Super-Apollonian circles and lattices of Gaussian integers

Marc Fleury[1*] and Nicolas Hannachi[1]

[1*]Département de Mathématiques, Lycée Chateaubriand, boulevard de Vitré, Rennes, 35000, France.

*Corresponding author(s). E-mail(s): marc.fleury4@free.fr;
Contributing authors: nicolas_hannachi@yahoo.fr;

Abstract

We study the circles of the Apollonian band circle super-packing, which are also the images of the real projective line by all linear fractional transformations of the group $\boldsymbol{PLS(2,\mathbb{Z}[i])}$. This super-packing takes place on the torus rather than on the plane. We focus first on the connection between these circles and lattices in the ring of Gaussian integers. Then we explore the group structure of the set of such circles with given curvature. The end of this paper is more geometrically-minded and describes first a test to determine whether a Gaussian circle is Apollonian or not, then a process which yields quickly all Gaussian circles with curvature smaller than a given integer. We develop algorithms for each of the computational problems we encounter.

Keywords: Quadratic Forms, Diophantine Geometry, Finite abelian groups, Circle packings

MSC Classification: 11E25 , 11G99 , 20K01 , 52C26

Introduction

The circles of the band Apollonian packing can be obtained as the images of four of them by the elements of a subgroup of $PSL(2,\mathbb{Z}[i])$ (see *e.g.* [2, 7] and figure 1).

This led the authors of the present paper to consider all the images of the real projective line by all linear fractional transformations of $PSL(2,\mathbb{Z}[i])$,

that we call Gaussian circles and to which Apollonian circles belong. These circles have already been introduced in previous publications, either the way we do here [1, 3], or as images of four or them by a group called 'Apollonian super-group' (see [4, 5]).

In Section One, we give elementary properties of Gaussian circles.

In Section Two, we show that the quotient set of the set of oriented Gaussian circles by the group of translations by Gaussian integers (this amounts to drawing Gaussian circles on the torus $\mathbb{C}/\mathbb{Z}[i]$ rather than on the plane $\mathbb{C}$) is in one to one correspondence with the set of oriented primitive lattices in $\mathbb{Z}[i]$, the absolute curvature of a Gaussian "true circle" (not a line) being the double of the index of its associated lattice, which we call lattice of denominators of this circle.

Section Three is devoted to the study of the primitive lattices of index n, where n is a given integer. These lattices form a group with respect to lattice multiplication, which is isomorphic to the projective line $(\mathbb{Z}/n\mathbb{Z})[i]^*/(\mathbb{Z}/n\mathbb{Z})^*$ on the ring $\mathbb{Z}/n\mathbb{Z}$, provided with the multiplication induced by the multiplication in $(\mathbb{Z}/n\mathbb{Z})[i]$ (where i denotes an external square root of -1). We study the structure of this finite abelian group and provide an algorithm giving the points of this projective line, once each.

We also show that the set of centres of Gaussian circles of half-curvature n drawn on the torus is a conic on the ring $\mathbb{Z}/n\mathbb{Z}$ which inherits a group law analogous to an angle addition.

In Section Four, we remark that the curvatures of the Gaussian circles (oriented in a suitable manner) through a given rational point z (these circles are all tangent at this point) form an arithmetic progression with common difference $|c|^2$ where $z = a/c$ with coprime $a, c \in \mathbb{Z}[i]$. Hence we will say that two tangent oriented Gaussian circles are immediately tangent when their curvatures are successive in this progression.

Looking then for a point of minimal denominator squared modulus among the rational points on a Gaussian circle, which amounts to minimizing the quadratic form associated with the lattice of denominators of this circle, allows to define a finite sequence of Gaussian circles, each of them being immediately tangent to its predecessor and of lower curvature. This provides a fast algorithm which caracterizes the Apollonian circles among the Gaussian ones.

Conversely, rising curvatures instead of lowering them enables a quick recursive computation of all Gaussian circles (drawn on the torus) whose curvatures are bounded by some given integer.

Appendix A is a short *vade mecum* about the reduction of positive definite integer binary quadratic forms taken from Reference [2].

The algorithms derived from the present work are given in Appendix B.

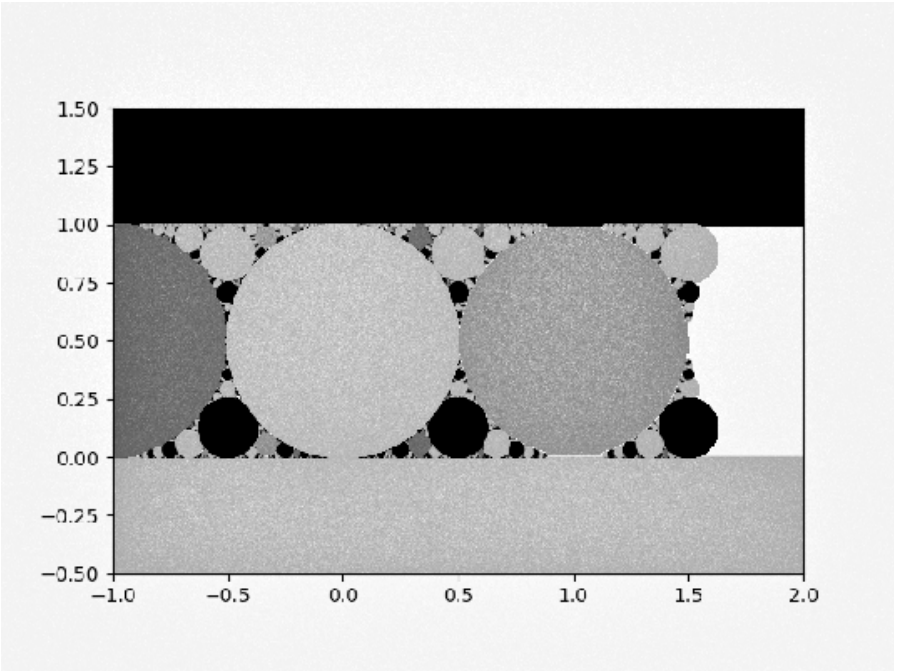

Fig. 1 Apollonian circles

1 Images of the real projective line by linear fractional transformations of $\boldsymbol{PSL(2,\mathbb{Z}[i])}$

Definition 1 : The image

$$\mathcal{C} = \left\{ \frac{at+b}{ct+d}, t \in \hat{\mathbb{R}} \right\} \text{ where } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}[i])$$

of the real projective line $\mathbb{R} \cup \{\infty\}$, which we will denoted $\hat{\mathbb{R}}$, by any linear fractional transformation with Gaussian integer coefficient will be called a *Gaussian circle*.

Figure 2 shows a finite number of circles obtained this way.

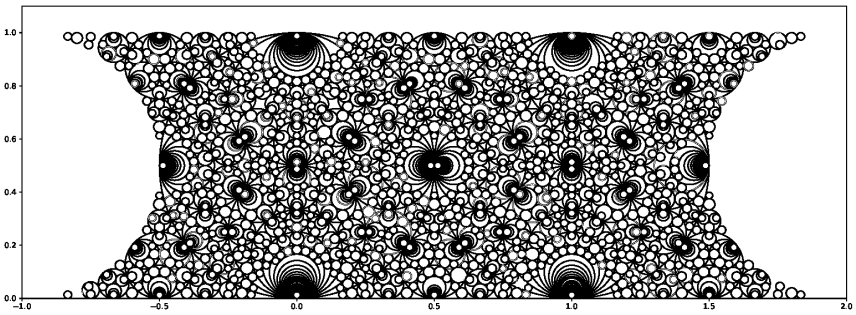

Fig. 2 Gaussian circles (with half-curvature at most 1000)

Proposition 1 *: Denoting also g the linear fractional transformation of matrix g, $g(0) = b/d, g'(0) = 1/d^2, g''(0) = -\frac{2c}{d^3}$ and $g(\hat{\mathbb{R}})$ has curvature $\gamma = 2\,\mathfrak{Im}(\bar{c}d)$ and centre $\omega = \frac{b}{d} + i\frac{\bar{d}}{2\,\mathfrak{Im}(\bar{c}d)d} = \frac{i(a\bar{d}-b\bar{c})}{\gamma}$.*

Proof :

$$
\begin{aligned}
g'(t) &= \frac{a(ct+d) - c(at+b)}{(ct+d)^2} = \frac{1}{(ct+d)^2} \\
\gamma &= \frac{[g'(0), g''(0)]}{||g'(0)||^3} = \frac{[\frac{1}{d^2}, -\frac{2c}{d^3}]}{|\frac{1}{d^6}|} \\
&\qquad \text{where } [\,.\,,\,.\,] \text{ denotes the skew product on } \mathbb{C} \\
&= -2\,\mathfrak{Im}\frac{c}{\bar{d}^2 d^3}|d|^6 = -2\,\mathfrak{Im}(c\bar{d})\frac{|d|^6}{|d|^6} = 2\,\mathfrak{Im}(\bar{c}d) \\
\omega &= g(0) + \frac{i}{\gamma}\frac{g'(0)}{|g'(0)|} = \frac{b}{d} + i\frac{\bar{d}}{2\,\mathfrak{Im}(\bar{c}d)d} \\
&= i\frac{b(c\bar{d} - d\bar{c}) + \bar{d}}{\gamma d} = i\frac{(ad-1)\bar{d} - bd\bar{c} + \bar{d}}{\gamma d} = i\frac{a\bar{d} - b\bar{c}}{\gamma}
\end{aligned}
$$

□

Proposition 2 *Any two distinct Gaussian circles are either tangent at some point in $\mathbb{Q}[i] \cup \{\infty\}$ or disjoint. In case of tangency at some finite point b/d with $b, d \in \mathbb{Z}[i]$ and $\gcd(b, d) = 1$, the common tangent is directed by $1/d^2$ ($= \infty$ if the tangent is vertical). Zero curvature Gaussian circles are horizontal lines.*

Proof : Since $SL(2,\mathbb{Z}[i]$ acts transitively on Gaussian circles, preserving tangency, and on rational points of $\mathbb{C} \cup \{\infty\}$, it suffices to prove that any Gaussian circle is either tangent at some rational point to the real projective line or disjoint from it. Let $\mathcal{C} = g(\hat{\mathbb{R}})$ with $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a Gaussian circle distinct from the real projective line. If $\mathcal{C}$ is a line (a zero curvatuve circle through $\infty = g(t)$ for some $t \in \hat{\mathbb{Q}}$) then since $SL(2,\mathbb{R})$ acts transitively on $\hat{\mathbb{Q}}$ one may suppose $\infty = g(\infty)$ by multiplying g on the right by some matrix $h \in SL(2,\mathbb{R})$ if needed. So $c = 0$, $|a| = |d| = 1$ and therefore $\mathcal{C}$ is a horizontal line $y = \mathfrak{Im}(b/d) = \textit{some integer}$, tangent to the real projective line at ∞.

Otherwise $\mathcal{C}$ is a true circle with curvature $\gamma = 2\,\mathfrak{Im}(\bar{c}d)$ and centre $\omega = \frac{i(a\bar{d}-b\bar{c})}{\gamma}$. Then $\mathfrak{Im}((i(a\bar{d} - b\bar{c})) = \mathfrak{Re}(a\bar{d} - b\bar{c})$ is a non zero integer because it has the same parity as $1 = ad - bc = \mathfrak{Re}(ad - bc) = \mathfrak{Re}(a\bar{d} - b\bar{c}) + \mathfrak{Re}(a(d - \bar{d}) - b(c\bar{c}) = \mathfrak{Re}(a\bar{d} - b\bar{c}) + 2\,\mathfrak{Im}(a)\,\mathfrak{Im}(d) - 2\,\mathfrak{Im}(b)\,\mathfrak{Im}(c)$. Thus we have $|\,\mathfrak{Im}(i(a\bar{d} - b\bar{c})| \geq |1/\gamma|$ so $\mathcal{C}$ is either tangent to the real projective line at $\mathfrak{Re}(\omega) \in \mathbb{Q}$ or disjoint from it.

□

2 The lattice of denominators of a Gaussian circle

Definition 2 A lattice in $\mathbb{Z}[i]$ is called *primitive* if and only if the set of common divisors of its elements is $\{\pm 1, \pm i\} = (\mathbb{Z}[i])^*$.

Remark 1 All primitive lattices in $(\mathbb{Z}[i], +)$ have rank 2 except $\mathbb{Z}$ and $i\mathbb{Z}$.

Theorem 3 *: Let $\mathcal{R}$ denote the set of oriented primitive lattices in $(\mathbb{Z}[i], +)$.*

The map

$$\begin{aligned} \varphi :\ & SL(2,\mathbb{Z}[i]) \to \mathcal{R} \\ & g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto L = c\mathbb{Z} + d\mathbb{Z} \end{aligned}$$

where $c\mathbb{Z} + d\mathbb{Z}$ is oriented by (c, d) if it has rank 2, by c if it has rank 1 and $c \neq 0$ and by $(-d)$ otherwise,

is surjective.

Let g, g' be two elements of $SL(2,\mathbb{Z}[i])$ et L, L' their images by φ.

g and g' define the same oriented Gaussian circle drawn on the torus if and only if L and L' are the same oriented lattice.

Remark 2 : Beware of the troubling fact that to the canonically oriented projective line $\hat{\mathbb{R}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(\hat{\mathbb{R}})$ is associated the rank 1-lattice $0\mathbb{Z} + 1\mathbb{Z}$ oriented by (-1).

Proof :

- For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}[i])$ one has $ad - bc = 1$ so by Bézout's lemma, $gcd(c, d) = 1$ and $\varphi(g)$ is primitive.

• Let $L \in \mathcal{R}$.

If $L = c\mathbb{Z} + d\mathbb{Z}$ with $gcd(c,d) = 1$ then by Bézout's lemma , there exist some $a, b \in \mathbb{Z}[i]$ such that $ad - bc = 1$ so $L = \varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Thus φ is surjective.

• Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $g' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL(2, \mathbb{Z}[i])$. Suppose that $\varphi(g) = \varphi(g')$.

Assume that $\mathfrak{Im}(\bar{c}d) \neq 0$. Then $\mathfrak{Im}(\bar{c'}d')$ and $\mathfrak{Im}(\bar{c}d) \neq 0$ have same sign.

Thus there is some $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in SL(2, \mathbb{Z})$ such that

$$(c' \ d') = (c \ d) \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$$

Set

$$g'' = g \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \begin{pmatrix} a'' & b'' \\ c' & d' \end{pmatrix}$$

Since

$$1 = a'd' - b'c' = a''d' - b''c'$$

one has

$$0 = (a' - a'')d' - (b' - b'')c'$$

Since $gcd(c', d') = 1$, by Euclid's lemma there is some $k \in \mathbb{Z}[i]$ such that $\begin{cases} a' - a'' = kc' \\ b' - b'' = kd' \end{cases}$

Therefore

$$g' = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} g'' = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$$

Since $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in SL(2, \mathbb{Z}) \subset SL(2, \mathbb{R})$, if maps $\hat{\mathbb{R}}$ to itself leaving its orientation unchanged. Besides, $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ represents the translation $z \mapsto z + k$.

Thus the oriented circles $g\hat{\mathbb{R}}$ and $g'\hat{\mathbb{R}}$ are the same when drawn on the torus.

The same result holds when $\mathfrak{Im}(\bar{c}d) = 0$: in that case $c \in \{\pm 1, \pm i\}$ or ($c = 0$ and $d \in \{\pm 1, \pm i\}$), and the same is true for c' and d'. Suppose for example that $c = 1$. Then $c' = 1$ or ($c' = 0$ and $d' = -1$). In the first case $b = b' = -1$ and $g' = \tau g$ where $\tau = \begin{pmatrix} 1 & a' - a \\ 0 & 1 \end{pmatrix}$ so g and g' define the same oriented circle drawn on the torus. In the second case, $a' = -1$ and multiplying g' on the right by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ which maps $\hat{\mathbb{R}}$ onto itself leaving its orientation unchanged, we are brought back to the first case.

• Conversely, suppose that the oriented circles $g\hat{\mathbb{R}}$ and $g'\hat{\mathbb{R}}$ are images of one another by some translation by a Gaussian integer k.

Set $g'' = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}^{-1} g'$. Then :

$$g\hat{\mathbb{R}} = g''\hat{\mathbb{R}}$$
$$g''^{-1} g\hat{\mathbb{R}} = \hat{\mathbb{R}}$$

Set $g''^{-1} g = h = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$.

$$t \mapsto \frac{\alpha t + \gamma}{\beta t + \delta}$$

maps $\hat{\mathbb{R}}$ onto itself with orientation unchanged, so differentiating :

$$\forall t \in \hat{\mathbb{R}} \qquad \frac{1}{(\beta t + \delta)^2} \geq 0 \text{ therefore } \beta \text{ and } \delta \text{ are reals.}$$

α and γ are thus also reals so $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ belongs to $SL(2, \mathbb{Z})$. Since

$$g = g'' \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} g' \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$$

$c\mathbb{Z} + d\mathbb{Z}$ and $c'\mathbb{Z} + d'\mathbb{Z}$ are the same oriented lattice. □

Proposition 4 *: Let* $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}[i])$.

Then the set of rational points in $g(\hat{\mathbb{R}})$ *is* $\left\{ \frac{ap+bp}{cp+dq},\ (p,q) \in \mathbb{Z}^2 \setminus \{(0,0)\} \right\}$

Proof :

Let $p, q \in \mathbb{Z}$ not both equal to zero. Then $\frac{p}{q} \in \hat{\mathbb{Q}}$ and $g(\frac{p}{q}) = \frac{ap+bq}{cp+dq}$ is a rational point in $g(\hat{\mathbb{R}})$.

Conversely if $m = \frac{p'}{q'}$ with $(p', q') \in \mathbb{Z}[i]$, not both equal to zero, is a rational point in $g(\hat{\mathbb{R}})$ then $x = g^{-1}(m) = \frac{dp'-bq'}{-cp'+aq'} \in \widehat{\mathbb{Q}[i]} \cap \hat{\mathbb{R}} = \hat{\mathbb{Q}}$ and thus there exist $p, q \in \mathbb{Z}$, not both equal to zero, such that $x = \frac{p}{q}$.

One as then $\frac{p'}{q'} = \frac{ap+bq}{cp+dq} \in g(\hat{\mathbb{Q}})$ □

Definition 3 : The oriented lattice $\mathbb{Z}c + \mathbb{Z}d$ will be called the *lattice of denominators* of the oriented circle $g(\hat{\mathbb{R}})$.

Remark 3 The previous proposition shows that this oriented lattice depends uniquely on the oriented circle $g(\hat{\mathbb{R}})$ drawn on the torus.

The term "lattice of denominators" is a little deceptive : every rational point of a Gaussian circle has at least one fractional representation with denominator in its lattice of denominators but this does not hold for all the fractional representations of this point.

Proposition 5 *:*

1) $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *and* $h = \begin{pmatrix} -b & -a \\ d & c \end{pmatrix}$ *define the same lattices but with opposite orientation and circles on the torus which are symmetric of one another with respect to the origin and of opposite orientations.*

2) $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *and* $h = \begin{pmatrix} -ia & ib \\ -ic & id \end{pmatrix}$ *define identical circles with opposite orientations and lattices which are symmetric of one another with respect to the line* $y = x$ *and with opposite orientations.*

Proof :

1) $h(\infty) = -\frac{b}{d} = -g(0)$ and the associated Gaussian circles have opposite curvatures and their tangent lines at the points b/d and $-b/d$ are parallel.

2) $g\hat{\mathbb{R}}$ and $h\hat{\mathbb{R}}$ correspond to each other by time reversal, and $[-\bar{i}c, id] = \mathfrak{Im}(i\bar{c}id) = -\mathfrak{Im}(\bar{c}d)$

□

3 Primitive lattices of given index n

3.1 Correspondence with the projective line on $\mathbb{Z}/n\mathbb{Z}$

Theorem 6 *Let $n \in \mathbb{N}^*$.*

1) Let $\alpha \in \mathbb{Z}[i]$ such that $gcd(\alpha, n) = 1$ i.e. $gcd(|\alpha|^2, n) = 1$.

(since if α is prime to n, so is $\bar{\alpha}$ thus $\alpha\bar{\alpha}$ also, and conversely if $|\alpha|^2$ is prime to n, so is α since it divides $|\alpha|^2$).

Then $\{z \in \mathbb{Z}[i],\ \mathfrak{Im}(\bar{\alpha}z) \equiv 0\,[n]\}$ is an unoriented primitive lattice of index n in $\mathbb{Z}[i]$.

2) Let L be an unoriented primitive lattice of index n in $\mathbb{Z}[i]$. Then there exists $\alpha \in L$ such that $gcd(\alpha, n) = 1$, and for any such α, one has $L = \{z \in \mathbb{Z}[i],\ \mathfrak{Im}(\bar{\alpha}z) \equiv 0\,[n]\}$.

Proof :

1) Let $A = \alpha + n\mathbb{Z}[i]$ be the congruence class of α modulo n.

Let $(\mathbb{Z}/n\mathbb{Z})[i]$ denote the set of couples of elements of $\mathbb{Z}/n\mathbb{Z}$ provided with the complex multiplication $(a,b)(c,d) \mapsto (ac - bd, ad + bc)$ (i denotes the couple $(0,1)$ and is an *external* square root of -1 and therefore -1 will always have more square roots in $(\mathbb{Z}/n\mathbb{Z})[i]$ than in $\mathbb{Z}/n\mathbb{Z}$).

$A \in \mathbb{Z}[i]/(n\mathbb{Z}[i]) \simeq (\mathbb{Z}/n\mathbb{Z})[i]$. Since α is prime to n, A is invertible.

Let $z \in \mathbb{Z}[i]$ and $Z = z + n\mathbb{Z}[i]$.

$$\begin{aligned}
\mathfrak{Im}(\bar{\alpha}z) \equiv 0\,[n] &\Leftrightarrow \mathfrak{Im}(\bar{A}Z) = 0_{\mathbb{Z}/n\mathbb{Z}} \\
&\Leftrightarrow \bar{A}A\,\mathfrak{Im}(A^{-1}Z) = 0 \\
&\Leftrightarrow \mathfrak{Im}(A^{-1}Z) = 0 \quad \text{since } |A|^2 \text{ is invertible in } \mathbb{Z}/n\mathbb{Z} \\
&\Leftrightarrow Z \in \mathbb{Z}A \\
&\Leftrightarrow z \in \mathbb{Z}\alpha + \mathbb{Z}n + \mathbb{Z}in = L
\end{aligned}$$

L is primitive because $gcd(\alpha, n) = 1$, and L is of index n as being the kernel of the surjective group homomorphism $z \mapsto \mathfrak{Im}(\bar{\alpha}z) + n\mathbb{Z}$ from $(Z[i], +)$ onto $(\mathbb{Z}/n\mathbb{Z}, +)$. This homomorphism is indeed surjective because $1 + n\mathbb{Z}$ is in its image set since by Bézout's lemma, there are some $u, v \in \mathbb{Z}[i]$ such that $1 = \bar{\alpha}u + nv$ and thus

$$\mathfrak{Im}(\bar{\alpha}iu) = \mathfrak{Im}(i - nvi) \equiv 1\ [n]$$

2) By Smith normal form, there exist $e_1', e_2' \in \mathbb{Z}[i]$ and $\lambda, \mu \in \mathbb{N}^*$ such that $\lambda|\mu$ and

$$\mathbb{Z}[i] = \mathbb{Z}e_1' + \mathbb{Z}e_2' \quad \text{et } L = \mathbb{Z}\lambda e_1' + \mathbb{Z}\mu e_2'$$

$\lambda = 1$ because L is primitive, and thus $\mu = n$ since L is of index n and also of index $\lambda\mu$.

Setting $P = Mat_{can}(e'_1, e'_2) \in GL_2(\mathbb{Z})$ (where *can* denotes the canonical basis of $\mathbb{R}^2$), L has equation $y' \equiv 0[n]$ with $\begin{pmatrix} x' \\ y' \end{pmatrix} = P^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$.

Setting $P^{-1} = \begin{pmatrix} u & v \\ -b & a \end{pmatrix}$ with $au + bv = \pm 1$, L has equation $-bx + ay \equiv 0[n]$.

L contains $a + ib$ and $n(v - iu)$ as well as the subgrouup they generate. This subgroup has index n since $a + ib$ and $v - iu$ generate $\mathbb{Z}[i]$.

By inclusion and equality of indices, $L = \mathbb{Z}(a+ib)+\mathbb{Z}n(v-iu)$. Eventually, since L is primitive, $a + ib$ and n are relatively prime.

Let $\alpha \in L$, prime to n. Set $M = \{z \in \mathbb{Z}[i] \mid \mathfrak{Im}(\bar{\alpha}z) \equiv 0\,[n]\}$. This is a lattice with same index n as L (by the first point in the present theorem). M contains α and the multiples of n, so writing $\alpha = xe'_1 + nye'_2$ with $x, y \in \mathbb{Z}$ (which exist since $\alpha \in L$) one has $gcd(x, n) = 1$ so by Bézout's lemma, there are some $u, v \in \mathbb{Z}$ such that $1 = xu + nv$, hence

$$e'_1 = uxe'_1 + nve'_1$$
$$e'_1 = u\alpha - unye'_2 + nve'_1 \in M$$

so $M \supset \mathbb{Z}e'_1 + n\mathbb{Z}e'_2 = L$.

Thus $L = M$. □

Definition 4 : $\mathcal{G}(n)$ will denote the set of unoriented primitive lattices of index n in $(\mathbb{Z}[i], +)$

Theorem 7 *: $\mathcal{G}(n)$ is stable under multiplication and the map*

$$\Phi \;:\; ((\mathbb{Z}/n\mathbb{Z})[i])^* \to \mathcal{G}(n)$$
$$A \mapsto L = \{z \in \mathbb{Z}[i],\ \ \mathfrak{Im}(\bar{\alpha}z) \equiv 0\,[n]\}$$

is a surjective group homomorphism with kernel $(\mathbb{Z}/n\mathbb{Z})^*$.

(α denotes any representative of A in $\mathbb{Z}[i]$, $(\mathbb{Z}/n\mathbb{Z})\,[i]$ being identified with $(\mathbb{Z}[i])/(n\mathbb{Z}[i])$)

(the product of two lattices L, L' in $\mathcal{G}(n)$ is defined as the lattice generated by all the products zz' with $(z, z') \in L \times L'$, see e.g. [2]).

Proof : Φ is well defined and surjective by the previous theorem.

Let $A, A' \in ((\mathbb{Z}/n\mathbb{Z})[i])^*$ with representatives α, α'.

For any $z \in \Phi(A)$ and $z' \in \Phi(A')$,

$$\begin{aligned} \mathfrak{Im}(\alpha\bar{\alpha}'zz') &= \mathfrak{Im}(\bar{\alpha}z\bar{\alpha}'z') \\ &= \mathfrak{Re}(\bar{\alpha}z)\,\mathfrak{Im}(\bar{\alpha}'z') + \mathfrak{Im}(\bar{\alpha}z)\,\mathfrak{Re}(\bar{\alpha}'z') \\ &\equiv \mathfrak{Re}(\bar{\alpha}z)0 + 0\,\mathfrak{Re}(\bar{\alpha}'z')\,[n] \\ &\equiv 0\,[n] \end{aligned}$$

hence $zz' \in \Phi(AA')$

Thus $\Phi(A)\Phi(A') \subset \Phi(AA')$.

Moreover,

$$\Phi(A)\Phi(A') = (\mathbb{Z}\alpha + n\mathbb{Z}[i])(\mathbb{Z}\alpha' + n\mathbb{Z}[i])$$

is generated by $\alpha\alpha', n\alpha, n\alpha', in\alpha, in\alpha', n^2$ and in^2.

By Bézout's lemma,

$$\mathbb{Z}[i]n\alpha + \mathbb{Z}[i]n^2 = n\mathbb{Z}[i]$$

Hence $\Phi(A)\Phi(A')$ contains $\alpha\alpha'$, n and in so it contains $\Phi(AA')$.

Hence $\Phi(A)\Phi(A') = \Phi(AA')$ (which proves *en passant* that $\mathcal{G}(n)$ is stable under multiplication).

Let $A \in \ker(\Phi)$. $\Phi(A) = \Phi(1)$. Since $\alpha \in \Phi(A)$, $\mathfrak{Im}(\bar{1}\alpha) \equiv 0[n]$ hence $A \in \mathbb{Z}/n\mathbb{Z}$. Since A is invertible, $A \in (\mathbb{Z}/n\mathbb{Z})^*$.

Conversely, if $A \in \mathbb{Z}/n\mathbb{Z}$ then for all $z \in \mathbb{Z}[i]$, setting $Z = z + n\mathbb{Z}[i]$,

$$\begin{aligned} z \in \Phi(A) &\Leftrightarrow \mathfrak{Im}(\bar{A}Z) = 0 \\ &\Leftrightarrow A\,\mathfrak{Im}(Z) = 0 \\ &\Leftrightarrow \mathfrak{Im}(Z) = 0 \\ &\Leftrightarrow z \in \Phi(1) \end{aligned}$$

Hence $\Phi(A) = \Phi(1)$ and thus $A \in \ker\Phi$. □

Proposition 8 *: $\mathcal{G}(n) \simeq ((\mathbb{Z}/n\mathbb{Z})[i])^*/(\mathbb{Z}/n\mathbb{Z})^*$*

This identification between $\mathcal{G}(n)$ and the projective line on the ring $\mathbb{Z}/n\mathbb{Z}$ will be made further on.

3.2 Multiplicative structure of the projective line $\mathcal{G}(n)$ on $\mathbb{Z}/n\mathbb{Z}$

Proposition 9 *: For m, n such that $m \wedge n = 1$,*

$$\mathcal{G}(mn) \simeq \mathcal{G}(m) \times \mathcal{G}(n)$$

and

$$\mathcal{G}(mn) = \{M \cap N, (M, N) \in \mathcal{G}(m) \times \mathcal{G}(n)\}$$

Remark 4 : Thus if n has at least two distinct prime divisors then $\mathcal{G}(n)$ is not cyclic since $\mathcal{G}(p^\alpha)$ (p prime, $\alpha \in \mathbb{N}^*$) has even order, as will be shown later.

Proof : The isomorphism results from the Chinese remainders theorem :

$$(\mathbb{Z}/mn\mathbb{Z})^* \simeq (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

and

$$((\mathbb{Z}/mn\mathbb{Z})[i])^* \simeq ((\mathbb{Z}/m\mathbb{Z})[i])^* \times ((\mathbb{Z}/n\mathbb{Z})[i])^*$$

Moreover, for $\gamma \in \mathbb{Z}[i]$ prime to mn, setting

$$\begin{aligned} L &= \{z \in \mathbb{Z}[i],\ \mathfrak{Im}(\bar{\gamma}z) \equiv 0\ [mn]\} \\ M &= \{z \in \mathbb{Z}[i],\ \mathfrak{Im}(\bar{\gamma}z) \equiv 0\ [m]\} \\ N &= \{z \in \mathbb{Z}[i],\ \mathfrak{Im}(\bar{\gamma}z) \equiv 0\ [n]\} \end{aligned}$$

then $L = M \cap N$, and since γ is prime to m and to n, one has $M \in \mathcal{G}(m)$, $N \in \mathcal{G}(n)$

Conversely, for $\alpha \in \mathbb{Z}[i]$ prime to m and $\beta \in \mathbb{Z}[i]$ prime to n, there exists (by the Chinese remainders theorem) $\gamma \in Z[i]$ such that $\gamma \equiv \alpha\ [m]$ and $\gamma \equiv \beta\ [n]$.

$$\begin{aligned} M &= \{z \in \mathbb{Z}[i],\ \ \mathfrak{Im}(\bar{\alpha}z) \equiv 0[m]\} \\ N &= \{z \in \mathbb{Z}[i],\ \ \mathfrak{Im}(\bar{\beta}z) \equiv 0[n]\} \\ L &= \{z \in \mathbb{Z}[i],\ \ \mathfrak{Im}(\bar{\gamma}z) \equiv 0\ [mn]\} \end{aligned}$$

thus

$$\begin{aligned} M &= \{z \in \mathbb{Z}[i],\ \ \mathfrak{Im}(\bar{\gamma}z) \equiv 0\ [m]\} \\ N &= \{z \in \mathbb{Z}[i],\ \ \mathfrak{Im}(\bar{\gamma}z) \equiv 0\ [n]\} \end{aligned}$$

hence $L = M \cap N$, and γ is prime to mn so $L \in \mathcal{G}(mn)$. □

Theorem 10 *: For prime p and $k \in \mathbb{N}^*$,*

1) $\mathcal{G}(p^k)$ has cardinal

$$\begin{cases} p^{k-1}(p+1) & \text{if } p \equiv -1[4] \\ p^{k-1}(p-1) & \text{if } \ p \equiv 1[4] \\ 2^k & \text{if } \quad p = 2 \end{cases}$$

2) $\mathcal{G}(p^k)$ is cyclic for odd p.

3) $\mathcal{G}(2^k)$ has exponent 2^{k-1}.

Proof :

1) $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ has cardinal $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Besides, for any $A, B \in \mathbb{Z}/p^\alpha\mathbb{Z}$ with representatives $a, b \in \mathbb{Z}$,

$$\begin{aligned} A + iB \notin ((\mathbb{Z}/p^\alpha\mathbb{Z})[i])^* &\Leftrightarrow p \,|\, a^2 + b^2 \\ &\Leftrightarrow b^2 \equiv -a^2\,[p] \end{aligned}$$

• If $p \equiv -1\,[4]$ then -1 is not a square modulo p and the only solution to the previous equation is $a \equiv b \equiv 0\,[p]$. Thus $((\mathbb{Z}/p^\alpha\mathbb{Z})[i])^*$ has cardinal $(p^\alpha)^2 - (p^{\alpha-1})^2$ and therefore $\mathcal{G}(p)$ has cardinal

$$\frac{(p^\alpha)^2 - (p^{\alpha-1})^2}{p^{\alpha-1}(p-1)} = p^{\alpha-1}(p+1)$$

• If $p \equiv -1\,[4]$ then -1 is a square modulo p. Let k be a square root of -1 modulo p. The previous equation holds if and only if $b \equiv \pm ka\,[p]$, which gives exactly $1 + 2(p-1) = 2p-1$ solutions modulo p and $(2p-1)p^{2(\alpha-1)}$ solutions modulo p^α.

Hence $((\mathbb{Z}/p^\alpha\mathbb{Z})[i])^*$ has cardinal

$$(p^\alpha)^2 - (2p-1)p^{2(\alpha-1)} = p^{2(\alpha-1)}(p^2 - 2p + 1) = p^{2(\alpha-1)}(p-1)^2$$

and thus $\mathcal{G}(p)$ has cardinal

$$p^{\alpha-1}(p-1)$$

• If $p = 2$, the previous equation holds if and only if $a \equiv b\,[2]$ and so one has 2 solutions modulo 2 and $2.(2^{\alpha-1})^2 = 2^{2\alpha-1}$ solutions modulo 2^α.

Therefore $((\mathbb{Z}/2^\alpha\mathbb{Z})[i])^*$ has cardinal

$$2^{2\alpha} - 2^{2\alpha-1} = 2^{2\alpha-1}$$

and $\mathcal{G}(2^\alpha)$ has cardinal

$$\frac{2^{2\alpha-1}}{2^{\alpha-1}} = 2^\alpha$$

2) The forthcoming proof is similar to the classical proof of cyclicity of $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

• We start by proving that $\mathcal{G}(p^\alpha)$ has an element of order $p^{\alpha-1}$.

Consider the following powers of $1 + ip$:

$$(1+ip)^p = 1 + pip - p\frac{(p-1)}{2}p^2 + \ldots = 1 + p^2\beta \quad \text{with } \beta \equiv i[p]$$

$$(1+ip)^{p^2} = (1+p^2\beta)^p = 1 + pp^2\beta + p\frac{p-1}{2}p^4\beta^2 + \ldots = 1 + p^3\gamma \quad \text{with } \gamma \equiv i[p]$$

And so on, up to :

$$(1+ip)^{p^{\alpha-2}} = 1 + p^{\alpha-1}\omega \quad \text{with } \omega \equiv i[p]$$

Eventually,

$$(1+ip)^{p^{\alpha-1}} \equiv 1[p^\alpha]$$

Hence the order of class of $1 + ip$ modulo p^α divides $p^{\alpha-1}$, and so does the class of this class in the quotient by $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

But since $(1 + ip)^{p^{\alpha-2}}$ is not "real" modulo p^α, the class of this power in the quotient by $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ is not the neutral class.

Thus $((\mathbb{Z}/p^\alpha\mathbb{Z})[i])^*/((\mathbb{Z}/p^\alpha\mathbb{Z}))^*$ has an element of order $p^{\alpha-1}$.

• If $p \equiv -1[4]$ then $(\mathbb{Z}/p\mathbb{Z})[i]$ is ring-isomorphic to $\mathbb{F}_p[X]/(X^2+1)$ which is a field because $X^2 + 1$ is irreducible on F_p. Since the group of units of any finite field is cyclic, $((\mathbb{Z}/p\mathbb{Z})[i])^*$ is cyclic and thus contains an element of order $p^2 - 1$.

Hence $((\mathbb{Z}/p^\alpha\mathbb{Z})[i])^*$ has an element of order $k(p^2-1)$ for some positive integer k, and the k^{th} power of this element has order $p^2 - 1$. Denote it by Z.

Quotienting by $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$, the order of the class of Z is divided by $gpe(Z) \cap (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ which divides $pgcd(p^2-1, (p-1)p^{\alpha-1}) = p - 1$.

Therefore this order is a multiple of $p + 1$. Hence $\mathcal{G}(p^\alpha)$ contains an element of order $p + 1$.

Since it also contains an element of order $p^{\alpha-1}$ and since $p + 1$ and $p^{\alpha-1}$ are prime to each other, our group contains an element of order $(p+1)p^{\alpha-1}$ (the product of the previous ones) and therefore is cyclic.

• We examine now the case where $p \equiv 1[4]$. $\mathbb{F}_p[i]$ is no more a field.

Define $P \in \mathbb{F}_p[X]$ by

$$P = 2\,\mathfrak{Im}((1+iX)^e)$$

where e is the exponent of the group $\mathcal{G}(p)$.

For all $y \in \mathbb{F}_p$ such that $y^2 \neq -1$, $1 + iy$ is invertible in $\mathbb{F}_p[i]$ (since so is $(1+iy)(1-iy)$ in $\mathbb{F}p$) and the class in $\mathcal{G}(p)$ of $(1+iy)^e$ is the neutral class, so $(1+iy)^e$ is 'real' and therefore $P(y) = 0$.

Hence P has at least $p - 2$ roots in $\mathbb{F}_p$.

By the way, $P = \frac{(1+iX)^e-(1-iX)^e}{i}$ has degree $e-1$ or $e-2$ whether e is even or odd.

Since $\mathbb{F}_p$ is a field, the number of roots of P doesn't exceed its degree.

So $p-2 \leq e-1$ and thus $e \geq p-1$. Moreover, e divides $card(\mathcal{G}(p)) = p-1$. Hence $e = p-1$.

Thus $\mathcal{G}(p)$ contains an element of order $p-1$, hence so does $\mathcal{G}(p^\alpha)$. As it also contains an element of order $p^{\alpha-1}$ (which is prime to $p-1$), $\mathcal{G}(p^\alpha)$ is cyclic.

3) Eventually we examine the case $p = 2$.

It has already been proved that $\mathcal{G}(2^\alpha)$ contains an element of order $2^{\alpha-1}$.

We prove below that it has no element of order 2^α.

Let $a + ib \in (\mathbb{Z}/2^k\mathbb{Z}[i])^*$. Identify $a + ib$ with one of its representatives in $\mathbb{Z}[i]$. a and b are of opposite parities. Up to multiplication by i, which does not change the orders of non neutral elements since these orders are even and $i^2 = -1 = +1$, one may assume that a is odd and b is even. Thus :

$a + ib = 1 + 2c$ with $c \in \mathbb{Z}[i]$

$(a + ib)^2 \equiv 1$ modulo 4

$(a + ib)^4 \equiv 1$ modulo 8

...

$(a + ib)^{2^{\alpha-1}} \equiv 1$ modulo 2^α

Hence no element of $(\mathbb{Z}/2^\alpha\mathbb{Z})[i]^*$ is of order 2^α. *A fortiori*, this also holds for $\mathcal{G}(2^\alpha)$ □

3.3 Enumeration of the elements of $\mathcal{G}(n)$

We present here a method for obtaining all the points, once each, of the projective line on $\mathbb{Z}/n\mathbb{Z}$ without the use of generators of the groups $\mathcal{G}(p^\alpha)$ for prime p's. This method is effective, see Algorithm 1.

Proposition 11 *: Let $n \in \mathbb{N}^*$.*

1) Every element of the projective line $(\mathbb{Z}/n\mathbb{Z})[i]^*/(\mathbb{Z}/n\mathbb{Z})^*$ has some representative in $((\mathbb{Z}/n\mathbb{Z})[i])^*$ of the form $d + ib$ where d divides n.

2) For d, d' divisors of n and k prime to n, one has :

$$d' \equiv kd\ [n] \Rightarrow d = d'\ et\ k \equiv 1[n/d]$$

3) For d divisor of n and $\alpha = d+ib \in \mathbb{Z}[i]^*$, the lattice of solutions of the equation $\mathfrak{Im}(\bar{\alpha}z) \equiv 0\ [n]$ has basis $(\alpha, i\frac{n}{d})$.

Proof :

1) Let $z \in (\mathbb{Z}/n\mathbb{Z})[i]^*$ and $a, b \in \mathbb{Z}$ such that $z = a + ib + n\mathbb{Z}[i]$.

If $a \equiv 0[n]$ then b is prime to n and $z = bi$ is in the class of i in the quotient of $(\mathbb{Z}/n\mathbb{Z})[i]^*$ by $(\mathbb{Z}/n\mathbb{Z})^*$.

Assume $a \not\equiv 0[n]$

Let $d = pgcd(a, n)$. The map $\begin{cases} \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{d\mathbb{Z}}{n\mathbb{Z}} \sim \frac{\mathbb{Z}}{\frac{n}{d}\mathbb{Z}} \\ \omega \mapsto d\omega \end{cases}$ is a surjective ring-homomorphism, and therefore induces a surjective homomorphism from $(\mathbb{Z}/n\mathbb{Z})^*$ onto the group of the classes modulo n/d of the integers which are prime to n/d. This

group can be identified with the set of congruence classes modulo n of the integers k such that $\gcd(k,n)=d$.

Hence there exists some integer u prime to n such that $ud \equiv a[n]$. Let v be an inverse of u modulo n. Set $z' = vz$. Then $z' \in (\mathbb{Z}/n\mathbb{Z})[i]^*$ as the product of two elements of $(\mathbb{Z}/n\mathbb{Z})[i]^*$, and z and z' are in the same class in the quotient of $(\mathbb{Z}/n\mathbb{Z})[i]^*$ by $(\mathbb{Z}/n\mathbb{Z})^*$. Moreover $\mathfrak{Re}(z') = \mathfrak{Re}(va) \equiv d\ [n]$.

2) Let d, d' be divisors of n and k an integer prime to n such that $d' \equiv kd\ [n]$. Since d divides n, it also divides d'.

Let k' be an inverse of k modulo n. Then $k'd' \equiv d[n]$ and by the same argument as above, d divides d'.

Hence $d = d'$.

Thus $d(k-1) \equiv 0\ [n]$ so $k - 1 \equiv 0[n/d]$ *i.e.* $k \equiv 1[n/d]$

3) α and $i\frac{n}{d}$ belong to the lattice L of equation $\mathfrak{Im}(\bar{\alpha}z) \equiv 0\ [n]$ and their skew product is $\mathfrak{Im}((d-ib)i\frac{n}{d}) = \frac{n}{d}\mathfrak{Re}(d-ib) = n$, so they generate L since this lattice has index n.

□

Algorithm 1 provides a non redundant list of representatives of the points of the projective line on $\mathbb{Z}/n\mathbb{Z}$.

3.4 Centres of Gaussian circles of given curvature, 'modular half circle'

To any matrix $g \in SL(2,\mathbb{C})$ we associate the matrix $G = g\bar{g}^{-1} = g(com(g))^* = g(JgJ^{-1})^*$ with $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

The *a posteriori* motivation of such a trick is to define the same matrix G for two matrices g, g' such that $g(\hat{\mathbb{R}})$ and $g'(\hat{\mathbb{R}})$ are the same oriented circle, *i.e.* $g^{-1}g' \in SL(2,\mathbb{R})$ *i.e.* $\bar{g}^{-1}\bar{g}' = g^{-1}g'$ *i.e.* $G = G'$.

The entries of G are sometimes called 'inversive coordinates' of the oriented circle $\mathcal{C} = g(\hat{\mathbb{R}})$.

The deep origin of this trick relies on the Weyl representation [6]:

$$g \mapsto \tau(g) : \bar{W} \mapsto g\bar{W}g^*$$

of $SL(2,\mathbb{C})$ on the space of hermitian 2×2 hermitian matrices. The transformations in $\tau(SL(2,\mathbb{R}))$ fix the hyperplane of real hermitian (symmetric) matrices (the set of hermitian matrices with determinant 1 is a model of the hyperbolic space H^3 and the trace on this space of our hyperplane is a hyperbolic plane, whose vanishing circle is the projective real line in the horizon of Poincaré's half-space model of H^3). Thus $\tau(SL(2,\mathbb{R}))$ also fixes the orthogonal (with respect to Frobenius inner product) $\mathbb{R}iJ$ of this hyperplane. That is why we set $G = \tau(g)(iJ)(iJ)^{-1} = gJg^*J^{-1}$

Proposition 12 *: Let* $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{C})$ *and* $\mathcal{C} = g(\hat{\mathbb{R}})$ *the circle* $\hat{\mathbb{C}}$ *oriented by the natural orientation of* $\hat{\mathbb{R}}$.

Remind that $\mathcal{C}$ *has curvature* $\gamma = 2\,\mathfrak{Im}(\bar{c}d)$ *and centre* $\omega = i\frac{a\bar{d}-b\bar{c}}{\gamma}$.

In the previous framework, $\det G = 1$ *and*

$$G = \begin{pmatrix} a\bar{d} - b\bar{c} & 2i\,\mathfrak{Im}(\bar{a}b) \\ -2i\,\mathfrak{Im}(\bar{c}d) & \bar{a}d - \bar{b}c \end{pmatrix} = \begin{pmatrix} i\gamma\omega & i(-\frac{1}{\gamma} + \gamma|\omega|^2) \\ -i\gamma & \overline{i\gamma\omega} \end{pmatrix}$$

Proof :

$$\det G = \frac{\det(g)}{\det(\bar{g})} = (\det g)^2 = 1$$

A straightforward calculation gives the expressions of G.

□

Proposition 13 *:*

In the previous framework, the following assertions are equivalent :

(i) $\mathcal{C}$ *is Gaussian*

(ii) $G = \begin{pmatrix} A & -2iB \\ -2iC & \bar{A} \end{pmatrix}$ *where* $B, C \in \mathbb{Z}$ *et* $A \in 1 + 2\mathbb{Z}[i]$

(iii) The fractional representation of ω *with smallest positive denominator is of the form*

$$\omega = \frac{p}{2q} \text{ where } q \in \mathbb{N}^*,\ p \in i + 2\mathbb{Z}[i],\ |p|^2 \equiv 1[4q]$$

i.e.

$$\omega = \frac{2x + (2y+1)i}{2q} \text{ where } q \in \mathbb{N}^*\ x, y \in \mathbb{Z},\ x^2 + y^2 + y \equiv 0\,[q]$$

$$\text{and} \quad |\gamma| = 2q.$$

Therefore a Gaussian centre encodes the only Gaussian circle of which it is the centre.

Proof :

$(i) \Rightarrow (ii)$. Suppose $\mathcal{C}$ is Gaussian.

Since $ad - bc = 1$ and $a\bar{d} - b\bar{c} = A$ one has

$$(S) \begin{cases} \frac{1+A}{2} &= a\,\mathfrak{Re}(d) - b\,\mathfrak{Re}(c) \\ \frac{1-A}{2i} &= a\,\mathfrak{Im}(d) - b\,\mathfrak{Im}(c) \end{cases}$$

Thus $A \in 1 + 2\mathbb{Z}[i]$.

Moreover $B = -\,\mathfrak{Im}(\bar{a}b)$ and $C = \mathfrak{Im}(\bar{c}d)$ belong to $\mathbb{Z}$.

$(ii) \Rightarrow (iii)$

By the previous proposition, $\omega = \frac{A}{2C}$. Besides $1 = \det() = A\bar{A} + 4BC$, so A and $2C$ are coprime by Bézout's lemma, hence $\frac{A}{2C}$ is irreducible.

Moreover,

$$|p|^2 = |iA|^2 = 1 - 4BC = 1 - 4Bq \equiv 1\,[4q]$$

and

$$|p|^2 - 1 = 4(x^2 + y^2 + y) \equiv 0\,[q]$$

Eventually $|\gamma| = 2|C| = 2q$.

$(iii) \Rightarrow (ii)$

Same argument, backwards.

$(ii) \Rightarrow (i)$.

The purpose is to show that if G satisfies (ii) then it corresponds to some matrix $g \in SL(2, \mathbb{Z}[i])$.

Assume first that B and C are both non zero.

$$\left[\frac{1+A}{2},\frac{1-A}{2i}\right] = \mathfrak{Im}\left(\frac{1+\bar{A}}{2},\frac{1-A}{2i}\right) = \mathfrak{Im}\left(\frac{1-|A|^2-2i\ \mathfrak{Im}(A)}{4i}\right)$$
$$= \frac{|A|^2-1}{4} = -BC$$

since $1 = \det G = |A|^2 + 4BC$.

Therefore the index of the lattice L generated by $\frac{1+A}{2}$ and $\frac{1-A}{2i}$ is a multiple of $|B|$, so there exists some lattice L' of index $|B|$ that contains L.

Let (a, b) be a basis of L'. Switching b and a if needed, assume that $[a, b] = -B$. Since L' contains $\frac{1+A}{2}$ and $\frac{1-A}{2i}$, the (real) coordinates of those complexes in the basis (a, b) are integers. Thus there exist $c, d \in \mathbb{Z}[i]$ satisfying system (S).

So $ad - bc = 1$ and $a\bar{d} - b\bar{c} = A$.

Furthermore,

$$-BC = \left[\frac{1+A}{2},\frac{1-A}{2i}\right] = [a,b]\det_{(a,b)}\left(\frac{1+A}{2},\frac{1-A}{2i}\right)$$
$$= [a,b]\begin{vmatrix}\mathfrak{Re}(d) & \mathfrak{Im}(d)\\ -\mathfrak{Re}(c) & -\mathfrak{Im}(c)\end{vmatrix} = -B[c,d]$$

hence $[c, d] = C$.

We still have to examine the case where B or C is zero. Then $|A|^2 = 1$ and since $A \in 1 + 2\mathbb{Z}[i]$, $A = \pm 1$.

If $C = 0$ set $\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}1 & -2iB\\ 0 & 1\end{pmatrix}$ if $A = 1$, or $\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}i & 2B\\ 0 & -i\end{pmatrix}$ if $A = -1$.

The case $B = 0$ is managed the same way.

Hence $\mathcal{C}$ is Gaussian. □

Theorem 14 *: Let $q \in \mathbb{N}^*$. The set of centres of Gaussian circles of curvature q drawn on the torus $\mathbb{C}/\mathbb{Z}[i]$ is in one to one correspondence with the 'modular half-circle' :*

$$\mathcal{E}_q = \{p = X + iY \in (\mathbb{Z}/2q\mathbb{Z})[i],\ \ \mathfrak{Re}(p) = X \equiv 0[2] \text{ and } p\bar{p} = X^2 + Y^2 \equiv 1[4q]\}$$

and the modular conic

$$\mathcal{F}_q = \{(x, y) \in (\mathbb{Z}/q\mathbb{Z}),\ x^2 + y^2 + y = 0_{\mathbb{Z}/q\mathbb{Z}}\}$$

Remark 5 : $\mathcal{E}_q$ can be considered as half of a 'modular circle of centre O' since $p\bar{p}$ can be fancied as 'the square of the distance to O modulo $4q$' for the points in $(\mathbb{Z}/2q\mathbb{Z})[i]$ whose real and imaginary parts have opposite parities, and it is imposed here to the real part to be even. This is more problematic for $\mathcal{F}_q$ when q is even since in that case 2 is not invertible modulo q and the "centre" of $\mathcal{F}_q$ is no longer defined.

Proof : We just have to apply the previous proposition and to notice that for $x, y, x', y' \in \mathbb{Z}$, $\frac{2x+(2y+1)i}{2q}$ et $\frac{2x'+(2y'+1)i}{2q}$ represent the same point on the torus if and only if $x \equiv x'\,[q]$ and $y \equiv y'\,[q]$. □

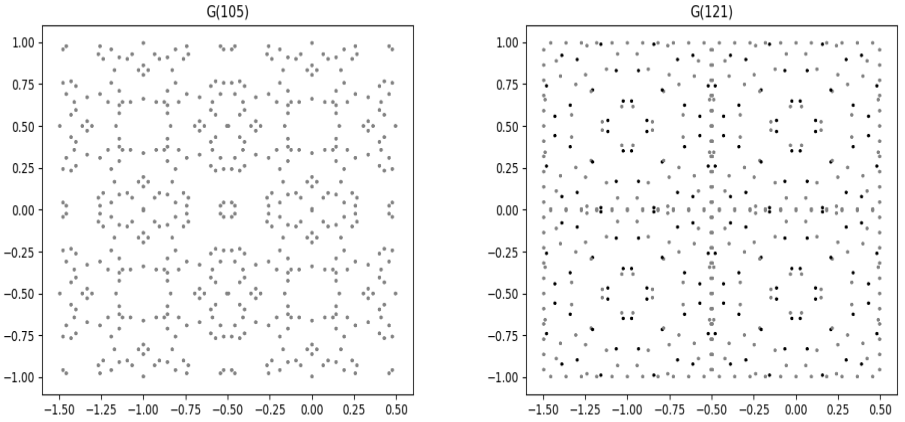

Fig. 3 'modular half circle' (four times) on $\mathbb{Z}/(2 \times 105\mathbb{Z})$ (on the left) and $\mathbb{Z}/(2 \times 121\mathbb{Z})$ (on the right)

Theorem 15 *: Let $A, A' \in (\mathbb{Z}/q\mathbb{Z})[i])^*/(\mathbb{Z}/q\mathbb{Z})^*$ and $A'' = AA'$ be three points on the projective line on $\mathbb{Z}/q\mathbb{Z}$. Let $\mathcal{C}, \mathcal{C}', \mathcal{C}''$ be the Gaussian circles of curvature $2q$ drawn on the torus corresponding to A, A', A'' (see section 3.1) and p, p', p'' be the points on $\mathcal{E}_q$ which are the numerators of the centres of these circles.*

Then

$$\frac{p''}{i} = \frac{p}{i}\frac{p'}{i}$$

(i.e. setting $p = X + iY$, etc... one has : $X'' = XY' + YX'$ and $Y'' = XX' - YY'$)

Proof : As shown in subsection 3.3, some $\alpha \in Z[i]$ can be chosen such that $\mathfrak{Re}(\alpha)$ is a divisor d of q and $\alpha + q\mathbf{Z}[i]$ is a representative of A. Then $(\alpha, i\frac{q}{d})$ is a basis of the lattice $\{z \in \mathbb{C},\ \mathfrak{Im}(\bar{\alpha}z) \equiv 0[q]\}$

α and q are then coprime, hence by Bézout's lemma, there exist $a, b \in \mathbb{Z}[i]$ such that $1 = ai\frac{q}{d} - b\alpha$ where a is a multiple of d.

By proposition 1 (section 1), the circle drawn on the torus corresponding to this lattice as centre $\frac{p}{2q}$ where

$$\frac{p}{i} = a\frac{-iq}{d} - b\bar{\alpha} = -1 - b\alpha - b\bar{\alpha} = -1 - 2\,\mathfrak{Re}(\alpha)b = -1 - 2db$$

Therefore

$$\frac{p}{i} = -1 - 2db \text{ where } b \text{ is the inverse of } -\alpha \text{ modulo } q$$

(this defines p modulo $2q$ and thus $\frac{p}{2q}$ modulo $\mathbb{Z}[i]$)

The same holds for A' and A'' and one have :

$$\begin{aligned}\frac{p}{i}\frac{p'}{i} &= (-1 - 2db)(-1 - 2d'b') \\ &= 1 + 2db + 2d'b' + 4dd'bb'\end{aligned}$$

where b (respectively b') is the inverse of $-\alpha$ (respectively $-\alpha'$) modulo q.

Besides $A'' = AA'$ has representatives in $(\mathbb{Z}/q\mathbb{Z})^*$:

$$\begin{array}{c} \alpha\alpha' = (dd' - ee') + i(de' + ed') \quad \text{on the one hand} \\ \alpha'' = d'' + ie'' \text{ where } d'' \text{ divides } q \text{ on the other hand} \end{array}$$

hence there exists some $k \in (\mathbb{Z}/q\mathbb{Z})^*$ such that $\alpha'' = \alpha\alpha' k$.

Therefore

$$\frac{p''}{i} = -1 - 2d''b''$$

where $d'' = k\,\mathfrak{Re}(\alpha\alpha')$ and b'' is the inverse of $-\alpha'' = -(-\alpha)(-\alpha')k$ modulo q.

Hence

$$b'' = -bb'\ell$$

where ℓ is the inverse of k modulo q.

Thus

$$\begin{aligned} \frac{p''}{i} &= -1 + 2k\,\mathfrak{Re}(\alpha\alpha')bb'\ell = -1 + 2\,\mathfrak{Re}(\alpha\alpha')bb' \\ &= -1 + 2\alpha\alpha' bb' - 2i\,\mathfrak{Im}(\alpha\alpha')bb' \\ &= -1 + 2 - 2i(de' + ed')bb' \\ &= 1 + 2i\left(d\frac{d' - \alpha'}{i} + d'\frac{d - \alpha'}{i}\right)bb' \\ &= 1 + 4dd' + 2(db + d'b') \end{aligned}$$

□

Remark 6 : Hence the 'modular half-circle' $\frac{1}{i}\mathcal{E}_q$ is a subgroup of $((\mathbb{Z}/2q\mathbb{Z})[i]^*, .)$ isomorphic to the projective line on $\mathbb{Z}/q\mathbb{Z}$ provided with its natural multiplication inherited from $(\mathbb{Z}/q\mathbb{Z})[i]$. The composition law on $\frac{1}{i}\mathcal{E}_q$ is analogous to the multiplication of exponentials of pure imaginary numbers, and building an additive 'angular parameter' on $\mathcal{E}_q$ amounts to building a logarithm on the projective line. This amounts to choosing a generator of that line if q is some power of an odd prime, an element of order 2^{k-1} and an element of order 2 (non power of the previous one) if $q = 2^k$ for some integer k, and a tuple of such elements in the general case. These considerations might have cryptographic applications.

4 Tangent Gaussian circles

4.1 Gaussian circles through a given point

Proposition 16 *:*

Let $a, b, c, d \in \mathbb{Z}[i]$ such that $ad - bc = 1$ (the fractions $\frac{a}{c}$ and $\frac{b}{d}$ are thus irreductible)

The Gaussian circles through $\frac{b}{d}$ have half-curvature $\mathfrak{Im}(\bar{c}d) + k|d|^2,\ k \in \mathbb{Z}$.

The Gaussian circles through $\frac{a}{c}$ have half-curvature $\mathfrak{Im}(\bar{c}d) + k|c|^2,\ k \in \mathbb{Z}$.

Proof Let $\mathcal{C}$ be a Gaussian circle through $\frac{b}{d}$ and $g = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL(2,\mathbb{Z}[i])$ such that $\mathcal{C} = g(\bar{R})$. Multiplying g on the right by some linear fractional substitution in $(P)SL(2,\mathbb{Z})$ if needed, one may assume that $\frac{b}{d} = g(0)$ *i.e.* $\frac{b}{d} = \frac{b'}{d'}$.

Multiplying the second column by $-1, i$ or $-i$ and the first one by $-1, -i$ or i, one may assume that $(b,d) = (b',d')$.

Then $(a',c') = (a,c) + \ell(b,d)$ avec $\ell \in \mathbb{Z}[i]$.

Hence $\mathcal{C}$ has half-curvature $\mathfrak{Im}(\bar{c}'d) = \mathfrak{Im}(\bar{c}d) + k|d|^2$ where $k = \mathfrak{Im}(\ell) \in \mathbb{Z}$. Conversely for all $k \in \mathbb{Z}$, setting $(a',c') = (a,c) + ik(b,d)$ one gets a Gaussian circle with half-curvature $\mathfrak{Im}(\bar{c}d) + k|d|^2$.

The other statement is proved by noticing that $\frac{a}{c} = g(1/0) = g(\infty)$. □

Definition 5 : Two distinct Gaussian circles $\mathcal{C}$ and $\mathcal{C}'$ tangent at some point z will be said **immediately tangent** if and only if there is no Gaussian circle tangent at z to both these circles and 'intermediary' between them.

More rigorously, let $p, q \in \mathbb{Z}[i]$ be coprime Gaussian integers such that $z = \frac{p}{q}$. Assume also that $\mathcal{C}$ and $\mathcal{C}'$ are oriented likewise if they are internally tangent, and oppositely if they are externally tangent. Let $g, g' \in SL(2,\mathbb{Z}[i]$ with same first column $\binom{a}{c}$ such that $g(\infty) = g'(\infty) = \frac{p}{q} = \frac{a}{c}$.

$\mathcal{C}$ and $\mathcal{C}'$ are immediately tangent if and only if $\mathfrak{Im}(\bar{c}d') = \mathfrak{Im}(\bar{c}d) \pm |c|^2$.

4.2 'Apollonism' criterium

Proposition 17 *:*

In the previous framework, let Q be the binary quadratic form $(p,q) \mapsto |pc+qd|^2 = |c|^2p^2 + 2\,\mathfrak{Re}(\bar{c}d)pq + |d|^2q^2$.

- *Q has discriminant $-4\,\mathfrak{Im}(\bar{c}d)^2$.*
- *Let m_1, m_2 be the first and second minima of Q on $\mathbb{Z}^2 \setminus \{(0,0)\}$, i.e. m_1 is the minimum of the squared moduli of non zero elements of the 'lattice of denominators' of $\mathcal{C}$, and choosing a point (p_1,q_1) where m_1 is reached by Q, m_2 is the minimum of Q on $\mathbb{Z}^2 \setminus \mathbb{Z}(p_1,q_1)$. Let $Q' : (p',q') \mapsto m_1p'^2 + b'p'q' + m_2q'^2$ be the reduced form of Q and $T \in SL(2,\mathbb{Z})$ such that*

$$Q(p,q) = Q(p',q') \text{ where } \begin{pmatrix} p \\ q \end{pmatrix} = T \begin{pmatrix} p' \\ q' \end{pmatrix}$$

(see Appendix A concerning the reduction of positive definite integer binary quadratic forms)

Set $T = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \in SL(2,\mathbb{Z})$ and $g' = g \circ T$. Since $\mathcal{C} = g(\bar{\mathbb{R}}) = g(T(\bar{\mathbb{R}})) = g'(\bar{\mathbb{R}})$, the point $\frac{ap+bq}{cp+dq} = g'(1/0) = g'(\infty)$ is a rational point of $\mathcal{C}$ with squared denominator modulus m_1, hence minimal.

- *The circle $\mathcal{C}'' = g''(\bar{\mathbb{R}})$ with g'' derived from g' by subtracting to its second column the first one multiplied by $+i$ (respectively : $-i$) if the curvature of $\mathcal{C}$ is non negative (respectively : non positive) is a Gaussian circle which is immediately tangent to $\mathcal{C}$, with minimal (respectively : maximal)* **relative** *curvature among the Gaussian circles immediately tangent to $\mathcal{C}$.*
- *The* **absolute** *curvature of $\mathcal{C}''$ is smaller than the absolute curvature of $\mathcal{C}$.*

Proof :

The proofs of all these statements but the last one are straightforward.

Assume for example that $\mathcal{C}$ has non negative half-curvature $\mathfrak{Im}(\bar{c}d) = \mathfrak{Im}(\bar{c'}d')$.

Since Q' is reduced, its discriminant satisfies

$$4\,\mathfrak{Im}(\bar{c'}d'))^2 = -\Delta = 4m_1m_2 - b'^2 \geq 4m_1^2 - m_1^2 = 3m_1^2 = 3|c'|^4$$

Thus, since $\mathfrak{Im}(\bar{c'}d'') = \mathfrak{Im}(\bar{c'}d') - |c'|^2$,

$$-\mathfrak{Im}(\bar{c'}d') < \left(1 - \frac{2}{\sqrt{3}})\right) \mathfrak{Im}(\bar{c'}d') \leq \mathfrak{Im}(\bar{c'}d') - |c'|^2 = \mathfrak{Im}(\bar{c'}d'') < \mathfrak{Im}(\bar{c'}d')$$

hence $|\,\mathfrak{Im}(\bar{c'}d'')| < |\,\mathfrak{Im}(\bar{c'}d')|$. □

Remark 7 :

If $\mathcal{C}$ and $\mathcal{C}''$ have curvatures of the same sign then they are internally tangent, otherwise they are externally tangent.

In case of external tangency, absolute curvature is divided by at least $3 + 2\sqrt{3}$.

Remark 8 :

Most times $m_1 \neq m_2$ and the quadratic form Q reaches its minimum at two opposite couples of integers, *e.g.* there are exactly two non zero points in the lattice of denominators of $\mathcal{C}$ at minimum distance to zero, et these denominators are opposite of each other. The corresponding numerators are also opposite and an unique point of tangency is obtained on $\mathcal{C}$.

Sometimes, $m_1 = m_2$, and then 4 points are obtained on the lattice of denominators, that correspond to two points on $\mathcal{C}$.

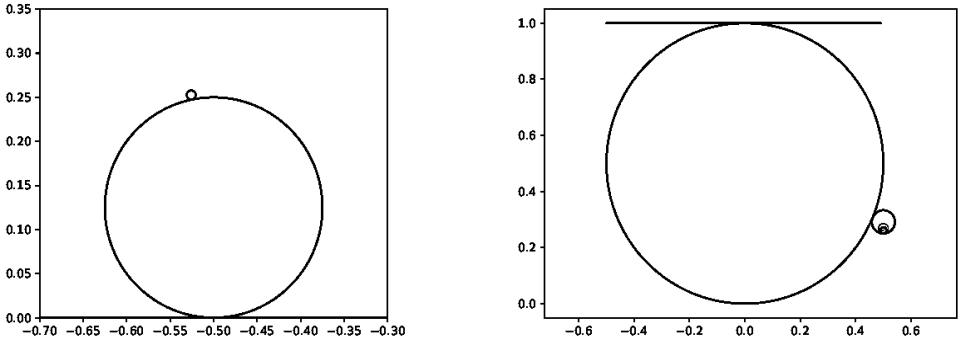

Fig. 4 Apollonism (on the left) - Non apollonism (on the right) of the smallest circle

Theorem 18 *(apollonism criterium) :*

Let $\mathcal{C}$ be a Gaussian circle located in the band $0 \leq y \leq 1$.

Iterating the process of the previous proposition, a finite sequence of Gaussian circles located in the same band is obtained, such that each circle (but the first) is immediately tangent to its predecessor, with absolute curvature lower than the absolute curvature of its predecessor. The last circle has zero curvature so is one of the lines $y = 0$ or $y = 1$.

The Gaussian circle $\mathcal{C}$ is Apollonian if and only if each circle but the first in the sequence described above is externally tangent to its predecessor, i.e. the curvature of any two successive circles have opposite sign.

Proof : Let $(\mathcal{C}_0 = \mathcal{C}, \mathcal{C}_1, \ldots, \mathcal{C}_n = \mathcal{D})$ be the sequence of Gaussian circles described above, where $\mathcal{D}$ is one of the lines $\mathbb{R}$ or $\mathbb{R} + i$.

Let $i < n$ such that $\mathcal{C}_i$ is Apollonian. Then $\mathcal{C}_{i+1}$ is externally tangent to $\mathcal{C}_i$.

Let us prove that $\mathcal{C}_{i+1}$ is Apollonian. If this does not hold, then $\mathcal{C}_{i+1}$ is part of the disk limited by some Gaussian circle $\mathcal{C}'$ with absolute curvature strictly lower than the absolute curvature of $\mathcal{C}_{i+1}$. Since $\mathcal{C}_i$ is Apollonian, $\mathcal{C}'$ is exterior or equal to $\mathcal{C}_i$, and thus $\mathcal{C}', \mathcal{C}_i$ and $\mathcal{C}_{i+1}$ are tangent at the same point, but this contradicts the minimality of the absolute curvature of $\mathcal{C}'$ among the Gaussian circles tangent to $\mathcal{C}_i$.

Hence by induction all the circles in our sequence are Apollonian, each one but the first being externally tangent to its predecessor.

The converse implication is proved *ad absurdum*. Assume that $\mathcal{C}$ is not Apollonian and that each circle but the first is externally tangent to its predecessor.

Since $\mathcal{C}$ is not Apollonian; it is interior to some Gaussian circle $\mathcal{C}'$ of absolute curvature strictly lower than the absolute curvature of $\mathcal{C}$. For each $i < n$, $\mathcal{C}_i$ is interior to $\mathcal{C}'$ since otherwise, selecting minimal i for which this property does not hold, $\mathcal{C}_{i-1}$ and $\mathcal{C}_i$ being tangent and on opposite sides of $\mathcal{C}'$, $\mathcal{C}'$ is tangent to $\mathcal{C}_{i-1}$, and this contradicts the definition of $\mathcal{C}_i$.

Hence $\mathcal{D}$ is interior to $\mathcal{C}'$ and therefore equal to $\mathcal{C}'$. Moreover, $\mathcal{C}$ is exterior to $\mathcal{D}$.

Hence $\mathcal{C}$ is both interior and exterior to $\mathcal{C}'$, thus equal to $\mathcal{C}'$, but these circles have different curvature. This is contradictory.

□

Algorithm 2 describes how to implement this apollonism criterium.

4.3 Algorithmic construction of Gaussian circles with bounded curvature

Proposition 19 *: Let $M \in \mathbb{N}$.*

Let $\mathcal{C} = g(\mathbb{R})$ be an oriented Gaussian circle (with $g \in SL(2, Z[i])$). Suppose that this circle has absolute half-curvature at most M. Then the Gaussian circles with absolute half-curvature at most M and immediately tangent to $\mathcal{C}$ meet $\mathcal{C}$ at points a/c ($a, c \in \mathbb{Z}[i]$) such that $|c|^2 \leq 2M$.

Proof : If $\mathcal{C}$ and $\mathcal{C}'$ are immediately tangent at (irreducible) a/c , the difference between their relative half-curvatures is $\pm|c|^2$. If moreover their absolute half-curvatures are at most M then $|c|^2 \leq 2M$. □

Proposition 20 *: Let $Q : (p, q) \mapsto m_1 p^2 + epq + m_2 q^2$ be a reduced definite positive integer binary quadratic form (see Appendix A). Then*

$$\forall (p, q) \in \mathbb{Z}^2,\ Q(p, q) \geq m_1 \frac{p^2 + q^2}{2}$$

Proof :

Let $(p, q) \in \mathbb{Z}^2$. Since $|e| \leq m_1 \leq m_2$,

$$Q(p, q) \geq m_1(p^2 - |pq| + cq^2) \geq m_1(p^2 - \frac{p^2 + q^2}{2} + q^2)$$

by arithmetico-geometric inequality.

□

Algorithm 3 gives the circles $\mathcal{C}'$ with bounded curvature immediately tangent to a given Gaussian circle $\mathcal{C}$.

It relies on the fact that if $\mathcal{C}$ and $\mathcal{C}'$ have relative half-curvatures $\not\gamma$ and $\not\gamma'$ between $-M$ and M, if $g = a, b//c, d$ is such that $\mathcal{C} = g(\hat{\mathbb{R}})$ and $(p, q) \mapsto |cp + dq|^2$ is reduced and if $\mathcal{C}$ and $\mathcal{C}'$ are immediately tangent at some rational point $(ap + bq)/(cd + dq) = g(p/q)$ then the denominator squared modulus $Q(p, q)$ satisfies (by the previous proposition):

$$2M \geq \pm(\not\gamma' - \not\gamma) = Q(p, q) \geq m_1 \frac{p^2 + q^2}{2}$$

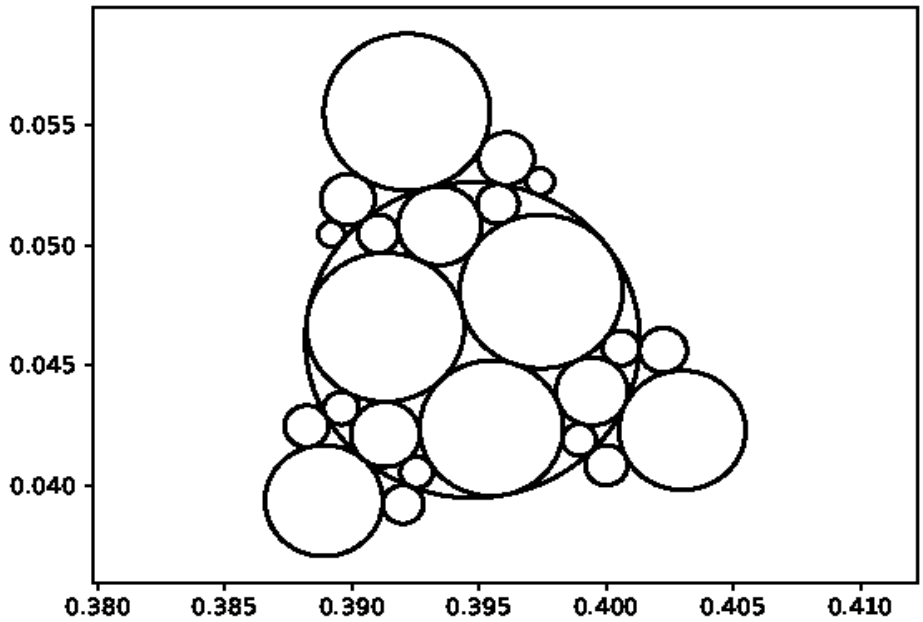

Fig. 5 Gaussian circles immediately tangent to the biggest one, with absolute half-curvature at most 1000 and not smaller than that of this circle

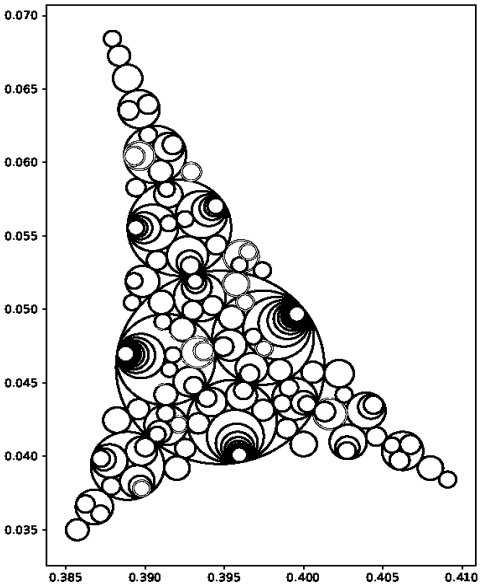

Fig. 6 Recursion of the previous algorithm, with the same initial circle (with half-curvature at most 1000)

In order to obtain all the Gaussian circles of bounded curvature transitively connected by immediate tangency (with non smaller curvature) to some Gaussian circle, one just uses recursively the previous algorithm. As curvature is only non-increasing in this process, cyclicity is avoided by recording matrices $G = g\bar{g}^{-1}$ (see subsection 3.4) of already calculated circles in a hash table. See Figure 6 and also Figure 2.

Conclusion

Some late bibliographical researches revealed this subject to be still an active one (see *e.g.* [3]) and some of our ideas might not be so new, yet we hope to have brought some contribution to the study of the (band-) Apollonian super-packing and its connection with the (band-) Apollonian packing.

References

[1] Stange, Katherine E., 'The Farey structure of the Gaussian integers', Asia Pacific Math Newsletter, 2 : 10-13 (2016)
[2] Buchmann, Johannes & Vollmer, Ulrich, 'Binary Quadratic Forms: An Algorithmic Approach', Springer, (2007)
[3] Kapovich, Michael & Kontorovich, Alex. (2021). 'On Superintegral Kleinian Sphere Packings, Bugs, and Arithmetic Groups', https://doi.org/10.48550/arXiv.2104.13838 (2021)

[4] Graham, Ronald L. & Lagarias, Jeffrey C. & Mallows, Colin L. &Wilks, Allan R. Yan,& Catherine H. , 'Apollonian Circle Packings: Geometry and Group Theory I. The Apollonian Group', https://doi.org/10.48550/arXiv.math/0010298 (2000)
[5] Graham, Ronald L. & Lagarias, Jeffrey C. & Mallows, Colin L. &Wilks, Allan R. Yan,& Catherine H. 'Apollonian Circle Packings: Geometry and Group Theory II. Super-Apollonian Group and Integral Packings', Discrete and computational geometry 35 :1–36 (2006)
[6] Weyl, Hermann, 'Elektron und Gravitation', Zeitschrift für Physik, 56 : 330–352 (1929)
[7] Hirst, K.E., 'The Apollonian packing of circles', J. Lond. Math. Soc. 42 : 281–291 (1967)

Appendix A reduction of positive definite integral binary quadratic forms

We follow here *verbatim* chapter 5 of [2] where the reader will find the motivations of the definitions and the proofs of of the results below, as well as considerations of complexity.

Definition 6 Let $Q : (x, y) \mapsto ax^2 + bxy + cy^2$ be a positive definite integral binary quadratic form.

Q is said *normal* if $-a < b \leq a$.

Q is said *reduced* if it is normal and ($a < c$ ou ($a = c$ et $b \geq 0$)).

Proposition 21 *If Q is reduced then $a = min_{(x,y)\in\mathbb{Z}^2\setminus\{(0,0)\}} Q(x, y)$.*

Proposition 22 *Consider the following functions :*

`rho` : $(Q, T) \mapsto (Q', T')$
where $Q' : (x', y') \mapsto cx'^2 + (-b + 2sc)x'y' + (cs^2 - bs + a)y'^2$ *(où* $Q : (x, y) \mapsto ax^2 + bxy + cy^2$ *is integral and positive definite)*
and $T' = T \begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix}$
where $s = \left\lfloor \frac{b+c}{2c} \right\rfloor$

`normalize` : $Q \mapsto (Q', U)$
where $Q' : (x', y') \mapsto ax'^2 + (b + 2sa)x'y' + (as^2 + bs + c)y'^2$
and $U = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$
where $s = \left\lfloor \frac{a-b}{2a} \right\rfloor$

`reduce` : $Q \mapsto (Q', T)$
where Q', T *are defined by*

$(Q', T) \leftarrow$ `normalize`(Q)
`while` Q' *is not reduced* `do` $(g, T) \leftarrow$ `rho`(g, T)

Then the funtion `reduce` *terminates, and* Q' *is reduced,* $T \in SL(2, \mathbb{Z})$ *and*

$$\forall (x, y) \in \mathbb{R}^2 \quad Q(x, y) = Q'(x', y') \text{ with } \begin{pmatrix} x \\ y \end{pmatrix} = T \begin{pmatrix} x' \\ y' \end{pmatrix}$$

In particular

$$min_{(x,y)\in\mathbb{Z}^2\setminus\{(0,0)\}} Q(x, y) = Q(p, q) \text{ where } \begin{pmatrix} p \\ q \end{pmatrix} = T \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ is the first column of } T$$

2 Algorithms derived from the present work

Algorithm 1 Calculates a list of representatives of points of $(\mathbb{Z}/n\mathbb{Z}[i])^*/(\mathbb{Z}/n\mathbb{Z})^*$, one for each

Require: $n > 0$
1: *Result* $\Leftarrow$ empty list
2: `append` i `to` *Result*
3: **for** $d|n$, $d \neq n$ **do**
4: *Sieve* $\Leftarrow$ boolean array of length n set to `False`
5: **for** $b = 0$ `to` $n - 1$ **do**
6: **if** `not` *Sieve*$[b]$ `and` $\gcd(d^2 + k^2, n) = 1$ **then**
7: `append` $d + ib$ `to` *Result*
8: **for** $k \in \{1, 1 + \frac{n}{d}, \ldots, 1 + (d - 1)\frac{n}{d}\}$ **do**
9: *Sieve*$[bk \bmod n] \Leftarrow$ `True`
10: **end for**
11: **end if**
12: **end for**
13: **end for**
14: `return` *Result*

Algorithm 2 Apollonism criterium

Require: $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}[i])$ that defines an oriented Gaussian circle $\mathcal{C} = g(\hat{\mathbb{R}})$ in the band $0 \leq y \leq 1$.

while $\mathcal{C}$ has non zero half-curvature $\mathfrak{Im}(\bar{c}d)$ **do**
  $Q \leftarrow$ the quadratic form $(x, y) \mapsto |xc + yd|^2$ associated to the lattice of denominators of $\mathcal{C}$
  $(Q', T) \leftarrow$ (the reduced form of Q and a matrix $T \in SL(2, \mathbb{Z})$ such that $Q(x, y) = Q'(x', y')$ where $\binom{x}{y} = T\binom{x'}{y'}$) ▷ see appendix A
  $g' \leftarrow gT$ ▷ $g'(\hat{\mathbb{R}}) = \mathcal{C}$ and $g'(\infty) = a'/c'$ has minimal denominator modulus among the rational points of $\mathcal{C}$
  if $\mathfrak{Im}(\bar{c}d) > 0$ **then** ▷ relative curvature to be lowered preserving $g'(\infty) = a'/c'$
    substract to the second column of g' its first column multiplied by i
  else
    add to the second column of g' its first column multiplied by i
  end if
  if the curvature of $g'(\hat{\mathbb{R}})$ has the same sign as that of $\mathcal{C}$ **then**
    return False
  else
    $g \leftarrow g'$
  end if
end while
return True

Algorithm 3 Circles immediately tangent to a given circle $\mathcal{C}$ with half-curvature at most M and not smaller than the half-curvature of $\mathcal{C}$

Require: $g \in SL(2,\mathbb{Z}[i])$ (defining a Gaussian oriented circle $\mathcal{C} = g(\hat{\mathbb{R}})$ in the band $0 \le y \le 1$, $M \ge 1$, $X > 0$)

if $\mathcal{C}$ is a (horizontal) line **then**
  return a list of g's corresponding to the circles tangents to this line at points with integer real part x such that $|x| \le X$ or at infinity and in the band $0 \le y \le 1$.
else
  $result \leftarrow$ empty list
  $g' \leftarrow$ a matrix in $SL(2,\mathbb{R})$ such that $g'(\hat{\mathbb{R}}) = \mathcal{C}$ and $(p',q') \mapsto |p'c' + q'd'|^2$ is reduced and equivalent to $(p,q) \mapsto |pc+qd|^2$
    ▷ see appendix A and Algorithm 2
  for $(p'_0, q'_0) \in \mathbb{N} \times \mathbb{Z}$ such that ${p'_0}^2 + {q'_0}^2 \le 4M/m_1$ where $m_1 = |c'|^2$ **do**
    if $Q'(p'_0, q'_0) \le 2M$ **then**
      $\not{\jmath} \leftarrow \mathfrak{Im}(\bar{c}d)$ $(= \mathfrak{Im}(\bar{c'}d'))$
      for $\varepsilon = \pm 1$ **do**
        if $|\not{\jmath}| \le |\not{\jmath} + \varepsilon m_1| \le M$ **then**
          $(r'_0, s'_0) \leftarrow$ a couple of integers such that $p'_0 s'_0 - q'_0 r'_0 = 1$
          $g'' \leftarrow g' \begin{pmatrix} p'_0 & r'_0 \\ q'_0 & s'_0 \end{pmatrix}$
            ▷ $g''(\hat{\mathbb{R}}) = \mathcal{C}$ and $g''(\infty) = (a'p'_0 + b'q'_0)/((c'p'0 + d'q'_0)$
          $g''' \leftarrow$ the matrix derived from g'' by adding εi times the first column of g'' to its second column
            ▷ adds $\varepsilon |c''|^2$ to half-curvature
          append g''' to result
        end if
      end for
    end if
  end for
  return result
end if