INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus
Mathématique

Roland Bacher

Euclid meets Popeye: The Euclidean Algorithm for 2 × 2 Matrices

Volume 361 (2023), p. 889-895

Published online: 18 July 2023

https://doi.org/10.5802/crmath.451

CENTRE MERSENNE

Les Comptes Rendus. Mathématique *sont membres du*
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org
e-ISSN : 1778-3569

Comptes Rendus Mathématique
2023, Vol. 361, p. 889-895
https://doi.org/10.5802/crmath.451

Number theory / *Théorie des nombres*

Euclid meets Popeye: The Euclidean Algorithm for 2 × 2 Matrices

Roland Bacher [a]

[a] Univ. Grenoble Alpes, Institut Fourier, 38000 Grenoble, France
E-mail: roland.bacher@univ-grenoble-alpes.fr

Abstract. An analogue of the Euclidean algorithm for square matrices of size 2 with integral non-negative entries and positive determinant n defines a finite set $\mathscr{R}(n)$ of Euclid-reduced matrices corresponding to elements of $\{(a,b,c,d)\in\mathbb{N}^4 \mid n=ab-cd,\ 0\le c,d<a,b\}$. With Popeye's help[1] on the use of sails of lattices we show that $\mathscr{R}(n)$ contains $\sum_{d|n,\ d^2\ge n}\left(d+1-\frac{n}{d}\right)$ elements.

2020 Mathematics Subject Classification. 11A05, 11H06, 11J70.

Manuscript received 29 October 2022, revised 7 December 2022, accepted 29 November 2022.

1. Introduction

We let $\mathbb{N}=\{0,1,2,\ldots\}$ denote the set of all non-negative integers and we let $\mathscr{P}=\left\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\,\middle|\, a,b,c,d\in\mathbb{N},\ ad-bc>0\right\}$ denote the set of all square matrices of size 2 with entries in $\mathbb{N}$ and positive determinant. The subset of matrices of determinant n in $\mathscr{P}$ is written as $\mathscr{P}(n)$.

An *elementary reduction* of a matrix M is a matrix which belongs to the set $\{EM, E^tM, ME, ME^t\}$ where $E=\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right)$. Elementary reductions of M subtract a row/column from the other row/column of M.

A matrix M in $\mathscr{P}$ is *Euclid-reduced* if and only if $\mathscr{P}$ contains no elementary reduction of M. Equivalently, $M=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ in $\mathscr{P}$ is Euclid-reduced if $\min(a,d)>\max(b,c)$.

Euclid-reduced matrices are sort of a 2-dimensional analogue of the greatest common divisor computed by Euclid's algorithm: Given two natural integers A,B, replace $\max(A,B)$ by $\max(A,B)-\min(A,B)$ until $AB=0$. Here we do the same with rows and columns of 2×2-matrices and we stop if we get negative entries.

We let $\mathscr{R}$ denote the subset of Euclid-reduced matrices in $\mathscr{P}$ and we let $\mathscr{R}(n)=\mathscr{R}\cap\mathscr{P}(n)$ denote the subset of $\mathscr{R}$ corresponding to Euclid-reduced matrices of determinant n.

The main result of this paper describes the number $\sharp(\mathscr{R}(n))$ of elements in the set $\mathscr{R}(n)$ of Euclid-reduced matrices of determinant n:

[1] Acknowledged by his appearance in the title (he refused co-authorship on the flimsy pretext of a weak contribution due to a poor spinach-harvest).

Theorem 1. *The number of elements* (a,b,c,d) *in* $\mathbb{N}^4$ *such that* $n = ab - cd$ *and* $\min(a,b) > \max(c,d)$ *is given by*

$$\sum_{d|n,\ d^2 \geq n} \left(d + 1 - \frac{n}{d}\right). \tag{1}$$

The map $(a,b,c,d) \longmapsto \left(\begin{smallmatrix} a & c \\ d & b \end{smallmatrix}\right)$ *is a one-to-one correspondence between such solutions and elements in the set* $\mathscr{R}(n)$ *of Euclid-reduced matrices having determinant* n.

Remark 2. The finite set occuring in Theorem 1 has two natural descriptions: In terms of matrices in $\mathscr{R}(n)$ or as solutions of the Diophantine equation occuring at the beginning of Theorem 1. Natural notations for both descriptions are unfortunately somewhat incompatible. We have opted for the Diophantine viewpoint in Theorem 1 and in the sequel. This makes the coeffients of the associated matrices a bit awkward.

All summands occurring in (1) are positive and the last summand (corresponding to the trivial divisor $d = n$ of n) equals n. We have therefore $\sharp(\mathscr{R}(n)) \geq n$ with equality for $n > 1$ if and only if n is a prime number. Our proof of Theorem 1 shows that solutions associated with a prime number p are in one-to-one correspondence with the p sublattices of index p in $\mathbb{Z}^2$ which do not contain the vector $(1,1)$.

Similarly, $\sharp(\mathscr{R}(n)) = n+1$ if and only if $n = p^2$ is the square of prime number p.

Cardinalities of the sets $\mathscr{R}(1), \mathscr{R}(2), \ldots$ are given by the integer sequence

$$1,2,3,5,5,8,7,11,10,14,11,19,13,20,18,24,17,30,19,31,\ldots$$

defining sequence A357259 of the Online-Encyclopedia of Integer Sequences [4].

Klein's Vierergruppe $\mathbb{V}$ (underlying the 2-dimensional vector space over the field of two elements) acts on solutions (a,b,c,d) by permuting the first two entries, the last two entries or the first two and the last two entries. We let $\mathscr{O} = \{(a,b,c,d),(b,a,c,d),(a,b,d,c),(b,a,d,c)\}$ denote the orbit of a solution (a,b,c,d) under the action of $\mathbb{V}$. The following lists give lexicographically largest representants of all orbits for the sets of solutions associated with the prime numbers 11, 13 and 17:

a	b	c	d	$\sharp(\mathscr{O})$
11	1	0	0	2
6	2	1	1	2
4	3	1	1	2
5	3	2	2	2
5	4	3	3	2
6	6	5	5	1
				11

a	b	c	d	$\sharp(\mathscr{O})$
13	1	0	0	2
7	2	1	1	2
5	3	2	1	4
4	4	3	1	2
5	5	4	3	2
7	7	6	6	1
				13

a	b	c	d	$\sharp(\mathscr{O})$
17	1	0	0	2
9	2	1	1	2
6	3	1	1	2
5	4	3	1	4
7	3	2	2	2
5	5	4	2	2
7	6	5	5	2
9	9	8	8	1
				17

For $n = 12, 14, 15$ we get

$$\begin{aligned}
\sharp(\mathscr{R}_{12}) &= (4+1-3)+(6+1-2)+(12+1-1) = 19, \\
\sharp(\mathscr{R}_{14}) &= (7+1-2)+(14+1-1) = 20, \\
\sharp(\mathscr{R}_{15}) &= (5+1-3)+(15+1-1) = 18.
\end{aligned}$$

The associated lexicographically largest solutions in orbits are given by

a	b	c	d	$\sharp(\mathscr{O})$
12	1	0	0	2
6	2	0	0	2
6	2	1	0	4
4	3	0	0	2
4	3	1	0	4
4	3	2	0	4
4	4	2	2	1
				19

a	b	c	d	$\sharp(\mathscr{O})$
14	1	0	0	2
7	2	0	0	2
7	2	1	0	4
5	3	1	1	2
4	4	2	1	2
6	3	2	2	2
5	4	3	2	4
6	5	4	4	2
				20

a	b	c	d	$\sharp(\mathscr{O})$
15	1	0	0	2
5	3	0	0	2
5	3	1	0	4
5	3	2	0	4
8	2	1	1	2
4	4	1	1	1
6	4	3	3	2
8	8	7	7	1
				18

It is perhaps worthwhile to note that non-negative integral solutions of $n = ab + cd$ with $\min(a,b) > \max(c,d)$ are also interesting: For $n = p$ an odd prime there are $(p+1)/2$ solutions. If p is congruent to 1 modulo 4, the number $(p+1)/2$ of such solutions is odd and the action of Klein's Vierergruppe has a fixed point expressing p as a sum of two squares, see [2].

The sequel of this paper is organized as follows:

Section 2 uses Moebius inversion in order to obtain the number of elements with coprime entries in $\mathscr{R}(n)$.

Section 3 recalls a well-known formula for the number of sublattices of index n in $\mathbb{Z}^2$. We give an elementary proof.

Unless stated otherwise, a lattice is always a discrete subgroup isomorphic to $\mathbb{Z}^2$ of the Cartesian coordinate plane $\mathbb{R}^2$ considered as a vector space.

Section 4 describes the sail of a lattice Λ contained in the Cartesian coordinate plane $\mathbb{R}^2$.

Section 5 is devoted to the proof of Theorem 1.

Section 6 contains a few complements: An elementary proof for finiteness of the set $\mathscr{R}(n)$, a short discussion on matrices of larger size or of determinant 0. It ends with the description of a perhaps interesting variation over the ring of Gaußian integers.

2. Coprime solutions

We let $\mathscr{R}'(n)$ denote the subset of $\mathscr{R}(n)$ containing all Euclid-reduced matrices with coprime entries. Dividing all entries of matrices in $\mathscr{R}(n)$ by their greatest common divisor, we get a bijection between $\mathscr{R}(n)$ and the union $\bigcup_{d,d^2|n}\mathscr{R}'(n/d^2)$ showing the identity $\sharp(\mathscr{R}(n)) = \sum_{d,\ d^2|n}\sharp(\mathscr{R}'(n/d^2))$. Moebius inversion of this identity yields now the formula

$$\sharp(\mathscr{R}'(n)) = \sum_{d^2|n}\mu(d)\sharp(\mathscr{R}(n/d^2)) \tag{2}$$

(where the Moebius function μ is defined by $\mu(n) = (-1)^e$ if n is a product of e distinct primes and $\mu(n) = 0$ if n has a non-trivial square-divisor).

Observe that $\mathscr{R}'(n) = \mathscr{R}(n)$ if and only if $\mu(n) \neq 0$.

Cardinalities of $\mathscr{R}'(1), \mathscr{R}'(2), \ldots$ yield the integer sequence

$$1,2,3,4,5,8,7,9,9,14,11,16,13,20,18,19,17,28,19,26,\ldots$$

defining A357260 of [4].

3. Sublattices of finite index in $\mathbb{Z}^2$

The following well-known result (see Remark 4 below) is a crucial ingredient for proving Theorem 1. We give an elementary proof for the comfort of the reader.

Theorem 3. *The lattice $\mathbb{Z}^2$ has $\sum_{d,d|n} d$ different sublattices of index n.*

Proof. Let Λ be a sublattice of index n in $\mathbb{Z}^2$. The order d of $(1,0)$ in the finite quotient group $\mathbb{Z}^2/\Lambda$ is therefore a divisor of n and we have $\Lambda \cap \mathbb{Z}(1,0) = \mathbb{Z}(d,0)$. Hence there exists a unique element a in $\{0,\dots,d-1\}$ such that $\Lambda = \mathbb{Z}(d,0) + \mathbb{Z}(a,n/d)$. This shows that the lattice $\mathbb{Z}^2$ has d different sublattices of index n intersecting $\mathbb{Z}(1,0)$ in $\mathbb{Z}(d,0)$ for every divisor d of n. Summing over all divisors yields the result. $\square$

Remark 4. More generally, the number of sublattices of index n in $\mathbb{Z}^d$ is given by

$$\prod_{p|n} \binom{e_p+d-1}{d-1}_p \tag{3}$$

(see e.g. [3] or [5]) where $\prod_{p|n} p^{e_p} = n$ is the factorization of n into prime-powers and where

$$\binom{e_p+d-1}{d-1}_p = \prod_{j=1}^{d-1} \frac{p^{e_p+j}-1}{p^j-1}$$

is the evaluation of the q-binomial

$$\begin{bmatrix} e_p+d-1 \\ d-1 \end{bmatrix}_q = \frac{[e_p+d-1]_q!}{[e_p]_q!\,[d-1]_q!}$$

(with $[k]_q! = \prod_{j=1}^k \frac{q^j-1}{q-1}$) at the prime-divisor p of n.

Formula (3) boils of course down to $\sum_{k,k|n} k$ if $d = 2$.

4. The sail of a lattice

Sails of lattices in $\mathbb{R}^d$, introduced and studied by V. Arnold, cf. e.g. [1], are a possible generalization of continued fraction expansions to higher dimension. We define and discuss here only the case $d = 2$ corresponding to ordinary continued fractions.

We let $Q_{\mathrm{I}} = \{(x,y) \mid 0 \le x, y\}$ denote the closed first quadrant containing all points with non-negative coordinates of the Cartesian coordinate plane $\mathbb{R}^2$.

The *sail* $\mathscr{S} = \mathscr{S}(\Lambda)$ of a lattice $\Lambda \subset \mathbb{R}^2$ is the boundary with respect to the closed first quadrant Q_{I} of the convex hull of all non-zero elements $(\Lambda \setminus (0,0)) \cap Q_{\mathrm{I}}$ of Λ contained in Q_{I}.

The sail $\mathscr{S}$ of a lattice Λ is a piecewise linear path with vertices in Λ which intersects every 1-dimensional subspace of finite positive slope in a unique point. Affine pieces of sails have finite negative slopes. Any affine line intersecting a sail in two points has therefore finite negative slope.

Each coordinate axis intersects a sail either in a unique point (this happens if and only if the coordinate axis contains infinitely many points of the underlying lattice Λ) or is an asymptote of the sail (if Λ contains no non-zero elements of the coordinate axis).

The sail $\mathscr{S}(\Lambda)$ of a sublattice Λ of index n in $\mathbb{Z}^2$ is always bounded with endpoints $(\alpha_x,0), (0,\omega_y)$ for two divisors α_x and ω_y of n such that $\alpha_x\omega_y \ge n$.

Two distinct lattice elements $u, v \in \Lambda$ on the sail $S = \mathscr{S}(\Lambda)$ of a lattice Λ are *consecutive* if the open segment joining u and v is contained in $\mathscr{S} \setminus \Lambda$.

Lemma 5. *Two distinct lattice elements u, v on the sail $\mathscr{S}(\Lambda) \cap \Lambda$ of a lattice Λ generate Λ if and only if they are consecutive.*

Proof. Since all non-zero lattice points in Q_{I} belong to $\mathscr{S}$ or to the unbounded convex region of $Q_{\mathrm{I}} \setminus \mathscr{S}$, the closed triangle $\Delta = \Delta(u,v)$ with vertices $(0,0), u, v$ contains no other element of Λ if and only if u and v are consecutive.

Pairs of consecutive points u, v generate Λ since $\Delta \cup (-\Delta)$ is a fundamental domain for the lattice spanned by u and v. $\square$

A *sailbasis* of a lattice Λ is a basis of Λ consisting of two consecutive elements in the sail $\mathscr{S}$ of Λ. Every lattice has a sailbasis.

Two linearly independent elements u, v in the first quadrant Q_{I} form a sailbasis of the lattice $\mathbb{Z}u + \mathbb{Z}v$ generated by u and v if and only if the affine line containing u and v has finite negative slope.

Remark 6. Sails are generalisations of continued fractions: Given a real number θ, vertices of the sail for the lattice $e^{-i\arctan(\theta)}(\mathbb{Z} + i\mathbb{Z})$ correspond essentially to convergents of θ, see for example [1].

5. Proof of Theorem 1

A sailbasis u, v of a lattice is *central* if the open segment joining u and v intersects the diagonal line $x = y$. The two elements of a central sailbasis belong therefore to different connected components of $\mathbb{R}^2 \setminus \mathbb{R}(1,1)$. Every lattice has at most one central sailbasis.

A lattice Λ is *bad* if it has no central sailbasis. Equivalently, a lattice is bad if its sail $\mathscr{S}$ intersects the set $\Lambda \cap \mathbb{R}(1,1)$ of diagonal lattice-elements.

A sailbasis u, v of a bad lattice $\Lambda = \mathbb{Z}u + \mathbb{Z}v$ is *normalized* if u in $\mathbb{R}(1,1)$ is a diagonal element and v belongs to the open halfplane $\{(x, y) \mid x > y\}$ below the diagonal line. Lemma 5 shows that a bad lattice Λ has a unique normalized sailbasis given by $u = \mathscr{S} \cap \mathbb{R}(1,1)$ and by the unique consecutive element v in $\mathscr{S} \cap \Lambda$ of u which lies below the diagonal line $x = y$.

Proposition 7. *The lattice $\mathbb{Z}^2$ contains*

$$\sum_{d,\ d^2<n,\ d|n} d + \sum_{d,\ d^2\geq n,\ d|n} (n/d - 1)$$

bad sublattices of index n.

Proof. Bad lattices are in one-to-one correspondence with their normalized sailbases. We count them by adapting the proof of Theorem 3.

Let $u = (d, d)$ in $\Lambda \cap \mathscr{S}$ be the diagonal element of a normalized sailbasis u, v generating a bad sublattice $\Lambda = \mathbb{Z}u + \mathbb{Z}v$ of index n in $\mathbb{Z}^2$. The image of the element $(1,1)$ in the quotient group $\mathbb{Z}^2/\Lambda$ is therefore of order d dividing n. Since u, v is a sailbasis, the coefficients v_x, v_y of the remaining basis element $v = (v_x, v_y)$ satisfy the inequalities $0 \leq v_y < d < v_x$. Since $\Lambda = \mathbb{Z}u + \mathbb{Z}v$ is a sublattice of index n in $\mathbb{Z}^2$, the element v of $\mathbb{N}^2$ belongs to the line $(n/d, 0) + \mathbb{R}(1,1)$. We have therefore $v = (n/d + a, a)$ for a suitable non-negative integer a.

If $d < \sqrt{n}$, the trivial inequalities $d < n/d \leq n/d + a = v_x$ imply $v_x > d$ for all choices of a in $\mathbb{N}$. The inequality $v_y < d$ implies that $a = v_y$ belongs to the set $\{0, 1, 2, \ldots, d-1\}$ of the d smallest non-negative integers. For every divisor $d < \sqrt{n}$ there are therefore d bad sublattices of index n containing (d, d) in their sail.

If d is a divisor of n such that $d \geq \sqrt{n}$, the inequality $d < v_x = n/d + a$ implies $a \geq d - n/d + 1 \geq 0$. We have also $a = v_y < d$. This shows that a belongs to the set $\{d - n/d + 1, d - n/d + 2, \ldots, d - 1\}$ containing $n/d - 1$ elements.

Summing over all contributions given by divisors of n ends the proof. $\square$

Proof of Theorem 1. Solutions of $ab - cd = n$ with $\min(a, b) > \max(c, d)$ are in one-to-one correspondence with central sailbases $(a, d), (d, b)$ generating sublattices of index n in $\mathbb{Z}^2$. The number of elements in $\mathscr{R}(n)$ is therefore obtained by subtracting the number $\sum_{d,\ d^2<n,\ d|n} d + \sum_{d,\ d^2\geq n,\ d|n} (n/d - 1)$ of bad lattices of index n in $\mathbb{Z}^2$ given by Proposition 7 from the total number $\sum_{d, d|n} d$ of lattices of index n in $\mathbb{Z}^2$ given by Theorem 3. Simplification yields the result. $\square$

6. Complements

6.1. *Finiteness*

We discuss in this Section a few finiteness properties of Euclid-reduced sets.

First, we give an elementary proof of finiteness for the number of Euclid-reduced matrices in $\mathscr{P}$ of fixed positive determinant which does not make use of Theorem 1.

We consider then briefly the case of square matrices of size larger than 2 and of square matrices of size two with determinant 0.

6.2. *An easy bound on entries of Euclid-reduced matrices*

Proposition 8. *Matrices in $\mathscr{R}(n)$ involve only entries in $\{0, 1, \ldots, n\}$.*

Corollary 9. *There are at most $(n+1)^4$ matrices in the set $\mathscr{R}(n)$ of Euclid-reduced matrices of determinant n.*

We leave the obvious proof of the Corollary to the reader.

Proof of Proposition 8. Let $n = ab - cd$ with $\min(a, b) > \max(c, d)$ be a solution corresponding to the Euclid-reduced matrix $\left(\begin{smallmatrix} a & c \\ d & b \end{smallmatrix}\right)$ with $\max(a, b)$ maximal among entries occurring in elements of $\mathscr{R}(1), \ldots, \mathscr{R}(n)$. Up to exchanging a and b we can suppose that $a \geq b$. Since $n = ab - cd \geq ab - (b-1)^2 > 0$ we can assume $c = d = b - 1$. Restricting $ax - (x-1)^2$ to x in $[1, \ldots, a]$ we can furthermore assume either $x = 1$ or $x = a$. In the first case we get $n \geq a \cdot 1 - 0^2 = a$ and in the second case we get $n \geq a^2 - (a-1)^2 = 2a - 1$ showing the inequality $\max(a, b) = a \leq n$ in both cases. □

6.3. *Finiteness for size larger than two*

Euclidean reduction for square matrices of size 2 has an obvious generalization to square matrices of arbitrary size with coefficients in $\mathbb{N}$: Subtract (if possible) a different row or column from a given row or column. This leads in general to infinite sets of matrices of given positive determinant which have no further reductions: The matrix $\left(\begin{smallmatrix} 4+x & 2+x & 1+x \\ x & 1+x & 3+x \\ 1+x & 1+x & 2+x \end{smallmatrix}\right)$ has determinant 1 and is "Euclid-reduced" for any natural integer x.

6.4. *Finiteness for determinant zero*

All square matrices of size two with (at least) three zero entries and an arbitrary entry in $\mathbb{N}$ are Euclid-reduced and every Euclid-reduced matrix with determinant 0 and entries in $\mathbb{N}$ is of this form: If a matrix M (of square size two with entries in $\mathbb{N}$ has determinant 0 then its rows (or columns) are linearly dependent. Subtracting the smaller row iteratively from the larger one we end up with a matrix having a zero-row. Working with columns we get finally a matrix having a unique non-zero entry.

Requiring the entries of such a matrix to have a given non-zero greatest divisor ensures uniqueness up to the location of the non-zero entry. There are therefore exactly four Euclid-reduced matrices (of square size 2) with determinant 0 and greatest common divisor of entries a given positive integer $d \geq 1$.

6.5. *Gaußian integers*

We discuss briefly an analogue of $\mathscr{R}(n)$ over the ring of Gaußian integers (the case of integers in an imaginary quadratic number field is probably similar).

Given a non-zero Gaußian integer z, we define the set $\mathscr{S}(z)$ containing all solutions of $ab+cd=z$ satisfying $\min(|a|,|b|)>\max(|c|,|d|)$ with a,b,c,d in the set $\mathbb{Z}[i]$ of Gaußian integers.

The two identities

$$2m+1=(2n+(2n^2-m-1)i)(2n-(2n^2-m-1)i)-(2n^2-m)^2$$

and

$$2m=(2n+1+(2n^2+2n-m)i)(2n+1-(2n^2+2n-m)i)-(2n^2+2n-m+1)^2$$

show that the sets $\mathscr{S}(z)$ are always infinite for $z\in\mathbb{Z}\setminus\{0\}$.

More generally, $\mathscr{S}(z)$ is infinite for every Gaußian integer z of the form $z=nu^2$ for n in $\mathbb{N}\setminus\{0\}$ a sum of two squares (i.e. containing no odd power of a prime congruent to 3 modulo 4 in its prime-factorization) and for $u\in\mathbb{Z}[i]\setminus\{0\}$ an arbitrary non-zero Gaußian integer.

Solutions can be fairly large as shown by the identity

$$2+3i=-(7-18)^2+(3+19i)(-15+12i)$$

contributing to $\mathscr{S}(2+3i)$ which has seemingly only finitely many elements.

There are obvious bijections between $\mathscr{S}(z),\mathscr{S}(\overline{z}),\mathscr{S}(-z),\mathscr{S}(\pm iz)$. Moreover, $\mathscr{S}(z)$ infinite implies $\mathscr{S}(s\bar{s}t^2z)$ infinite for non-zero Gaußian integers s,t in $\mathbb{Z}[i]\setminus\{0\}$.

References

[1] V. I. Arnol′d, "Higher dimensional continued fractions", *Regul. Chaotic Dyn.* **3** (1998), no. 3, p. 10-17.
[2] R. Bacher, "A Quixotic Proof of Fermat's Two Squares Theorem for Prime Numbers", to appear in *Am. Math. Mon.*
[3] B. Gruber, "Alternative formulae for the number of sublattices", *Acta Crystallogr., Sect. A* **53** (1997), no. 6, p. 807-808.
[4] N. J. A. Sloane, "The On-Line Encyclopedia of Integer Sequences", 2010, http://oeis.org.
[5] Y. M. Zou, "Gaussian binomials and the number of sublattices", *Acta Crystallogr., Sect. A* **62** (2006), no. 5, p. 409-410.