C. R. Acad. Sci. Paris, Ser. I 348 (2010) 947–950

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number Theory

On a theorem of Friedlander and Iwaniec

Sur un théorème de Friedlander et Iwaniec

Jean Bourgain[a,1], Alex Kontorovich[a,b,2]

[a] Department of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540, USA
[b] Department of Mathematics, Brown University, Providence, RI 02912, USA

ARTICLE INFO

Article history:
Received and accepted 5 August 2010

Presented by Christophe Soulé

ABSTRACT

In [3], Friedlander and Iwaniec (2009) studied the so-called Hyperbolic Prime Number Theorem, which asks for an infinitude of elements $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ such that the norm squared

$$\|\gamma\|^2 = a^2 + b^2 + c^2 + d^2 = p,$$

is a prime. Under the Elliott–Halberstam conjecture, they proved the existence of such, as well as a formula for their count, off by a constant from the conjectured asymptotic. In this Note, we study the analogous question replacing the integers with the Gaussian integers. We prove unconditionally that for every odd $n \geqslant 3$, there is a $\gamma \in \mathrm{SL}(2,\mathbb{Z}[i])$ such that $\|\gamma\|^2 = n$. In particular, every prime is represented. The proof is an application of Siegel's mass formula.

RÉSUMÉ

Dans [3], Friedlander et Iwaniec (2009) ont introduit l'ensemble des nombres premiers qui admettent une représentation

$$\|\gamma\|^2 = a^2 + b^2 + c^2 + d^2 = p,$$

où $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. Ils y étudient la question de savoir si cet ensemble est infini, et le démontrent sous la conjecture de Elliott et Halberstam. Dans cette Note, nous considérons le problème analogue pour les entiers de Gauss, donc $\gamma \in \mathrm{SL}(2,\mathbb{Z}[i])$, et montrons que $\|\gamma\|^2$ représente alors en fait tout nombre impair. La formule de masse de Siegel joue un rôle essentiel.

Version française abrégée

Suivant [3], les nombres premiers hyperboliques sont ceux qui admettent une représentation de la forme

$$p = \|\gamma\|^2 = a^2 + b^2 + c^2 + d^2,$$

E-mail addresses: bourgain@ias.edu (J. Bourgain), avk@math.ias.edu (A. Kontorovich).

[1] Partially supported by NSF grant DMS-0808042.

[2] Partially supported by NSF grants DMS-0802998 and DMS-0635607, and the Ellentuck Fund at IAS.

1631-073X/$ – see front matter © 2010 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.
doi:10.1016/j.crma.2010.08.004

où $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. La question est alors : cet ensemble est-il infini ? La probléme est ouvert, [3] y apporte une réponse affirmative sous la conjecture de Elliott et Halberstam, en utilisant des méthodes de cribles. Dans cette Note, nous nous intéressons au même problème, en remplaçant $\mathrm{SL}(2,\mathbb{Z})$ par $\mathrm{SL}(2,\mathbb{Z}[i])$, où $\mathbb{Z}[i]$ est l'anneau des entiers de Gauss. Donc nous considérons les entiers de la forme

$$\|\gamma\|^2 = |a|^2 + |b|^2 + |c|^2 + |d|^2,$$

où $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z}[i])$.

En utilisant la formule de masse de Siegel et un calcul de densités locales, basé sur les résultats de [5], on montre que tout entier impair admet une telle répresentation.

1. Introduction

The Affine Linear Sieve, introduced by Bourgain, Gamburd and Sarnak [1], aims to produce prime points for functions on orbits of groups of morphisms of affine space. Friedlander and Iwaniec [3] considered the case of the full modular group $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, with the function being the norm-square. Let S be the set of norm-squares in Γ, that is,

$$S := \left\{n \in \mathbb{Z}_+ \colon\ n = \|\gamma\|^2 \text{ for some } \gamma \in \mathrm{SL}(2,\mathbb{Z})\right\}.$$

They proved, assuming an approximation to the Elliott–Halberstam conjecture, that S contains infinitely many primes.[3]

Unconditionally, one can easily show the existence of 2-almost primes in S. Indeed, for any $x \in \mathbb{Z}$, the parabolic elements

$$n_x := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

are in Γ, and their norm-square is $\|n_x\|^2 = x^2 + 2$. Then Iwaniec's theorem [4] produces infinitely many 2-almost primes in S.

In this Note, we ask an analogous question, replacing the integers in $\mathrm{SL}(2,\mathbb{Z})$ by the Gaussian integers, $\Gamma = \mathrm{SL}(2,\mathbb{Z}[i])$. We prove unconditionally the following

Theorem 1.1. *The set*

$$S := \left\{n \in \mathbb{Z}_+ \colon\ n = \|\gamma\|^2 \textit{ for some } \gamma \in \mathrm{SL}\big(2,\mathbb{Z}[i]\big)\right\}$$

contains all odd integers $n \geqslant 3$. *In particular, it contains all primes.*

The proof, given in the next section, is an application of Siegel's mass formula [7]. The argument is sufficiently delicate that it cannot replace the Gaussian integers above by the ring of integers of another number field, even an imaginary quadratic extension (as suggested to us by John Friedlander), see Remark 2.1.

2. Sketch of the proof

For odd $n \geqslant 3$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a = a_1 + ia_2$, etc., the conditions $n = \|\gamma\|^2$ and $\gamma \in \mathrm{SL}(2,\mathbb{Z}[i])$ imply

$$\begin{cases} \|\gamma\|^2 = a_1^2 + b_1^2 + c_1^2 + d_1^2 + a_2^2 + b_2^2 + c_2^2 + d_2^2 = n, \\ \mathfrak{Re}(\det\gamma) = a_1d_1 - b_1c_1 + b_2c_2 - a_2d_2 = 1, \\ \mathfrak{Im}(\det\gamma) = a_1d_2 + a_2d_1 - b_1c_2 - b_2c_1 = 0. \end{cases} \tag{1}$$

Changing variables

$$\begin{aligned} a_1 &\to (y_1 + y_4)/2, & b_1 &\to (y_3 + y_2)/2, \\ c_1 &\to (y_3 - y_2)/2, & d_1 &\to (y_1 - y_4)/2, \\ a_2 &\to (y_5 + y_8)/2, & b_2 &\to (y_7 + y_6)/2, \\ c_2 &\to (y_7 - y_6)/2, & d_2 &\to (y_5 - y_8)/2, \end{aligned}$$

---

[3] Moreover they gave a formula for the count of norm-squares (with multiplicities), off by a constant from the conjectured asymptotic.

the system (1) becomes

$$\begin{cases} y_3^2+y_4^2+y_5^2+y_6^2=n-2, \\ y_1^2+y_2^2+y_7^2+y_8^2=n+2, \\ y_1y_5+y_2y_6-y_3y_7-y_4y_8=0. \end{cases} \tag{2}$$

Write

$$F=\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \qquad G_n=\begin{pmatrix} n+2 & \\ & n-2 \end{pmatrix},$$

and

$$X=\begin{pmatrix} y_1 & y_2 & -y_7 & -y_8 \\ y_5 & y_6 & y_3 & y_4 \end{pmatrix},$$

so that (2) becomes

$$XF\,{}^tX=G_n. \tag{3}$$

Recall Siegel's [7] mass formula, cf. [2, Appendix B, Eqs. (3.10) to (3.17)]. Clearly F is positive definite and alone in its genus, and hence the number $\mathcal{N}(F,G_n)$ of solutions X to (3) is given by

$$\mathcal{N}(F,G_n)=\prod_{p\leqslant\infty}\alpha_p(F,G_n), \tag{4}$$

where the local densities α_p are given as follows. For $p<\infty$, they are defined by

$$\alpha_p(F,G_n)=p^{-5t}\cdot\#\bigl\{X\bigl(\mathrm{mod}\ p^t\bigr):\ XF\,{}^tX\equiv G_n\bigl(p^t\bigr)\bigr\}, \tag{5}$$

for t sufficiently large. For $p=\infty$, we have

$$\alpha_\infty(F,G_n)=2\pi^3\bigl(n^2-4\bigr)^{1/2}.$$

Remark 2.1. In complete generality, it is notoriously difficult to compute the local densities α_p and extract information such as non-vanishing, see e.g. the formulae in [8,9]. The main problem being how large is "sufficiently large" for t in (5) with a given p. In our special case of $\Gamma=\mathrm{SL}(2,\mathbb{Z}[i])$, the literature is sufficient to carry out the task.

For $p\neq 2$, both the ramified and unramified local densities can be evaluated as in e.g. [5, Theorem 2]. We turn first to the case p is unramified, $p\nmid(n^2-4)$. Then

$$\alpha_p(F,G_n)=\left(1-\frac{1}{p^2}\right)\left(1+\frac{\chi_p(4-n^2)}{p}\right),$$

where $\chi_p=(\frac{\cdot}{p})$ is the quadratic character mod p. For ramified primes $p\geqslant 3$, write $n+2=mp^a$ and $n-2=kp^b$ with $(mk,p)=1$. Assume $0\leqslant a\leqslant b$ (otherwise reverse their roles). Then if $a+b\equiv 0\pmod 2$,

$$\alpha_p(F,G_n)=\frac{(p+1)((p^{a+1}-1)(\chi_p(-mk)-1)+(a+1)(p^2-1)p^{(a+b)/2})}{p^{3+(a+b)/2}}.$$

Otherwise, if $a+b\equiv 1\pmod 2$, then

$$\alpha_p(F,G_n)=\frac{(p+1)^2((a+1)(p-1)p^{(a+b+1)/2}-(p^{a+1}-1))}{p^{3+(a+b+1)/2}}.$$

Inspection shows that these terms never vanish.

It remains to evaluate the dyadic density, α_2. As shown by Siegel, see [6], for n odd (and hence n^2-4 odd), it is sufficient to evaluate (5) for $t=3$, that is, compute the number of solutions mod $2^3=8$. One can compute explicitly that for any odd n, the number of solutions to (5) mod 8 is 49 152. Since $8^5=32\,768$, we have

$$\alpha_2(F,G_n)=\frac{3}{2}.$$

In conclusion, the α_p's never vanish so there are no local obstructions for odd n to be represented, and hence the set S of norm-squares in $\mathrm{SL}(2,\mathbb{Z}[i])$ contains all the primes. (The prime 2 is in S since it is the norm squared of the identity matrix.)

Acknowledgements

We thank Zeev Rudnick and Peter Sarnak for conversations regarding this work.

References

[1] Jean Bourgain, Alex Gamburd, Peter Sarnak, Sieving and expanders, C. R. Acad. Sci. Paris, Ser. I 343 (3) (2006) 155–159.
[2] J.W.S. Cassels, Rational Quadratic Forms, London Mathematical Society Monographs, vol. 13, Academic Press, London–New York–San Francisco, 1978.
[3] John B. Friedlander, Henryk Iwaniec, Hyperbolic prime number theorem, Acta Math. 202 (1) (2009) 1–19.
[4] Henryk Iwaniec, Almost-primes represented by quadratic polynomials, Invent. Math. 47 (1978) 171–188.
[5] Yoshiyuki Kitaoka, A note on local densities of quadratic forms, Nagoya Math. J. 92 (1983) 145–152.
[6] Irma Reiner, On the two-adic density of representations by quadratic forms, Pacific J. Math. 6 (1956) 753–762.
[7] Carl Ludwig Siegel, Über die analytische Theorie der quadratischen Formen, Ann. Math. (2) 36 (3) (1935) 527–606.
[8] Tonghai Yang, An explicit formula for local densities of quadratic forms, J. Number Theory 72 (2) (1998) 309–356.
[9] Tonghai Yang, Local densities of 2-adic quadratic forms, J. Number Theory 108 (2) (2004) 287–345.