Записки научных
семинаров ПОМИ
Том 413, 2013 г.

A. Smirnov

ON EXACT FORMULAS FOR THE NUMBER OF INTEGRAL POINTS

Abstract. Exact formulas for the number of integral points in certain ellipses are obtained. These formulas generalize a formula of Eisenstein and belong to a rare type of exact formulas for the number of lattice points in curvilinear domains. The obtained formulas can be useful when studying the Riemann–Roch problem for arithmetic varieties.

Introduction

In this paper, we deal with the counting function for the number of integral points associated with a family of homothetic domains. In other words we are interested in the function $h(D,r) = \operatorname{card}(\mathbb{Z}^n \cap rD)$, where $D \subset \mathbb{R}^n$ and $r \geqslant 0$. One of the well-known approaches to computing this function is related to asymptotic formulas for h when r tends to infinity and to estimations for the error term. Below we do not discuss this approach, because we are interested in exact formulas only.

From the viewpoint of the algebro-geometric approach to number theory a free Abelian group Λ can be considered as a vector bundle on the arithmetic curve $X_0 = \operatorname{Spec}\mathbb{Z}$. Moreover a couple $E = (\Lambda, D)$, where $D \subset \mathbb{R} \otimes \Lambda$, can be considered as a vector bundle on a compactification $X = X_0 \cup \infty$. Here the inclusion $D \subset \mathbb{R} \otimes \Lambda$ plays the role of the inclusion $\Gamma(\operatorname{Spec}\mathcal{O}_{\mathbb{R}}, E) \subset \Gamma(\operatorname{Spec}\mathbb{R}, E)$, where $\operatorname{Spec}\mathcal{O}_{\mathbb{R}}$ can be thought as a formal neighborhood of the point ∞ and $\operatorname{Spec}\mathbb{R} = \operatorname{Spec}\mathcal{O}_{\mathbb{R}} - \infty$ can be thought as the picked formal neighborhood. Then the problem of computing the function $h(D,r)$ is nothing other than the Riemann–Roch problem for the arithmetical curve X.

There is a well-developed and highly nontrivial theory of exact formulas for h in the case, when D is a convex polytop in $\mathbb{R} \otimes \Lambda$ with the vertices

Key words and phrases: arithmetic curve, Riemann–Roch theorem, Eisenstein, imaginary quadratic field, exact formula, lattice point.

The research was partially supported by the RFFI grant 10-01-00551 and by the EPSRC Responsive Mode grant EP/G032556/1.

in Λ. In that case the function h coincides with the Ehrhart polynomial when $r = 0, 1, 2, \ldots$. For a concrete D this polynomial can be found by means of explicit computations with small r's. There are also theoretical formulas for the coefficients [2], obtained by applying the Riemann–Roch theorem to toric varieties. Main difficulties of this approach are related with computation of the Todd class for singular toric varieties.

At first glance there is no chance to get a finite exact formula for the counting function associated with a curvilinear domain D. However, in 1994, working together with M. Kapranov on an arithmetical Riemann–Roch theorem, the author found in [1, p. 29] the following formula

$$h(D, r) = 1 + 4\left(\left[\frac{r}{1}\right] - \left[\frac{r}{3}\right] + \left[\frac{r}{5}\right] - \left[\frac{r}{7}\right] + \cdots\right). \tag{1}$$

Here D is the standard unit disk in $\mathbb{R}^2$, and $[x]$ denotes the greatest integer $\leqslant x$. Ehrhart assigns this formula to Gauss with no concrete reference. I could not find the formula (1) in Gauss's papers. Recently M. Kapranov kindly informed me that he had found the same formula in Eisenstein's paper [3]. As far as I have understood from a conversation with D. Zagier this formula is not too widely known.

Thus, the aim of this paper is to generalize slightly the formula (1) and to attract attention to such results. Further generalizations, relations with the arithmetical Riemann–Roch theorem and with models of arithmetic varieties are left beyond the scope of this paper.

The author thanks N. Durov for nice versions of some statements. A part of these paper is written in the Max Planck Institute for Mathematics. The author thanks the Institute for the hospitality.

§1. Divisors with bounded norm

Eisenstein's formula and its generalizations are obtained below by a specialization of a formula for the number of the effective divisors with bounded norm. To count the divisors we need certain relations for the function

$$x \mapsto [x],$$

where $[x]$ denotes the greatest integer $\leqslant x$.

1.1. Some relations for entier-functions. Let C be an Abelian group, $D \subset \mathbb{R}$, and $h : D \to C$ be a function.

We say that h is an entier-function, if for any $x, y \in D$ the equality $[x] = [y]$ implies the equality $h(x) = h(y)$. In other words, $h : x \mapsto h(x)$ is an entier-function, if it depends on $[x]$ only.

For example, for any integer $d > 0$ the function

$$x \mapsto [x/d]$$

is an entier-function. Informally speaking, the entier-functions can be used to study "quotient-spaces similar to $\mathbb{R}/\mathcal{O}_{\mathbb{R}}$."

Theorem 1.1.1. *Let $\{1, 2, \dots\} \subset D \subset \mathbb{R}_{\geqslant 1} = [1, +\infty)$ and let $h : D \to C$ be an entier-function. Then there exists a unique sequence $a_1, a_2, \dots \in C$, such that*

$$h(x) = a_1[x] + a_2[x/2] + \cdots \tag{2}$$

for every $x \in D$.

Proof. Under the assumptions of the theorem the formula (2) is equivalent to the set of relations, obtained by the substitution of $x = 1, 2, \dots$ into this formula. Therefore the assertion of the theorem is equivalent to the unique solvability of the linear system

$$\lambda(a_1, a_2, \dots)^t = (h(1), h(2), \dots)^t.$$

Here the upper index t denotes the transposition, the lines and the columns of the matrix λ are indexed by the numbers $i, j = 1, 2, \dots$, and

$$\lambda_{ij} = [j/i].$$

The matrix λ is invertible, because it is an upper triangular matrix with unities on the diagonal. □

Let $h(1), h(2), \dots$ be a sequence. We define the difference derivation Δh for $n \geqslant 1$ as

$$(\Delta h)(n) = h(n) - h(n-1), \tag{3}$$

where one has to use 0 as $h(0)$ for $n = 1$.

Proposition 1.1.2. *Let $h(x) = a_1[x] + a_2[x/2] + \cdots$ Then*

$$(\Delta h)(n) = \sum_{d|n} a_d \tag{4}$$

and

$$a_n = \sum_{d|n} \mu(n/d)(\Delta h)(d). \tag{5}$$

Proof. In fact, $(\Delta h)(n) = h(n) - h(n-1) = \sum a_d([n/d] - [(n-1)/d]$. However

$$[n/d] - [(n-1)/d] = \begin{cases} 1 & \text{if} \quad d|n; \\ 0 & \text{else.} \end{cases}$$

Therefore $\sum a_d([n/d] - [(n-1)/d]) = \sum\limits_{d|n} a_d$ and (4) is proven. It implies (5) by means of the Möbius inversion formula. □

1.2. Counting the number of divisors. Suppose that K is a field, $\mathbb{Q} \subset K$ and K is finite over $\mathbb{Q}$. Let M be a monoid of the effective divisors of the ring $\mathcal{O}_K$ and let $N = \{1, 2, \dots\}$ be a monoid of the effective divisors of $\mathbb{Z}$.

In this situation, there is the norm map

$$\mathrm{Nrm} : M \to N.$$

This norm map is defined by the formula $\mathrm{Nrm}(m) = \operatorname{card} \mathcal{O}_K/I$, where I is the ideal in the ring $\mathcal{O}_K$, corresponding to the divisor m.

1.2.1. General context for counting functions. Suppose that there are a set S and an Abelian group A. Consider a diagram of sets

$$\begin{array}{ccc} & S & \\ {\scriptstyle \nu}\swarrow & & \searrow{\scriptstyle \phi} \\ N & & A\,, \end{array} \tag{6}$$

where the set $\nu^{-1}(n)$ is finite for any $n \in N$.

For any real $e \geqslant 0$ set

$$h(e) = \sum_{\nu(m) \leqslant e} \phi(m). \tag{7}$$

Since $h(e)$ is an entier-function, Theorem 1.1.1 says that for certain coefficients b_n the equality

$$h(e) = b_1 \left[\frac{e}{1}\right] + b_2 \left[\frac{e}{2}\right] + b_3 \left[\frac{e}{3}\right] + \cdots$$

holds. This formula becomes interesting, if the coefficients b_n's are equipped with an intentional interpretation. One of such cases is given futher in Theorem 1.2.2.

Below we consider interesting for us counting functions just in this context. Namely we take Nrm as ν in the diagram (6), the additive group of $\mathbb{C}$ as A, and the constant function 1 as ϕ.

As a particular case of definition (7) for any real $e \geqslant 0$ we set

$$h(e) = \{m \in M \,|\, \mathrm{Nrm}\, m \leqslant e\}. \tag{8}$$

Theorem 1.2.2. *Let $\zeta_K(s)$ be the Dirichlet ζ-function, associated to the field K. In particular, $\zeta_{\mathbb{Q}}(s)$ is the Riemann ζ-function. Let a_n's be the coefficients of the Dirichlet series for the function $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$. In other words, let*

$$\zeta_K(s)/\zeta_{\mathbb{Q}}(s) = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \cdots .$$

Then for any real $e \geqslant 0$

$$h(e) = a_1 \left[\frac{e}{1}\right] + a_2 \left[\frac{e}{2}\right] + a_3 \left[\frac{e}{3}\right] + \cdots . \tag{9}$$

Proof. It is clear that $h(e)$ is an entier-function. Therefore, Theorem 1.1.1 says that the identity

$$h(e) = b_1 \left[\frac{e}{1}\right] + b_2 \left[\frac{e}{2}\right] + b_3 \left[\frac{e}{3}\right] + \cdots$$

holds for certain coefficients b_n's. We have to show that $b_n = a_n$ for $n = 1, 2, \ldots$. Set

$$r(n) = \mathrm{card}\, \mathrm{Nrm}^{-1}(n).$$

Definitions (3) and (8) imply immediately that

$$r(n) = (\Delta h)(n)$$

for $n = 1, 2, \ldots$. So, Proposition 1.1.2 implies, that

$$b_n = \sum_{d|n} \mu(n/d) r(d).$$

It remains to verify, that the coefficients of the Dirichlet series for $\zeta_K/\zeta_{\mathbb{Q}}$ are given by the same formula. By definition $\zeta_K(s) = \sum\limits_{m \in M} (\mathrm{Nrm}\, m)^{-s}$. Collecting terms shows that

$$\zeta_K(s) = \sum_{n \in N} r(n) n^{-s}.$$

The multiplication of the both sides of the equality by the corresponding parts of the equality $\zeta_{\mathbb{Q}}^{-1}(s) = \sum \mu(n)n^{-s}$ shows that $a_n = \sum\limits_{d|n} \mu(n/d)r(d)$.

□

§2. Imaginary quadratic fields

Below K is an imaginary quadratic field, D is the discriminant of K, χ is the Dirichlet character, corresponding to K.

2.1. Counting the number of integral points. We start with a specialization of the above formula (9) for the number of divisors.

Theorem 2.1.1. *Suppose K is an imaginary quadratic field. Then*

$$h(e) = \chi(1)\left[\frac{e}{1}\right] + \chi(2)\left[\frac{e}{2}\right] + \chi(3)\left[\frac{e}{3}\right] + \cdots$$

for any real $e \geqslant 0$.

Proof. This assertion is a particular case of Theorem 1.2.2. To see this take into account the well-known identity $\zeta_K(s) = \zeta_{\mathbb{Q}}(s)L_\chi(s)$, where $L_\chi(s) = \chi(1)\cdot 1^{-s} + \chi(2)2^{-s} + \chi(3)3^{-s} + \cdots$ is the Dirichlet series associated with χ. □

Suppose additionally that the ring $\mathcal{O}_K$ is a unique factorization domain, i.e., that

$$\operatorname{Pic}\mathcal{O}_K = 1.$$

For any real $e \geqslant 0$ set

$$H^0(e) = \{s \in \mathcal{O}_K \,|\, \operatorname{Nrm}(s) \leqslant e\}.$$

Consider the set

$$F = \{0\} \cup \mu(K),$$

where $\mu(K)$ is the group of all roots of unity contained in K. This set is a monoid relatively the multiplication. In other words,

$$F = \mathbb{F}_{1^m} \quad \text{with} \quad m = \operatorname{card}\mu(K).$$

The monoid F acts on $\mathcal{O}_K$ by multiplication and the subset $H^0(e) \subset \mathcal{O}_K$ is stable under this action. Thus $H^0(e)$ becomes an F-module. It is clear that this module is free. Set

$$h^0(e) = \operatorname{rk}_F H^0(e) = \frac{\operatorname{card} H^0(e) - 1}{m}.$$

Theorem 2.1.2. *Let K be an imaginary quadratic extension of $\mathbb{Q}$, $\operatorname{Pic}\mathcal{O}_K = 1$, and χ be the Dirichlet character, corresponding to K. Then for any real $e \geqslant 0$*

$$h^0(e) = \chi(1)\left[\frac{e}{1}\right] + \chi(2)\left[\frac{e}{2}\right] + \chi(3)\left[\frac{e}{3}\right] + \cdots . \tag{10}$$

Proof. This theorem follows immediately from Theorem 2.1.1 and from the following equality

$$e(n) = md(n).$$

Here $n \in N$, $d(n)$ is the number of the effective divisors in $\mathcal{O}_K$ with the norm n, and $e(n)$ is the number of the elements in $\mathcal{O}_K$ with the norm n. The equality is obvious in view of the unique factorization property of $\mathcal{O}_K$. □

It is well known that there are exactly nine imaginary quadratic fields with the unique factorization property for $\mathcal{O}_K$. They are the fields $\mathbb{Q}(\sqrt{-d})$ with $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. Thus, Theorem 2.1.2 gives nine formulas.

It makes sense to compare (10) with the Dirichlet formula for $L_\chi(1)$. In the general case,

$$L_\chi(1) = \frac{2\pi h}{m\sqrt{|D|}},$$

where $h = \operatorname{card}(\operatorname{Pic}\mathcal{O}_K)$. In the case of K with $\operatorname{Pic}\mathcal{O}_K = 1$, we get

$$\frac{2\pi}{m\sqrt{|D|}} = \chi(1)\frac{1}{1} + \chi(2)\frac{1}{2} + \chi(3)\frac{1}{3} + \cdots . \tag{11}$$

This relation can be considered as a limit case of (10).

2.2. Examples. Here we write down some of obtained relations quite explicitly.

2.2.1. $K = \mathbb{Q}(\sqrt{-1})$. In this case $\mathcal{O}_K = \mathbb{Z}[i]$ with $i = \sqrt{-1}$, $D = 4$, and

$$\chi(n) = \begin{cases} 1 & \text{if} \quad n \equiv 1 \mod 4; \\ -1 & \text{if} \quad n \equiv -1 \mod 4; \\ 0 & \text{if} \quad n \text{ is even.} \end{cases}$$

Take the pair $(1, i)$ as a basis for the lattice $\mathcal{O}_K$. This choice identifies $\mathcal{O}_K$ with $\mathbb{Z}^2$. After this identification we have

$$H^0(e) = \{(x, y) \in \mathbb{Z}^2 | x^2 + y^2 \leqslant e\}.$$

Here $\mu(K) = \{\pm 1, \pm i\}$, $m = 4$ and $H^0(e)$ is an F-module with $F = \mathbb{F}_{1^4}$. Theorem 2.1.2 gives the relation

$$\operatorname{rk}_F H^0(e) = \left[\frac{e}{1}\right] - \left[\frac{e}{3}\right] + \left[\frac{e}{5}\right] - \left[\frac{e}{7}\right] + \cdots .$$

This is just the formula from the papers of Eisenstein and of Ehrhart (see Introduction). As the limit case we get the well known Leibnitz formula

$$\frac{\pi}{4} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots .$$

2.2.2. $K = \mathbb{Q}(\sqrt{-3})$. In this case $\mathcal{O}_K = \mathbb{Z}[\rho]$ with $\rho = \sqrt[6]{1}$, $\sqrt{-3} = 2\rho - 1$, $D = 3$, and

$$\chi(n) = \begin{cases} 1 & \text{if} \quad n \equiv 1 \mod 3; \\ -1 & \text{if} \quad n \equiv -1 \mod 3; \\ 0 & \text{if} \quad n \equiv 0 \mod 3. \end{cases}$$

Take the pair $(1, \rho)$ as a basis for the lattice $\mathcal{O}_K$. This choice identifies $\mathcal{O}_K$ with $\mathbb{Z}^2$. After this identification we get

$$H^0(e) = \left\{(x, y) \in \mathbb{Z}^2 | x^2 + xy + y^2 \leqslant e\right\}.$$

Here $\mu(K) = \{\pm 1, \pm\rho, \pm\rho^2\}$, $m = 6$, and $H^0(e)$ is a an F-module with $F = \mathbb{F}_{1^6}$. Theorem 2.1.2 gives the relation

$$\operatorname{rk}_F H^0(e) = \left[\frac{e}{1}\right] - \left[\frac{e}{2}\right] + \left[\frac{e}{4}\right] - \left[\frac{e}{5}\right] + \cdots .$$

As the limit case we get the formula $\pi/(3\sqrt{3}) = 1 - 1/2 + 1/4 - 1/5 + \cdots$.

2.2.3. $K = \mathbb{Q}(\sqrt{-7})$. In this case, $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-7})/2$, $D = 7$, and

$$\chi(n) = \begin{cases} 1 & \text{if} \quad n \equiv 1, 2, 4 \mod 7; \\ -1 & \text{if} \quad n \equiv 3, 5, 6 \mod 7; \\ 0 & \text{if} \quad n \equiv 0 \mod 7. \end{cases}$$

Take the pair $(1, \omega)$ as a basis for the lattice $\mathcal{O}_K$. This choice identifies $\mathcal{O}_K$ with $\mathbb{Z}^2$. After this identification we get

$$H^0(e) = \left\{(x, y) \in \mathbb{Z}^2 | x^2 + xy + 2y^2 \leqslant e\right\}.$$

Here $\mu(K) = \{\pm 1\}$, $m = 2$, and $H^0(e)$ is an F-module with $F = \mathbb{F}_{1^2}$. Theorem 2.1.2 gives the relation

$$\operatorname{rk}_F H^0(e) = \left[\frac{e}{1}\right] + \left[\frac{e}{2}\right] - \left[\frac{e}{3}\right] + \left[\frac{e}{4}\right] - \left[\frac{e}{5}\right] - \left[\frac{e}{6}\right] + \left[\frac{e}{8}\right] + \cdots .$$

As the limit case, we get the formula

$$\pi/\sqrt{7} = 1 + 1/2 - 1/3 + 1/4 - 1/5 - 1/6 + \cdots .$$

§3. Conclusion

Here is a quotation from the paper [3], related to the considered subject.

"Es giebt Figuren, für welche man durch einfache Formeln die Anzahl der innerhalb derselben liegenden Gitterpuncte bestimmen kann. Stellt man sich z. B. einen Kreis vor, dessen Mittelpunct im Anfangspuncte der Coordinaten liegt und dessen Radius $\sqrt{m}$ ist, so wird die Anzahl der Gitterpuncte S, welche dieser Kreis umschiefst, die aus den Axen liegenden mitgerechnet, durch folgende Formel gegeben

$$S = 1 + 4\left(E(m) - E\Big(\frac{1}{3}m\Big) + E\Big(\frac{1}{5}m\Big) - \text{ etc.}\right),$$

bis die Reihe von selbst abbricht. Wie leicht zu sehen, drückt diese Gleichung eine Relation zwischen der Anzahl der Gitterpuncte enes **Kreises** und der Anzahl der Gitterpuncte eines zwischen zwei **Hyperbeln** eingeschlossenen Segments aus. Setzt man in der Formel

$$\frac{1}{m}S = \frac{1}{m} + 4\left(\frac{1}{m}E(m) - \frac{1}{m}E\Big(\frac{1}{3}m\Big) + \frac{1}{m}E\Big(\frac{1}{5}m\Big) - \text{ etc.}\right),$$

$m = \infty$, so verwandelt sich die linke Seite in π, während die rechte Seite in $4(1 - 1/3 + 1/5 - \text{etc})$ übergeht, so dass man hier die **Leibnitz**'she Formel für π erhält. Es giebt ähnliche Formeln für die Anzhal der Gitterpuncte eines Systems von Ellipsen oder Hyperbelsectoren; auch finden ähnliche Relationen im Raume und in Fällen mit mehr als 3 Dimensionen Statt. Wir werden auf diesen wichtigen Gegenstand, der aufs genauste mit den Eigenschaften der höheren Formen zusammenhängt, bei einer andern Gelegenheit zurückkommen."

We see that significant generalizations of formula (1) were planned. Of course, I do not think that I can guess the thoughts of Eisenstein completely, but some of such generalizations can be supposed and are related to the genus theory for quadratic forms and to the Siegel–Weil formulas. On the other hand, it would be interesting to match explicit finite formulas with finite type compactifications of arithmetic schemes.

References

1. E. Ehrhart, *Sur une problème de géométrie diophantine linéaire.* — J. für die reine und angew. Math. **226** (1967), 1-29.
2. S. E. Cappell, J. L. Shaneson, *Genera of algebraic varieties and counting of lattice points.* — Bulletin (New Series) Amer. Math. Soc. **30**, No. 1, Jan. (1994).
3. G. Eisenstein, *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste.* — J. für die reine und angew. Math. **28** (1844), 246–248.

Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
Фонтанка 27,
191023 Санкт-Петербург,
Россия
E-mail: smirnov@pdmi.ras.ru

Поступило 20 сентября 2012 г.