known that (see [**?**, Chapter 3])

$$\sum_{n \leq x} d(n) \sim x \log x + (2\gamma - 1)x, \tag{1.2}$$

where γ is Euler's constant. Using equation (**??**), one can prove that for a given $\varepsilon > 0$ there exist $n_0 = n_0(\varepsilon) \geq 1$ and $C_\varepsilon > 0$ such that if $n \geq n_0$ then $d(n) \leq C_\varepsilon n^\varepsilon$. The remainder term in the asymptotic expansion (**??**) is an important problem in number theory and it is called the Dirichlet divisor problem. Details can be found in [**?**, **?**].

Now let R be a domain. The arithmetic version of Hilbert's Nullstellensatz states that if the polynomials $f_1, ..., f_s$ belong to the ring $R[X_1, ..., X_n]$ without a

*Department of Mathematics, Koç University, Rumelifeneri Yolu, 34450, Sarıyer, Istanbul, TURKEY, Email: hagoral@ku.edu.tr
Partially supported by ValCoMo (ANR-13-BS01-0006) and MALOA (PITN-GA-2009-238381)

common zero in an algebraically closed field containing R, then there exist a in $R \setminus \{0\}$ and $h_1, ..., h_s$ in $R[X_1, ..., X_n]$ such that

$$a = f_1h_1 + \cdots + f_sh_s. \tag{1.3}$$

One can see that Nullstellensatz implies its arithmetic version. Finding degree bounds for $h_1, ..., h_s$ in equation (**??**) has received continuous attention, see [**?**, **?**, **?**, **?**]. By $\deg f$, we mean the total degree of the polynomial f in several variables. More generally given a field K, if $f_0, f_1, ..., f_s$ in $K[X_1, ..., X_n]$ all have degree less than D and f_0 is in the ideal $\langle f_1, ..., f_s\rangle$, then

$$f_0 = \sum_{i=1}^{s} f_ih_i$$

for certain h_i whose degree is bounded by a constant $c_1(n, D)$ depending only on n and D, not to K, the number of generators s or the polynomials $f_1, ..., f_s$. This result was first validated in a paper of G. Hermann [**?**], where her pattern was based on linear algebra and computational methods.

Throughout this note R stands for an integral domain and K for its field of fractions.

Recall that an *absolute value* on R is a map $|\cdot| : R \to [0, \infty)$ such that

- $|x| = 0$ if and only if $x = 0$,
- $|xy| = |x||y|$,
- $|x + y| \leq |x| + |y|$.

For a polynomial $f \in R[X_1, ..., X_n]$, we put

$$|f| = \max_i\{|a_i|\}$$

where a_i occurs as a coefficient in the monomial expression of f. If there is an absolute value on R then it extends to K.

The following theorem follows immediately from [**?**].

1.1. Theorem. *Let R be a ring with an absolute value $|\cdot|$. For all $n \geq 1$, $D \geq 1$, $H \geq 1$ there are two constants $c_1(n, D)$ and $c_2(n, D, H)$ such that if $f_1, ..., f_s$ in $R[X_1, ..., X_n]$ have no common zero in the algebraic closure of K with $\deg(f_i) \leq D$ and $|f_i| \leq H$, then there exist nonzero a in R and $h_1, ..., h_s$ in $R[X_1, ..., X_n]$ such that*

(i) $a = f_1h_1 + \cdots + f_sh_s$
(ii) $\deg(h_i) \leq c_1$
(iii) $|a|, |h_i| \leq c_2$

Proof. The degree bound c_1 reduces the Bézout identity $a = f_1h_1 + \cdots + f_sh_s$ to a system of K-linear equations. Applying Gauss-Jordan method to this linear system one obtains an estimate for the absolute value of a and the polynomials h_i. In other words, the existence of the constant c_1 yields the existence of c_2. □

1.2. Remark. The constants c_1 and c_2 do not depend on s because the vector space

$$V(n,D)=\{f\in K[X_1,...,X_n]:\deg(f)\leq D\}$$

is finite dimensional over K. In fact the dimension is $q=q(n,D)=\binom{n+D}{n}$. Given $1=f_1h_1+\cdots+f_sh_s$ with $f_i\in V(n,D)$, we may always assume $s\leq q$.

Generally, the Gauss-Jordan method gives a very large value for c_2. In order to obtain more effective and sharp results for c_2, there is no technique for an arbitrary domain. In this note, our aim is to discuss for which domains the bound c_2 in Theorem **??** is not trivial and it is worth to try sharper estimates than the one given by the Gauss-Jordan method. We also show that there is no uniform divisor bound for the Bézout identity (**??**) when $R=\mathbb{Z}$. This means that Theorem **??** fails when we replace the absolute value with the divisor function with a method based on Dirichlet's theorem on arithmetic progressions.

Now we explain when the bound c_2 is trivial. If R is a ring equipped with an absolute value which has a non-zero element ε of absolute value <1, then we can multiply both sides of the Bézout identity

$$a=f_1h_1+\cdots+f_sh_s. \tag{1.4}$$

by some power of $\varepsilon\in R$. Thus, we get that

$$a\varepsilon^k=f_1\cdot(\varepsilon^kh_1)+\cdots+f_s\cdot(\varepsilon^kh_s).$$

Therefore, the bound c_2 in Theorem **??** can be taken 1 and Theorem **??** becomes trivial by [**?**]. In this note, we also answer when the bound c_2 exists non-trivially.

From now on, our ring R is a unique factorization domain, UFD for short, endowed with an absolute value $|\cdot|$. By a small element in R, we mean an element of absolute value less than 1. An element is called big if it is of absolute value larger than 1. If we multiply both sides of equation (**??**) by en element ε of absolute value <1, we see that the elements $a,h_1,...,h_s$ have a common divisor ε. However, if there is a unit u with $|u|<1$, then multiplying both sides of the equation with powers of u, the absolute value bound c_2 can be made small again as before, as units do not affect the prime factorization. So the interesting case is when there are no small units, which is equivalent to all the units have absolute value 1. So imposing the condition

$$\gcd(a,a_1,...,a_m)=1$$

where $a_1,...,a_m$ are all elements that occur as some coefficient of some h_i in equation (**??**) with all the units have absolute value 1 will make perfect sense for effective and sharper results as it prevents us from multiplying both sides of equation (**??**) by elements of small absolute value.

We give a criterion when we can choose a such that $\gcd(a,a_1,...,a_m)=1$ where $a_1,...,a_m$ are all elements that occur as some coefficient of some h_i in equation (**??**) and also ensure a uniform bound for $a,a_1,...,a_m$ depending on n,D and the absolute values of f_i as in Theorem **??**. Interestingly, the answer depends on the

number of primes in R of absolute value less than 1, and this suggests us the following two definitions.

1.3. Definition. We say that R is a UFD with the p-property if R is a unique factorization domain endowed with an absolute value such that every unit has absolute value 1 and if there are primes p and q satisfying

$$|p| < 1 < |q|,$$

then there exists another prime r non-associated to p with $|r| < 1$.

1.4. Definition. We say that R is a UFD with the 1-property if R is a unique factorization domain equipped with an absolute value such that every unit has absolute value 1, and there is only one prime p of absolute value less than 1, and there exists a prime q of absolute value greater than 1.

Next, we extend the divisor function to $\mathbb{Z}$. We let $d(0) = 0$ and if $a < 0$ then we define $d(a) = d(-a)$. For a polynomial $f \in \mathbb{Z}[X_1, ..., X_n]$, we put

$$d(f) = \max_i \{d(a_i)\}$$

where a_i occurs as a coefficient in the monomial expression of f. Now we can state our results.

1.5. Theorem. *There is no uniform divisor bound for the Bézout identity. Precisely, there exist polynomials $f_{n1}, f_{n2}, g_{n1}, g_{n2}$ in $\mathbb{Z}[X]$ with*

$$d(f_{n1}), d(f_{n2}), d(g_{n1}), d(g_{n2}) \leq 3$$

such that f_{n1}, f_{n2} do not have a common zero in $\mathbb{C}$, the polynomials g_{n1}, g_{n2} also do not have a common zero in $\mathbb{C}$, and for every $u_{n1}, u_{n2}, v_{n1}, v_{n2}$ in $\mathbb{Z}[X]$ and $a_{n1}, a_{n2} \in \mathbb{Z} \setminus \{0\}$ with

$$f_{n1}u_{n1} + f_{n2}u_{n2} = a_{n1}$$

and

$$g_{1n}v_{1n} + g_{2n}v_{2n} = a_{n2}$$

we have

$$\lim_{n\to\infty} d(u_{n1}) = \lim_{n\to\infty} d(a_{n2}) = \infty.$$

The condition (iv) in the following theorem makes the computation of the absolute value constant c_2 non-trivial.

1.6. Theorem. *Let R be a domain with an absolute value $|\cdot|$. For all $n \geq 1$, $D \geq 1$, $H \geq 1$ there are two constants $c_1(n, D)$ and $c_2(n, D, H)$ such that if $f_1, ..., f_s$ in $R[X_1, ..., X_n]$ have no common zero in the algebraic closure of K with $\deg(f_i) \leq D$ and $|f_i| \leq H$, then there exist nonzero a in R and $h_1, ..., h_s$ in $R[X_1, ..., X_n]$ such that*

(i) $a = f_1h_1 + \cdots + f_sh_s$
(ii) $\deg(h_i) \leq c_1 + D + 1$
(iii) $|a|, |h_i| \leq c_2$
(iv) *If R is a UFD with the p-property, then we can choose a and $a_1, ..., a_m$ such that $\gcd(a, a_1, ..., a_m) = 1$ where $a_1, ..., a_m$ are all elements that occur as some coefficient of some h_i.*

- *Moreover, if R is a UFD with the 1-property, then we cannot ensure the existence of c_2 and $\gcd(a, a_1, ..., a_m) = 1$ simultaneously.*

Note also that if $|ab| < 1$ then $|a|$ can be very large and $|b|$ can be very small. So cancellation can make the absolute values larger if there are sufficiently small and big elements in the ring. Thus for the equation

$$a = f_1h_1 + \cdots + f_sh_s,$$

simply dividing by $\gcd(a, a_1, ..., a_m)$ may not work in order to obtain (iv) in the previous theorem.

2. Preliminaries

In this section, we prove several lemmas and we also give some examples of UFD with the p-property and 1-property. First, we recall Dirichlet's theorem on arithmetic progressions.

2.1. Fact. *(Dirichlet) For any two positive coprime integers a and q, there are infinitely many primes of the form*

$$a + nq,$$

where n is a non-negative integer. In other words, there are infinitely many primes p which are congruent to a modulo q.

The proof of Dirichlet's theorem is based on the non-vanishing of Dirichlet L-functions at 1. For more on Dirichlet's theorem, its generalizations and some special values of L-functions, we refer the reader to [**?**, **?**]. The next lemma will play a key role in the proof of Theorem **??**.

2.2. Lemma. *There exist two sequences $\{\alpha_n\}$ and $\{\beta_n\}$ in $\mathbb{N}$ such that $d(\alpha_n) \leq 2$ and $d(\beta_n) \leq 2$ but*

$$\lim_{n\to\infty} d(\alpha_n + \beta_n) = \infty.$$

Proof. Let $n \geq 1$ be a positive integer and p be a given prime number. Note that p^n and $p^n - 1$ are coprime positive integers. By Dirichlet's theorem on arithmetic progressions, the arithmetic progression

$$p^n - 1, p^n - 1 + p^n, ..., p^n - 1 + kp^n, ...$$

contains infinitely many prime numbers. Let p_n be a prime number in this arithmetic progression. Let $\alpha_n = 1$ and $\beta_n = p_n$. Clearly $d(\alpha_n) = 1$ and $d(\beta_n) = 2$. However, the sum $\alpha_n + \beta_n$ is divisible by p^n and so $d(\alpha_n + \beta_n) \geq n + 1$. Hence we are done. □

Now we give two examples of rings which have the p-property. At a first glance, the existence of a ring with the 1-property is not clear.

2.3. Example.
- $\mathbb{Z}$ is a UFD with the p-property whose all primes have absolute value greater than 1.
- $\mathbb{Z}_p$ (p-adic integers) is a UFD with the p-property whose only prime p has absolute value $1/p$.

Next, we recall the Gauss lemma. Let $f = a_0 + a_1X + \cdots + a_dX^d$ be in $\mathbb{Q}[X]$. For any prime number p in $\mathbb{N}$ we define

$$|f|_p = \max_i\{|a_i|_p\},$$

where $|\cdot|_p$ is the p-adic absolute value on $\mathbb{Q}$ with $|p|_p = 1/p$.

2.4. Lemma. *(Gauss lemma [?, 1.6.3]) Suppose that f and g are in $\mathbb{Q}[X]$. For any prime number p, we have $|fg|_p = |f|_p|g|_p$.*

Now we give an example of a ring with the p-property which has infinitely many small and big primes. We also give an example of a ring with the 1-property.

2.5. Lemma. *There exist rings S_1 and S_2 such that S_1 is a UFD with the p-property which has infinitely many small and big primes and S_2 is a UFD with the 1-property.*

Proof. Let $\gamma \in (0,1)$ be a transcendental number. Then the ring $S_1 = \mathbb{Z}[\gamma]$ can be seen as a unique factorization domain since it is isomorphic to $\mathbb{Z}[X]$ and its units are only 1 and -1. We put the usual absolute value on S_1 as it is a subset of $\mathbb{R}$. Then S_1 has infinitely many primes p with $|p| < 1$ and infinitely many primes q with $|q| > 1$. In particular S_1 is a UFD with the p-property.

Now let p be a prime number in $\mathbb{N}$. On $\mathbb{Z}[X]$, we define

$$|a_0 + a_1X + \cdots + a_kX^k| := \max_i p^i|a_i|_p = \left|a_0 + \frac{a_1}{p}X + \cdots + \frac{a_k}{p^k}X^k\right|_p.$$

Then $S_2 = \mathbb{Z}[X]$ becomes a UFD with the 1-property by the Gauss lemma with the absolute value above, and the only small prime is p in S_2 which is of absolute value $1/p$. □

2.6. Lemma. *Suppose R is a UFD with the p-property. If there are primes p and q with $|p| < 1 < |q|$, then there are infinitely many non-associated primes with absolute value strictly less than 1 and infinitely many non-associated primes with absolute value strictly larger than 1.*

Proof. By definition, we know there are at least two non-associated primes with absolute value less than 1. Let $p_1, ..., p_k$ (for $k \geq 2$) be non-associated primes with absolute value less than 1. Put $A = p_1 \cdots p_k$. Now choose m large enough such that

$$\left|\sum_{i=1}^{k}(A/p_i)^m\right| < 1.$$

Since this element is not a unit as all the units have absolute value 1, it must be divisible by a prime whose absolute value is strictly less than 1. This yields us a new prime. For the second part, given $q_1, ..., q_k$ primes of absolute value larger than 1, for large n the element ${q_1}^n q_2 \cdots q_k + 1$ provides a new prime that has absolute value greater than 1. □

3. Proof of Theorem ??

Set $f_{n1} = \alpha_n + X + \beta_n^2 X^2$ and $f_{n2} = X^3$ where α_n and β_n are as in Lemma **??**. Recall that $\alpha_n = 1$ for all $n \geq 1$. Then $d(f_{n1})$ and $d(f_{n2})$ are bounded by 3 and they have no common zero in $\mathbb{C}$. However, whenever we write

$$a_{n1} = f_{n1}u_{n1} + f_{n2}u_{n2}$$

where a_{n1} is non-zero, then u_{n1} must have degree bigger than 2 and the first three coefficients of u_{n1} are uniquely determined: if

$$u_{n1}(X) = e_0 + e_1 X + e_2 X^2 + \cdots + e_k X^k$$

then automatically we have $e_0 = a_{n1}$, $e_1 = -a_{n1}$ and $e_2 = a_{n1}(\alpha_n - \beta_n)(\alpha_n + \beta_n)$. Hence

$$d(u_{n1}) \geq d(e_2) \geq d(\alpha_n + \beta_n) \geq n + 1.$$

Moreover if we put $g_{n1} = \alpha_n + X$ and $g_{n2} = \beta_n - X$ then they have no common zero. Similarly, whenever we write

$$a_{n2} = g_{n1}v_{n1} + g_{n2}v_{n2},$$

then we see that $d(a_{n2}) \geq d(\alpha_n + \beta_n) \geq n + 1$. Thus a_{n2} has many divisors although $d(g_{n1})$ and $d(g_{n2})$ are bounded by 2. □

4. Proof of Theorem ??

We already know the existence of c_1 and c_2 by Theorem **??**. Now we prove (iv) and we still keep (i), (ii) and (iii). Clearly we may assume that $s \geq 2$ and a is not invertible. Assume R is a UFD with the p-property. We need to choose a and $a_1, ..., a_m$ such that

$$\gcd(a, a_1, ..., a_m) = 1$$

where $a_1, ..., a_m$ are all elements that occur as some coefficient of some h_i. If all the primes in R have absolute value larger than 1 or smaller than 1 (like R is $\mathbb{Z}$ or $\mathbb{Z}_p$ respectively), then we can divide both sides of the equation

$$a = f_1 h_1 + f_2 h_2 + \cdots + f_s h_s$$

by $\gcd(a, a_1, ..., a_m)$ and get the result because if all the primes in R have absolute value greater than 1, then cancellation makes the absolute value smaller and if all the primes in R have absolute value less than 1 then we can take c_2 to be 1. The remaining case is when there are primes of absolute value larger than 1 and primes of absolute value smaller than 1. Let d be the greatest common divisor of all the coefficients of f_1 and f_2. Then, the coefficients of f_1/d and f_2/d have no common divisor. On the other hand, since there are both small and large elements in the ring, the element d can be very small and so f_1/d and f_2/d may have very large absolute values. Let $p_1, ..., p_k$ be the all prime divisors of a. By Lemma **??**, there are infinitely many primes with absolute value strictly less than 1. Now choose a prime p such that $|p| < 1$ and p does not divide a, in other words p is not in the finite set $\{p_1, ..., p_k\}$. Choose a natural number k such that $\frac{p^k f_1}{d}$ and $\frac{p^k f_2}{d}$ have absolute values less than c_2. Put $v = c_1(n, D) + 1$. Then, we have

$$0 = f_1 \cdot \frac{p^k X_1^v f_2}{d} - f_2 \cdot \frac{p^k X_1^v f_1}{d}.$$

Therefore, by adding the previous equation to $a = f_1h_1 + f_2h_2 + \cdots + f_sh_s$, we obtain that

$$\begin{aligned} a &= f_1\left(h_1 + \frac{p^k X_1^v f_2}{d}\right) + f_2\left(h_2 - \frac{p^k X_1^v f_1}{d}\right) + \cdots + f_s h_s \\ &= f_1t_1 + f_2t_2 + \cdots + f_st_s \end{aligned}$$

where $\deg t_i \leq c_1 + D + 1$ and $|t_i| \leq c_2$. Observe that

$$\gcd(a, a_1, ..., a_m) = 1$$

where $a_1, ..., a_m$ are all elements that occur as some coefficient of some t_i.

Finally, we prove the remaining part of the Theorem. Let p be the unique small prime in R of absolute value less than 1. The reason behind the last part of the Theorem is the fact that an element has small absolute value if and only if its p-adic valuation is very large. Let B be an element in R of absolute value very big and coprime to p. Choose m minimal such that $|p^m B| \leq 1$. Similarly choose k minimal such that $|p^k B| \leq c_2$. Note that as B is very large then so are m and k. Let $n = D = H = 1$. Set $f_1 = p^{2m+1} + p^{2m}X$ and $f_2 = p^m B - p^m BX$. Clearly f_1 and f_2 have no common zero since

$$p^{2m}B(p+1) = Bf_1 + p^m f_2$$

and p is not -1. Whenever we write $a = f_1h_1 + f_2h_2$, we get that p^m divides h_2 and B divides h_1. Also we have that $p^{2m}B$ divides a. Now suppose $|h_i| \leq c_2$ for $i = 1, 2$. Since B divides h_1, we see that p^k divides h_1 since p is the unique small prime in R. Thus p^k divides a, h_1 and h_2. Furthermore, we may assume that the only prime divisor of a, h_1 and h_2 is p, because if there is q dividing all of them which is coprime to p, then there is $\ell \geq k$ such that p^ℓ divides h_1 in order to make the absolute value of h_1 less than c_2. Similar observation shows that p^ℓ also divides h_2 and a. Therefore, in order to satisfy the coprimality in the theorem, we need to divide a, h_1 and h_2 by p^k. So the absolute value of h_1/p^k becomes larger than B. □

We end our note by posing the following question:

4.1. Question. What is the condition on $f_1, ..., f_s$ to obtain a uniform divisor bound for a and $h_1, ..., h_s$ in (**??**)? For which rings that are a UFD with the p-property which have infinitely many small and big primes, we can obtain sharper estimates for c_2 which is better than the constant given by the Gauss-Jordan method?

References

[1] E. Alkan, *Values of Dirichlet L-functions, Gauss sums and trigonometric sums*, The Ramanujan Journal, 2011, Volume 26, Issue 3, 375–398.

[2] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, First edition, 1976.

[3] B. C. Berndt, S. Kim and A. Zaharescu, *The circle and divisor problems, and Ramanujan's contributions through Bessel function series*, The legacy of Srinivasa Ramanujan, 111–127, Ramanujan Math. Soc. Lect. Notes Ser., 20, Ramanujan Math. Soc., Mysore, 2013.

[4] E. Bombieri, W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs, Cambridge University Press, 2006.

[5] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics, Third edition, Springer, New York, 2000.
[6] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, 6th Edition, Oxford University Press, 2008.
[7] K. Hentzelt, E. Noether, *Zur Theorie der Polynomideale und Resultanten*, Math. Ann. **88**, 1923, 53–79.
[8] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788.
[9] J. Kollár, *Sharp Effective Nullstellensatz*, J. of the American Math. Soc. Volume 1, Number 4, (1988), 963–975.
[10] A. Seidenberg, *Constructions in algebra*, Trans. AMS **97**, (1974), 273–313.