Equidistribution of Divisors and Representations by Binary Quadratic Forms

Michael Drmota and Mariusz Skałba[1]

Abstract

We study the number of divisors in residue classes modulo m and prove, for example, that there is an exact equidistribution if and only if $m = 2^k p_1 p_2 \dots p_s$ where k and s are non-negative integers and p_j are distinct Fermat primes. We also provide a general lower bound for the proportion of divisiors in the residue class 1 mod m. Finally we present lower bounds for the number of representations by a binary quadratic form with a negative discriminant.

1 Introduction

Let $m > 1$ be a fixed natural number and $r \in \mathbb{Z}$ relatively prime to m. Our goal is to compare the behaviour of the two arithmetical functions

$$D_{m,\alpha,r}(n) = \sum_{d|n, d\equiv r \pmod m} d^\alpha$$

and "the total divisor function"

$$D_{m,\alpha}(n) = \sum_{d|n} d^\alpha$$

where α is a real parameter and we make the convention that functions $D_{m,\cdot}(n)$ are defined only for n relatively prime to m.

We shall show that for most natural n (coprime to m) the approximation

$$D_{m,\alpha,r}(n) \approx \frac{1}{\varphi(m)} D_{m,\alpha}(n)$$

holds independently on r (which are also coprime to m). Moreover we will characterize those n, for which the above approximations can be replaced by exact equalities. This is only possible for $\alpha = 0$. In such case we say that *divisors of n are equidistributed mod m*. The set of all such n will be denoted by $ED(m)$. It turn out that for any m the set $ED(m)$ is big. It contains a complete infinite arithmetic progression and intersects every arithmetic progression too - so $ED(m)$ is a dense open set in Furstenberg's topology [5]. We characterize as well those moduli m for which the set $ED(m)$ is very big, in the sense that it contains almost all natural numbers that are coprime to m. These are precisely those m for which the regular m-gon can be constructed by compass and rule. Moreover we prove that for any natural number n (coprime to m) at least a positive proportion of its divisors ly in the residue class $1 \mod m$.

[1]This work was supported by the Austrian Science Foundation, grant Nr. M 00233–MAT.

In the last part of the paper similar theorems are provided for the number of representations of a given natural number n by a positive definite binary quadratic form.

Results concerning upper bounds for the number of divisors in residue classes are obtained in [4, 7, 2].

2 Divisors

Theorem 1. *Let m be a positive integer. Then for almost all natural numbers n (coprime to m) the following estimate holds*

$$\left|\frac{D_{m,\alpha,r}(n)}{D_{m,\alpha}(n)} - \frac{1}{\varphi(m)}\right| < \frac{a(m)}{(\log n)^{b(m)}} \tag{1}$$

with positive constants $a(m), b(m)$ depending only on m.

Proof. With the help of Dirichlet characters we have

$$D_{m,\alpha,r}(n) = \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi(r)} \sum_{d|n} \chi(d) d^{\alpha} \tag{2}$$

and consequently we obtain

$$\left|\frac{D_{m,\alpha,r}(n)}{D_{m,\alpha}(n)} - \frac{1}{\varphi(m)}\right| \le \frac{1}{\varphi(m)} \sum_{\chi \ne \chi_0} \prod_{p^k \| n} \left|\frac{1 + \chi(p)p^{\alpha} + \ldots + \chi(p^k)p^{\alpha k}}{1 + p^{\alpha} + \ldots + p^{\alpha k}}\right|$$

There exists a positive constant $c(m) < 1$ depending only on m such that if $\chi(p) \ne 1$ then

$$\left|\frac{1 + \chi(p)p^{\alpha} + \ldots + \chi(p^k)p^{\alpha k}}{1 + p^{\alpha} + \ldots + p^{\alpha k}}\right| \le c(m).$$

By Hardy and Ramanujan [6] the function $\log\log n$ is a normal order of the function $\omega(n)$, hence for any $c \in (0, 1)$ almost all natural numbers n relatively prime to m have at least $c \log\log n$ distinct prime factors. This directly leads to (1).

Theorem 2. *Let m be a positive integer. For $n \in \mathbf{N}$ (coprime to m) the equality*

$$D_{m,\alpha,r}(n) = \frac{1}{\varphi(m)} D_{m,\alpha}(n) \tag{3}$$

holds for any r relatively prime to m if and only if $\alpha = 0$ and for any non-principal Dirichlet's character χ there exists a prime p with $p^k \| n$ such that

$$\chi(p) \ne 1 \quad \textit{and} \quad \chi(p)^{k+1} = 1$$

Proof. In virtue of the explicit formula (2) and the independence of Dirichlet characters the proposed equidistribution property is equivalent to the conditions

$$\sum_{d|n} \chi(d) d^{\alpha} = 0 \qquad \text{for} \quad \chi \ne \chi_0$$

and further to

$$\prod_{p^k \| n} (1 + \chi(p)p^{\alpha} + \ldots + \chi(p^k)p^{k\alpha}) = 0 \qquad (\chi \ne \chi_0)$$

Hence for any non-principal χ there exists a prime p with $p^k \| n$ such that

$$\chi(p) \neq 1 \qquad \text{and} \quad (\chi(p)p^{\alpha})^{k+1} = 1$$

and the assertion follows.

Remark. For $m = 4$ and $\alpha = 0$,$\alpha = 1$ the Theorem 2 has an interesting interpretation in the theory of quadratic forms. A classical result states that the number of representations of an odd natural number n as the sum of two squares equals to

$$4(D_{4,0,1}(n) - D_{4,0,3}(n)).$$

The condition given in Theorem 2 states now that n is not representable as the sum of two squares if and only if there exists $p \equiv 3 \mod 4$ such that $p^k \| n$ with odd k.

On the other hand the number of representations of an odd n as the sum of four squares is equal by Jacobi to

$$8(D_{4,1,1}(n) - D_{4,1,3}(n))$$

and again Theorem 2 is consistent with Lagrange theorem stating that the above number is always positive!

We recall that $ED(m)$ is the set of positive integers n (coprime to m) such that $D_{m,0,r}(n) = \frac{1}{\varphi(m)} D_{m,0}(n)$ holds for all r (coprime to m).

Theorem 3. *For any $m > 1$ the set $ED(m)$ contains an infinite arithmetic progression, whereas its complement $\mathbf{N} \setminus ED(m)$ does not contain an infinite progression.*

Proof. For any non-principal χ choose p_χ a prime such that $\chi(p_\chi) \neq 1$. Now choose $k_\chi \in \mathbb{N}$, such that $\chi(p_\chi)^{k_\chi+1} = 1$. By Theorem 2 the arithmetic progression

$$\prod_{\chi \neq \chi_0} p_\chi^{k_\chi} + t \prod_{\chi \neq \chi_0} p_\chi^{k_\chi+1}$$

meets our requirements. To prove the second part let us first remark that if $n_1 \in ED(m)$ and $\gcd(n_1, n_2) = 1$ than $n_1 n_2 \in ED(m)$ as well. Consider an arithmetic progression $b + ta$ and choose p_χ, k_χ as above but additionally p_χ cannot divide a. The non-empty subsequence of $b + ta$ determined by the congruence

$$at + b \equiv \prod_{\chi \neq \chi_0} p_\chi^{k_\chi} \mod \prod_{\chi \neq \chi_0} p_\chi^{k_\chi+1}$$

consists completely of elements of $ED(m)$. So we have proved even a stronger assertion.

Theorem 4. *The set $ED(m)$ consists of almost all natural numbers (coprime to m) if and only if*

$$m = 2^k p_1 p_2 \dots p_s,$$

where k and s are non-negative integers and p_j are distinct Fermat primes.

Proof. First let us assume that almost all natural numbers (coprime to m) are in $ED(m)$. Choose $n \in ED(m)$ squarefree. Hence $\varphi(m) | D_{m,0}(n) = 2^{\omega(n)}$, where $\omega(n)$ stands for the number of distinct primes dividing n. Of course implies that m must be of the form stated in the theorem.

Conversely, assume that m is of this form. It implies that any non-principal character χ attains the value -1. Let us denote by $P(\chi)$ the set of primes p with property $\chi(p) = -1$. This set is a union of some arithmetic progressions with common difference m intersected with the set of all primes. For a given non-principal χ let $M_\chi(x)$ denotes the number of $n \le x$ such that every $p \in P(\chi)$ appears of even order in n, that is, $p \| n$ implies $2|k$. By Dirichlet's prime number theorem and simple sieve-reasoning it follows easily that

$$M_\chi(x) = O\left(\frac{x}{(\log x)^{\frac{s_\chi}{\varphi(m)}}}\right)$$

where s_χ is the number of arithmetical progressions determining $P(\chi)$ (see e.g. [9], p.147, ex.4). If $ED(m,x)$ denotes the number of $n \in ED(m)$ with $n \le x$ then by Theorem 2

$$ED(m,x) \ge x - \sum_{\chi \ne \chi_0} M_\chi(x)$$

and this completes the proof.

Before we formulate the last theorem concerning divisors recall some useful definition. For any finite Abelian group G we define $D(G)$, the Davenport constant of G, as the smallest natural number k such that from any sequence $g_1, \dots, g_k \in G$ one can extract a subsequence $g_{i_1}, \dots, g_{i_t}$ satisfying

$$g_{i_1} \cdot \ldots \cdot g_{i_t} = e.$$

For simplicity let $G(m)$ denote the multiplicative group of reduced residue classes mod m.

Theorem 5. *For any natural number n, relatively prime to m we have*

$$D_{m,0,1}(n) \ge \frac{1}{2^{D(G(m))-1}} D_{m,0}(n)$$

Moreover this estimate is optimal.

Proof. The inequality is a direct consequence of the following general theorem of Zakarczemny, proved in his doctoral thesis [11]:

Zakarczemny's Theorem. *Let G be a finite Abelian group and $g_1, \dots, g_m$ the sequence of its elements. For any sequence of positive integers $(b_1, \dots, b_m)$ the number N of sequences $(e_1, \dots, e_m)$ fulfilling*

$$g_1^{e_1} \cdot \ldots \cdot g_m^{e_m} = e$$

and

$$0 \le e_j \le b_j, \text{ for } 1 \le j \le m,$$

satifies the inequality

$$N \ge 2^{1-D(G)} \prod_{j=1}^{m} (b_j + 1).$$

which is optimal. (A list of references to earlier partial results from many authors can be also found in [11].)

3 Representations by binary quadratic forms

Consider the equation
$$F(x,y)=n, \tag{4}$$
where $F(x,y)=ax^2+bxy+cy^2$ with $a,b,c\in\mathbb{Z}$ satisfying $a>0$, $\Delta=b^2-4ac<0$ and $\gcd(a,b,c)=1$. Although we are interested only in the form F we shall consider for any negative integer $\Delta\equiv 0,1 \pmod 4$ the whole form class group $C(\Delta)$ of all equivalence classes of integral binary primitive quadratic forms with discriminant Δ. The group structure in $C(\Delta)$ is given by Gauss composition of classes, see [3]. The symbol $C^2(\Delta)$ denotes the subgroup of squares in $C(\Delta)$. By Gauss theory $C^2(\Delta)$ coincides with the main-genus subgroup of $C(\Delta)$ but we will not use this important theorem. From now on assume that there are $x_0,y_0\in\mathbb{Z}$ satisfying $\gcd(x_0,y_0)=1$ and $F(x_0,y_0)=n$ and let us ask for the number $N_F(n)$ of all $x,y\in\mathbb{Z}$ satisfying (4). We can also ask for the number $N_F^*(n)$ of $x,y\in\mathbb{Z}$ satisfying (4) and additionally $(x,y)=1$. We adopt here and in the sequel the following convention: we identify (x,y) and $(-x,-y)$ in the definitions of $N_F(n)$ and $N_F^*(n)$. First we prove a lower bound for $N_F^*(n)$.

Theorem 6. *Let F be a binary quadratic form with coprime coefficients and negative discriminant Δ and let n be a positive integer that is represented by F by coprime integers and satisfies $\gcd(n,\Delta)=1$. Then we have*
$$N_F^*(n)\ge 2^{1-D(C^2(\Delta))}\cdot 2^{\omega(n)}. \tag{5}$$
where $\omega(n)$ stands for the number of distinct primes dividing n.

Proof. In order to prove (5) we need the correspondence between the quadratic forms and quadratic orders ([1, 3, 10]) and reformulate the problem as follows. Let K be a class of proper ideals of the order $\mathcal{O}_\Delta$ corresponding to the class of the form F – the class K is an element of the ideal-class-group $C(\mathcal{O}_\Delta)$. Further, let $S(K,n)$ denote the set of all integral ideals of $\mathcal{O}_\Delta$) lying in the class K, having no rational factor but norm n. By assumption $S(K,n)\neq\emptyset$ so let us fix some $I\in S(K,n)$. Let
$$I=\mathfrak{p}_1^{k_1}\cdot\ldots\cdot\mathfrak{p}_m^{k_m}$$
be the canonical decomposition of I into prime ideals of $\mathcal{O}_\Delta$. All $\mathfrak{p}_j$ are pairwise distinct, not conjugate and $\bar{\mathfrak{p}_j}\neq\mathfrak{p}_j$. Now let $J\in S(K,n)$ be different from I. We have
$$J=\prod_{j\in A}\bar{\mathfrak{p}}_j^{k_j}\prod_{j\notin A}\mathfrak{p}_j^{k_j} \tag{6}$$
and the property that
$$\prod_{j\in A}(\mathfrak{p}_j^{k_j})^2 \tag{7}$$
is principal, where $\emptyset\neq A\subseteq\{1,\ldots,m\}$ is uniquely determined by J. On the other hand, any A with the propery that the ideal (7) is principal produces by the formula (6) an ideal J in $S(K,n)$. In virtue of this bijection the proof of (5) is finished by applying a very special case of the above theorem of Zakarczemny for $b_1=\ldots=b_m=1$ (by the way this is a classical theorem of J.E. Olson and has been proved in [8]).

The corresponding result concerning arbitrary representations is the following one.

Theorem 7. *Let F be a binary quadratic form with coprime coefficients and negative discriminant Δ and let n be a positive integer that is represented by F by coprime integers and satisfies* $\gcd(n, \Delta) = 1$. *Then we have*

$$N_F(n) \geq 2^{1-D(C^2(\Delta))}\tau(n) \tag{8}$$

where $\tau(n)$ stands for the number of all positive divisors of n.

Proof. For $(x, y) \in \mathbb{Z}^2$ satisfying (4) we put $x' = x/D$, $y' = y/D$ with $D = \gcd(x, y)$. Then

$$F(x', y') = \frac{n}{D^2} \quad \text{and} \quad \gcd(x', y') = 1.$$

In this way we can see that

$$N_F(n) = \sum_{d|n} \Box(d) N_F^*(\frac{n}{d}),$$

where $\Box$ is the characteristic function of integral squares

$$\Box(d) = \begin{cases} 1 & \text{if} \quad d = D^2 \\ 0 & \text{in} \quad \text{other cases.} \end{cases}$$

By (5) we infer

$$N_F(n) \geq 2^{1-D(C^2(\Delta))} \sum_{d|n} \Box(d) 2^{\omega(n/d)}.$$

The sum on the right-hand side is a Dirichlet convolution of multiplicative functions and therefore it is multiplicative, too. We verify easily that for prime powers it coincides with τ, hence we get (8).

References

[1] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Nauka, Moscow 1985 (in Russian).

[2] D. Coppersmith, N.Howgrave-Graham, S.V.Nagaraj,*Divisors in residue classes, constructively*, Math. of Comp. 77 (2008), 531-545.

[3] D.A. Cox , *Primes of the form $x^2 + ny^2$*, Wiley-Interscience, New York 1989.

[4] H. Cohen, *Diviseurs appartenant a une meme classe residuelle*, Seminaire de Theorie Nomb. de Bordeaux 1982-83, 1-12.

[5] H. Furstenberg,*On the infinitude of primes*, American Mathematical Monthly, Vol. 62, 1955, p. 353.

[6] G.H.Hardy, S.Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Pure Appl. Math. 48 (1917), 76-92.

[7] H.W.Lenstra, *Divisors in residue classes*, Math. of Comp. 42 (1984), 331-340.

[8] J.E. Olson,*A combinatorial problem on finite Abelian groups*, J.Number Theory 1 (1969), 8-10.

[9] K. Prachar, *Primzahlverteilung*, Die Grundlehren der Math. Wissen. **91**, Springer-Verlag 1957.

[10] M. Skałba, *On numbers with a unique representation by a binary quadratic form*, Acta Arith. 64 (1993), 59-68.

[11] M. Zakarczemny, *Number of solutions in a box of a linear homogeneous equation in a finite Abelian group*, doctoral dissertation, Institute of Mathematics Polish Academy of Sciences 2012.

Michael Drmota
Institute of Discrete Mathematics and Geometry
Technical University of Vienna
Wiedner Hauptstrasse 8-10
A-1040 Vienna
Austria

Mariusz Skałba
Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warsaw
Poland