8-2006

On integral Apollonian circle packings

Sam Northshield
SUNY Plattsburgh

Recommended Citation
Northshield, S. (2006). On integral Apollonian circle packings. *Journal of Number Theory, 119* (2), 171-193.

PREPRINT
December 22 , 2002

ON APOLLONIAN CIRCLE PACKINGS

S. Northshield

Department of Mathematics, SUNY-Plattsburgh
Plattsburgh, NY 12901

Abstract. The curvatures of four mutually tangent circles with disjoint interior form what is called a Descartes quadruple. The four smallest curvatures of circles in an Apollonian circle packing form what is called a root Descartes quadruple and, if the curvatures are relatively prime, we say that it is a primitive root quadruple. We prove a conjecture of Mallows by giving a closed formula for the number of primitive root quadruples with minimum curvature -n.

An Apollonian circle packing is called strongly integral if every circle has curvature times center a Gaussian integer. The set of all such circle packings for which the center of the largest circle is in the unit square and for which curvature plus curvature times center is congruent to 1 modulo 2 is called the "standard super-gasket". These centers are in one-to-one correspondence with the primitive root quadruples and exhibit certain symmetries first conjectured by Mallows. We prove these symmetries; in particular, the centers are symmetric around $y = x$ if n is odd, around $x = 1/2$ if n is an odd multiple of 2, and around $y = 1/2$ if n is a multiple of 4.

1. Introduction.

A Descartes' quadruple is a set of four integers that satisfies Descartes' theorem for curvatures of four mutually tangent circles:

$$2(a^2 + b^2 + c^2 + d^2) = (a + b + c + d)^2.$$

Such a quadruple can be 'realized'; that is, one can construct four circles which are mutually tangent and whose curvatures agree with the four given numbers. Furthermore, one can form an Apollonian circle packing (uniquely) from four mutually tangent circles. By Descartes' theorem, it is easy to see that the curvatures of all circles in this packing are integral. The four smallest curvatures form a Descartes quadruple which we call a 'root quadruple'. Such a root quadruple is called 'primitive' if the four curvatures are relatively prime.

Let $N(n)$ be the number of primitive root quadruples for packings with minimum curvature $-n$. A test of the first 4800 natural numbers agrees with the following conjectural formula:

$$N(n) = \frac{1}{4}(n \prod_{p|n}(1 - \chi(p)/p) + 2^{\omega^*(n)+1}) \tag{1}$$

where $\chi(p) = (-1)^{\frac{p-1}{2}}$ or 0 according to whether p is odd or even respectively and $\omega^*(n)$ is the number of prime divisors of n if $n \not\equiv 2(\mod 4)$ and is 1 less than that if $n \equiv 2(\mod 4)$. This is indeed the case, and we shall prove the following:

Theorem 1. For $n > 1$, formula (1) holds.

AMS 1991 Subject Classification: Primary ; Secondary .
Key words and phrases: .

Outline of proof: The function $\hat{\phi}(n) = n\Pi_{p|n}(1 - \chi(p)/p)$ is similar to Euler's phi function $\phi(n) = n\Pi_{p|n}(1 - 1/p)$ and, in fact, the product of the two, $\phi^*(n) = \phi(n)\hat{\phi}(n)$, counts the number of Gaussian integers relatively prime to n and with both coordinates non-negative but less than n. We shall construct a function $\mathcal{C}$ which assigns to each Gaussian integer $x+iy$ with x and y relatively prime, a circle packing and show that

a) every reduced Apollonian quadruple with $a = -n$ is represented by some $\mathcal{C}(z)$,

b) the quadruple from $\mathcal{C}$ is primitive if and only if z and n are relatively prime in $\mathbb{Z}[i]$,

c) $\mathcal{C}(z)$ and $\mathcal{C}(w)$ yield the same quadruple if and only if $z = kuw$ or $ku\overline{w}$ for some unit u and non-zero integer k.

A careful counting then shows that formula (1) holds for $n > 1$.

The circle packings $\mathcal{C}(z)$ do not have integral curvature-centers (i.e., the product of curvature and center is not a Gaussian integer). However, we shall define a function f so that the 'shifted' packing $\mathcal{C}(z) + f(z)/n$ does have integral curvature centers. We say that $f(z)$ is the center of the corresponding shifted packings and that the packing $\mathcal{C}(z) + f(z)/n$ is a member of the "Standard Super Gasket" if it is arrived at via standard Möbius transformations of a certain fixed packing corresponding to the Descartes quadruple (0,0,1,1). Equivalently, the sum of the curvature and the curvature-center is congruent to 1 modulo 2 for every circle. It turns out that there is a one to one correspondence between such standard packings and the primitive Descartes quadruples. It was conjectured by Mallows that the centers of these packings obey certain symmetries:

Theorem 2. *Let C denote the set of all centers of packings in the standard super-gasket. If n is odd, then C is symmetric around $y = x$, if n is an odd multiple of 2, then C is symmetric around $x = 1/2$, and if n is a multiple of 4, then C is symmetric around $y = 1/2$.*

I thank my colleague Don West for showing me the numbers $N(n)$ for $n = 1, \ldots, 2500$,for checking the correctness of (1) for $n = 2, \ldots, 2400$, and for many discussions on this topic. I also thank Jeff Lagarias, Ronald Graham, and Colin Mallows for discussions on this material.

2. The Circle Packings $\mathcal{C}(z)$.

Throughout this section, we fix an odd integer $n > 1$. The equivalence $\equiv$ will mean congruence modulo n unless otherwise stated. We write $a \perp b$ for "a and b are relatively prime" and note that a Gaussian integer z is relatively prime to n if and only if $|z|^2 \perp n$.

Let $C(z, r)$ denote the circle with center z and radius r. Define, for $z \in Z[i]$,

$$C_z = C\left(\frac{z^2}{n(n + |z|^2)}, \frac{1}{n + |z|^2}\right).$$

Then C_0 is a circle centered at the origin with radius $1/n$ and, for any Gaussian integer z, C_z is a circle inside and tangent to C_0. We let $C_z \parallel C_w$ mean that the circles C_z and C_w are tangent.

Lemma 1. *For $z, w \in \mathbb{Z}[i]$, $C_z \parallel C_w$ if and only if $|Im(\overline{z}w)| = n$.*

Proof. Let $a = n + |z|^2$, $b = n + |w|^2$, and $m = Re(\overline{z}w)$. There exist positive real numbers R and θ such that $w = zRe^{i\theta}$. Then

$$m^2 + n^2 = |zw|^2 = (a-n)(b-n) = ab - na - nb + n^2$$

and so $m = \sqrt{ab - na - nb}$.

By the law of cosines, C_z and C_w are tangent if and only if

$$(\frac{1}{a} + \frac{1}{b})^2 = (\frac{1}{n} - \frac{1}{a})^2 + (\frac{1}{n} - \frac{1}{b})^2 - 2(\frac{1}{n} - \frac{1}{a})(\frac{1}{n} - \frac{1}{b})\cos 2\theta$$

which holds if and only if

$$\cos 2\theta = \frac{m^2 - n^2}{m^2 + n^2}. \tag{2}$$

Suppose (2) holds. Then $e^{2i\theta} = \dfrac{(m \pm in)^2}{m^2 + n^2}$ and it follows that $w^2/z^2 = R^2(m \pm in)^2$ and, since $|\overline{z}w|^2 = m^2 + n^2$, $(\overline{z}w)^2 = (m \pm in)^2$ and so $|Im(\overline{z}w)| = n$.

Conversely, suppose $|Im(\overline{z}w)| = n$. Since $|\overline{z}w|^2 = m^2 + n^2$, $Re(\overline{z}w) = \pm m$ and $(\overline{z}w)^2 = (m \pm in)^2$. Then $w^2/z^2 = R^2(m \pm in)^2$ and therefore (2) holds. □

We remark that C_z and C_w can not have centers with the same argument unless $z = \pm w$. Hence, given Gaussian integers z and w with $|Im(\overline{z}w)| = n$, the circles C_0, C_z, and C_w are mutually tangent and so define an Apollonian circle packing which we denote by $\mathcal{C}(z, w)$. For any a, b such that $a \perp b$, $C_{az+bw} \in \mathcal{C}(z, w)$.

We write $x \perp y$ for 'x and y are relatively prime' and define $\mathbb{Z}[i]^*$ to be the set of Gaussian integers $x + iy$ for which $x \perp y$.

Given $z = x + iy \in \mathbb{Z}[i]^*$, there exist integers a and b such that $ax + by = 1$. Let $z_0 = -b + ia$ and define

$$\rho(z) = nz_0 - lz \tag{3}$$

where

$$l = \left[\frac{n(ay - bx)}{x^2 + y^2}\right].$$

Then $\rho(z)$ is the unique Gaussian integer such that $\overline{z}\rho(z) = m + in$ where $0 \le m < |z|^2$.

For $z = x + iy \in \mathbb{Z}[i]$ let $g = \gcd(x, y)$ and define

$$\mathcal{C}(z) = \mathcal{C}(z/g, \rho(z/g)).$$

Proposition 1. *The circle packing $\mathcal{C}(z)$ generated by $z \in Z[i]^*$ is primitive if and only if $z \perp n$.*

Proof. If ξ is a [Gaussian] prime which divides both z and n, then, by (3), $\xi|\rho(z)$. Hence, ξ divides the curvatures of the circles C_0, C_z, and $C_{\rho(z)}$ and so, by Descartes' formula for curvatures, ξ divides every curvature in $\mathcal{C}(z)$ and so $\mathcal{C}(z)$ is not primitive.

If $z \perp n$, then $|z|^2 + n \perp n$ and thus the curvatures of C_0 and C_z are relatively prime. Therefore $\mathcal{C}(z)$ is primitive. □.

Every primitive Descartes quadruple may be represented by some $\mathcal{C}(z)$. We shall show this in two steps. First, given a Descartes quadruple $(-n, a, b, c)$, we find Gaussian integers z and w such that $a = n + |z|^2$, $b = n + |w|^2$, and $Im(\overline{z}w) = n$

and, therefore, $(-n, a, b, c)$ is represented by $\mathcal{C}(z, w)$. Then, secondly, we shall show that any such $\mathcal{C}(z, w)$, there exists z_0 such that $\mathcal{C}(z, w) = \mathcal{C}(z_0)$. We start with three lemmas

Lemma 2. *If $m \perp n$ and $d|(m^2 + n^2)$, then $\exists x, y \in \mathbb{Z} : (x + iy)|(m + in)$ and $x^2 + y^2 = d$.*

Proof. If $p|(m^2 + n^2)$ and $p \equiv 3(\mod 4)$, then p is prime in $Z[i]$. Then p divides both $m \pm in$ and so divides both m and n; contradicting $m \perp n$. Thus d is a product of primes each of which is a product $\xi^j\overline{\xi}^j$ of primes in $Z[i]$. Since $m + in$ is not divisible by both ξ and $\overline{\xi}$ (otherwise $m - in$ is also and so $m \not\perp n$), we may assume $\xi^j|(m+in)$. Let $x+iy$ be the product of all such ξ^j. Then $d = x^2+y^2$ and $(x + iy)|(m + in)$. □

This can be extended further to where m and n are not relatively prime.

Lemma 3. *If $d|(m^2 + n^2)$ where gcd(n, d, $\frac{m^2+n^2}{d}$)=1, then there exist integers x, y such that $(x + iy)|(m + in)$ and $x^2 + y^2 = d$.*

Proof. Let $g = \gcd(m, n)$, $g_1 = \gcd(g, d)$, and $g_2 = \gcd(g, d')$, where $d' = (m^2 + n^2)/d$. Then $g = g_1g_2$ and $g_1 \perp g_2$. Let $\hat{m} = m/g$, $\hat{n} = n/g$, $\hat{d} = d/g_1^2$, and $\hat{d'} = d'/g_2^2$. Then $\hat{m} \perp \hat{n}$ and $\hat{m}^2 + \hat{n}^2 = \hat{d}\hat{d'}$. Hence $\hat{d}|(m^2 + \hat{n}^2)$ and, by Lemma 2, there exist $\hat{x}$ and $\hat{y}$ such that $\hat{x}^2 + \hat{y}^2 = \hat{d}$ and $(\hat{x} + i\hat{y})|(\hat{n} + i\hat{m})$. Let $x = \hat{x}g_1$ and $y = \hat{y}g_1$. Then $(x + iy)|(n + im)$ and $x^2 + y^2 = d$. Let $s + it = \frac{n+im}{x+iy}$. Then $s^2 + t^2 = d'$ and $(x + iy)(s + it) = n + im$. □

Lemma 4. *Every primitive root quadruple is represented by some $\mathcal{C}(z, w)$.*

Proof. Suppose $(-n, a, b, c)$ is a Descartes quadruple. Define $z_0 = 0$, $z_1 = \frac{1}{n} - \frac{1}{a}$, and $z_2 = (\frac{1}{n} - \frac{1}{b})e^{i\theta}$ for some angle such that the circles with centers z_0, z_1, and z_2 are mutually tangent. By Descartes' theorem, $c = a + b - n \pm \sqrt{ab - na - nb}$ and so there exists an integer m such that $m^2 = ab - na - nb$. By the law of cosines,

$$(\frac{1}{a} + \frac{1}{b})^2 = (\frac{1}{n} - \frac{1}{a})^2 + (\frac{1}{n} - \frac{1}{b})^2 - 2(\frac{1}{n} - \frac{1}{a})(\frac{1}{n} - \frac{1}{b})\cos\theta$$

and, solving for the cosine, we may assume m satisfies

$$e^{i\theta} = \frac{(m + in)^2}{m^2 + n^2}.$$

Let $d = a - n$. Then, since

$$m^2 + n^2 = (a - n)(b - n),$$

$d|(m^2+n^2)$ and, since the quadruple is primitive, the hypothesis of Lemma 3 holds and there exist x, y such that $(x + iy)|(m + in)$ and $x^2 + y^2 = d$. Let $z = x - iy$, $e^{i\phi} = \frac{z^2}{|z|^2}$, and $w = \frac{m+in}{x+iy}$. Then

$$naz_1e^{i\phi} = z^2$$

and

$$nbz_2e^{i\phi} = w^2.$$

It then follows that $\mathcal{C}(z,w)$ is a rotation, by the angle ϕ, of the circle packing constructed above. □

It turns out that z need not be relatively prime to n and so one cannot write $\mathcal{C}(z,w)=\mathcal{C}(z)$. With some work, we may get around this problem.

Proposition 2. *Every primitive root quadruple is represented by some $\mathcal{C}(z)$.*

Proof. It is enough to show that every primitive $\mathcal{C}(z,w)$ is of the form $\mathcal{C}(z_0)$. Let g=gcd$(|z|^2, 2\langle w,z\rangle, |w|^2)$. If $\mathcal{C}(z,w)$ is primitive, then $g \perp n$. Let F be the primitive quadratic form $F(a,b)=|az+bw|^2/g$. By Hua [H: Ch. 12, lemma 2], there exist relatively prime integers a and b such that $F(a,b)\perp n$ or, equivalently, $az+bw\perp n$. Let $z_0=az+bw\perp n$. Since $a\perp b$, there exist integers c,d such that $ad-bc=1$. Let $w_0=cz+dw$. Then $Im(\overline{z_0}w_0)=(ad-bc)Im(\overline{z}w)=n$ and, since $C_{z_0}, C_{w_0}\in\mathcal{C}(z,w)$, $\mathcal{C}(z,w)=\mathcal{C}(z_0,w_0)$.

Suppose $z_0=x+iy$ and $w_0=u+iv$. Since $|Im(\overline{z_0}w_0)|=n$, then $xv-yu=n$ and, since $z_0\perp n$, there exist a,b,c such that $ax+by+cn=1$. Hence $(a+cv)x+(b-cu)y=1$ and thus $x\perp y$. Again, since $xv-yu=n$, $\overline{z_0}(w_0-\rho(z_0))$ is real and thus $w_0-\rho(z_0)$ is a real multiple of z_0. Since $x\perp y$, there exists an integer k such that $kz_0-w_0-\rho(z_0)$ and thus $C_{z_0,w_0}\in\mathcal{C}(z_0)$ and the result follows. □

We next investigate when two circle packings are the same.

Proposition 3. *For $z,w\perp n$ and in $\mathbb{Z}[i]^*$, the following are equivalent:*
a) $\mathcal{C}(z)=\mathcal{C}(w)$,
b) $\exists k\in\mathbb{Z}: w\equiv kz(\mod n)$,
c) $n|Im(\overline{z}w)$,
d) $\exists A\in SL_2(\mathbb{Z}): A\binom{z}{\rho(z)}=\binom{w}{\rho(w)}$.

Proof. ($a\Rrightarrow b$). Let $\mathcal{C}(z)=\mathcal{C}(w)$. Then $C_w\in\mathcal{C}(z)$ and so there exist integers a and b such that $w=az+b\rho(z)$. By (2), $\rho(z)+lz\equiv 0$. Let $k=a-bl$. Then $kz=az-blz\equiv az+b\rho(z)=w$.

($b\Rrightarrow c$). Let $kz\equiv w$. Then $k|z|^2\equiv\overline{z}w$ and therefore $Im(\overline{z}w)\equiv 0$.

($c\Rrightarrow d$). Define $z_1\sim z_2$ if and only if $Im(\overline{z_1}z_2)\equiv 0$. This is an equivalence relation. By definition of ρ, $z\sim\rho(z)$ and $w\sim\rho(w)$. If $Im(\overline{z}w)\equiv 0$, the $z\sim w$ and so $w\sim\rho(z)$, $z\sim\rho(w)$, and $\rho(z)\sim\rho(w)$. If $z=x+iy$, $w=x'+y'$, $\rho(z)=t+is$, and $\rho(w)=t'+is'$, then

$$x's-y't, y'x-x'y, s'x-t'y, t's-s't\in n\mathbb{Z}$$

and so the matrix

$$A=\frac{1}{n}\begin{pmatrix}x' & y'\\ t' & s'\end{pmatrix}\begin{pmatrix}s & -y\\ -t & x\end{pmatrix}$$

has integer entries. By the definition of ρ, the matrices $\left(\begin{smallmatrix}x & y\\ t & s\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}x' & y'\\ t' & s'\end{smallmatrix}\right)$ each have determinant n and so A has determinant 1 and

$$A\left(\begin{smallmatrix}x & y\\ t & s\end{smallmatrix}\right)=\left(\begin{smallmatrix}x' & y'\\ t' & s'\end{smallmatrix}\right).$$

($d\Rrightarrow a$). Let $A=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in SL_2(\mathbb{Z})$ and suppose $A\binom{z}{\rho(z)}=\binom{w}{\rho(w)}$. Then $a\perp b$, $c\perp d$, $az+b\rho(z)=w$, and $cz+d\rho(z)=\rho(w)$. Therefore $C_w, C_{\rho(w)}\in\mathcal{C}(z)$ and thus $\mathcal{C}(z)=\mathcal{C}(w)$. □

The restriction that z and w each have relatively prime coordinates can be partly removed in the theorem above.

Corollary 1. *For $z, w \perp n$, $\mathcal{C}(z) = \mathcal{C}(w)$ if and only if there exists an integer k such that $w \equiv kz(\mod n)$.*

Proof. Choose integers g, h so that $\frac{z}{g}, \frac{w}{h} \in \mathbb{Z}[i]^*$. Then $g, h \perp n$ since $z, w \perp n$ and so g and h have multiplicative inverses modulo n.

If $\mathcal{C}(z) = \mathcal{C}(w)$, then $\mathcal{C}(\frac{z}{g}) = \mathcal{C}(\frac{w}{h})$ and so, by Proposition 2, there exists an integer k such that $\frac{w}{h} \equiv k\frac{z}{g}$. Hence there exists an integer, $l = g^{-1}kh$, such that $w \equiv lz$.

Conversely, if $w \equiv lz$, then $gw \equiv glz \equiv (glh^{-1})hz$. Hence $\frac{w}{h} \equiv (glh^{-1})\frac{z}{g}$ and thus $\mathcal{C}(z) = \mathcal{C}(z/g) = \mathcal{C}(w/h) = \mathcal{C}(w)$. □

3. Counting primitive root quadruples.

Let $S_n = \{x + iy : 0 \leq x, y < n, x^2 + y^2 \perp n\}$ and T denote the set of circle packings. By Corollary 1,

$$\mathcal{C} : S_n \to T$$

is a $\phi(n)$-to-1 mapping.

The cardinality of S_n is a sort of totient function.

Lemma 5. $|S_n| = n\phi(n)\prod_{p|n}(1 - \chi(p)/p)$.

Proof. A prime p is either congruent to $1, 2$, or 3 modulo 4, and, in each of these cases, it is easy to verify that

$$|S_p| = (p - 1)(p - \chi(p)).$$

Next, we claim that for $n > 1$,

$$|S_{p^{n+1}}| = p^2|S_{p^n}|$$

which follows from fact that $a + ib \perp p^n$ if and only if $a + p^n + ib \perp p^{n+1}$. Hence the lemma holds for prime powers. Finally, the proof that ϕ^* is multiplicative follows the classical proof that ϕ is multiplicative as in [3, Th. 61]. □

Example. Consider the case where n=15. There are eight distinct root Descartes quadruples:

$$(-15, 16, 240, 241)$$
$$(-15, 24, 40, 49)$$
$$(-15, 17, 128, 128)$$
$$(-15, 20, 60, 65)$$
$$(-15, 25, 40, 40)$$
$$(-15, 28, 33, 40)$$
$$(-15, 32, 32, 33)$$
$$(-15, 24, 41, 44)$$

.

We shall abbreviate them by the numbers 241,49,128,65,40',40,33,and 44 respectively. Note that only the quadruples represented by 40' and 65 are not primitive.

The table below contains $128 = \phi^*(15)$ entries.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0		241	241		241			241	241			241		241	241
1	241	128			33	44	40			40	44	33			128
2	241		128	40		44		33	33		44		40	128	
3			40			49		40	40		49			40	
4	241	33			128	44	40			40	44	128			33
5		44	44	49	44		49	44	44	49		44	49	44	44
6		40			40	49					49	40			40
7	241		33	40		44		128	128		44		40	33	
8	241		33	40		44		128	128		44		40	33	
9		40			40	49					49	40			40
10		44	44	49	44		49	44	44	49		44	49	44	44
11	241	33			128	44	40			40	44	128			33
12			40			49		40	40		49			40	
13	241		128	40		44		33	33		44		40	128	
14	241	128			33	44	40			40	44	33			128

Note that all 6 primitive root quadruples are represented in the table. For example, '33' occurs 16 times and '44' occurs 32 times. Let

Since $\mathcal{C}(1+4i)$ corresponds to '33', so do $\mathcal{C}(2+8i), \mathcal{C}(4+i), \mathcal{C}(7+13i), \mathcal{C}(8+2i), \mathcal{C}(11+14i), \mathcal{C}(13+7i)$, and $\mathcal{C}(14+11i)$ (by equation (3)). Let $U(n)$ denote the set of units in $\mathbb{Z}/n\mathbb{Z}$, and let $[z] = zU(n)$. Hence $8 = \phi(15)$ occurences of '33' come from $[1+4i]$ and the other eight occurences of '33' come from $[1+11i]$.

As for '44', its 32 occurences come from $[5+i], [5+2i], [2+5i]$, and $[1+5i]$. The factor of 2 in the difference of the two cases comes from the fact that $[1+4i] = [4+i]$ and so there are really only 2 equivalence classes for '33' but 4 for '44'.

Using this example as a guide, we count. Given any $x+iy$ for which $\mathcal{C}$ is defined, it is clear that $x-iy, -x+iy, -x-iy, y+ix, y-ix, -y+ix$, and $-y-ix$ give congruent, but not necessarily identical, circle packings under the map $\mathcal{C}$. Furthermore, the only congruent packings arise in this way. Clearly, multiplication by -1 preserves identity, so only four classes of packings are possible.

Given $z \in S_n$, we say z is of "type 1" if $[z] = [\overline{z}]$, "type 2" if $[z] = [i\overline{z}]$, "type 3" if $[z] = [iz]$, and "type 0" otherwise.

Proposition 4. Let $z = x + iy \in S_n$, and $n > 1$.

a) z is type 1 if and only if $n|2xy$.
b) z is type 2 if and only if $n|(x^2 - y^2)$.
c) z is type 3 if and only if $n|(x^2 + y^2)$.
d) There are no type 3 elements in S_n.
e) No $z \in S_n$ is both type 1 and type 2.
f) If n is odd, then, in S_n, there is a one-to-one correspondence between elements of type 1 and elements of type 2.
g) If n is even, then there are no elements of type 2.

Proof.

a) Suppose z is type 1. Then there exists k such that $kx \equiv x$ and $ky \equiv -y$. Hence $xy \equiv kxy \equiv -xy$ and so $2xy \equiv 0$. Conversely, suppose $2xy \equiv 0$. Without loss of generality, we may assume that y is odd and thus $2x \perp y$. Let x_0=gcd$(2x, n)$ and y_0=gcd(y, n). Since $x \perp y$ (since, otherwise, gcd(n,x,y)$\neq 1$), $x_0 y_0 = n$ and $x_0 \perp y_0$. By the Chinese Remainder Theorem, there exists k such that $k \equiv 1($ mod $y_o)$ and $k \equiv -1($ mod $x_0)$ from which it follows that $kz \equiv \overline{z}$.

b) Let $[x + iy] = [y + ix]$. Then there exists k such that $kx \equiv y$ and $ky \equiv x$ and so $x^2 \equiv kxy \equiv y^2$. Conversely, if $x^2 \equiv y^2$, then $x \perp n$ and $y \perp n$ and so $x, y \in U(n)$. Hence, there exists k such that $kx \equiv y$.

c) This is virtually the same as for part (b).

d) Since $x + iy \perp n$ implies $x^2 + y^2 \perp n$, $n|(x^2 + y^2)$ is impossible.

e) If $x + iy$ is both type 1 and type 2, and $p|n$,then $p|xy$ (so either $p|x$ or $p|y$) and $p|(x^2 - y^2)$. This is impossible since, if $p|x$, then $p|y$ and gcd(n,x,y)$\neq 1$.

f) Consider the map $\tau(x + iy) = Res_n((x - y) + i(x + y))$. If $x + iy$ is type 2, then $n|(x^2 - y^2)$ and thus $n|2(x - y)(x + y)$ and $\tau(x + iy)$ is type 1. Similarly, if $x + iy$ is type 1, then $n|2xy$ and thus $n|((x - y)^2 - (x + y)^2)$ and $\tau(x + iy)$ is type 2. It is easy to verify that, since n is odd, τ is one-to-one. The result follows.

g) If n is even and z is type 2, then $x^2 - y^2$ is even and, since $z \in S_n$, x and y must both be odd. Since

$$2a + 1 + i(2b + 1) = (1 + i)(a + b + 1 + i(b - a)),$$

it follows that $(1 + i)$ is a common divisor of both z and n; a contradiction. □

We write $z \approx w$ if $z = uw$ or $z = u\overline{w}$ for some unit u in $\mathbb{Z}[i]$. Then $|\bigcup_{w \approx z} [w]| = 4\phi(n)$ or $2\phi(n)$ according to whether z is type 0 or not. Let T_0, T_1, and T_2 denote the number of distinct primitive root quadruples corresponding to types 0,1, and 2 respectively. For example, when $n = 15$, we have $T_0 = |\{`40', `44'\}| = 2$ $T_1 = |\{`241', `49'\}| = 2$, and $T_2 = |\{`33', `128'\}| = 2$.

It follows that $N(n) = T_0 + T_1 + T_2$ and $\phi^*(n) = (4T_0 + 2T_1 + 2T_2)\phi(n)$ and, therefore

$$N(n) = \frac{1}{4}\hat{\phi}(n) + T_1$$

if n is odd and

$$N(n) = \frac{1}{4}\hat{\phi}(n) + \frac{1}{2}T_1$$

if n is even. Let $\omega(n)$ denote the number of distinct prime divisors of n. Theorem 1 then follows from:

Lemma 6. *If $n > 1$ is not divisible by 4, then $T_1 = 2^{\omega(n)-1}$. If n is divisible by 4, then $T_1 = 2^{\omega(n)}$.*

Proof. Given $x + iy \in S_n$ of type 1 (i.e., $n|2xy$), let

$$F(x + iy) = \{\gcd(x, n), \gcd(y, n)\}.$$

If $4 \not| n$ then $n|xy$ [obvious if n is odd; follows from fact that either x or y is even (as in proof of Proposition 4g) if n is even]. Hence $F(x + iy)$ is a factorization of n into two relatively prime factors. The number of such factors is clearly $2^{\omega(n)-1}$

(the $2^{\omega(n)}$ is the number of ways to choose a subset from the set of prime factors of n, the "-1" is due to discarding the order). If $4|n$, then either $n|xy$ in which case $F(x+iy)$ is a factorization of n into two relatively prime factors or $n \not| xy$ in which case $\frac{n}{2}|xy$ and $F(x+iy)$ is a factorization of $\frac{n}{2}$ into two relatively prime factors. The number of such factorizations of n and of $\frac{n}{2}$ are equal and so the total number of factorizations is $2^{\omega(n)}$.

It is enough to show that z and w of type 1 give congruent packings if and only if $F(z) = F(w)$.

Let $x+iy$ and $u+iv$ give rise to congruent packings. Since both are type 1, there exists $k \perp n$ such that either $k(x+iy) = (u+iv)$ or $k(x+iy) = v+iu$. Without loss of generality, we may assume the first. Then $kx \equiv u(\mod n)$ and $ky \equiv v(\mod n)$ which implies, since $k \perp n$ that $F(x+iy) = F(u+iv)$.

Conversely, suppose $F(x+iy) = F(u+iv)$. In one case, we may define a and b so that a= gcd(x,n)=gcd(u,n) and b=gcd(y,n)=gcd(v,n). Then there exist integers l_1, l_2, l_3, l_4 such that $x = al_1, u = al_2, y = bl_3$, and $v = bl_4$. Furthermore, $l_1 \perp b, l_2 \perp b, l_3 \perp a$, and $l_4 \perp a$. By the Chinese Remainder Theorem, there exists k such that

$$kl_2 \equiv l_1(\mod b) \text{ and } kl_4 \equiv l_3(\mod a)$$

from which it follows that $k(u+iv) \equiv (x+iy)(\mod n)$ and therefore $u+iv$ and $x+iy$ give the same packing. In the other case, the u and v switch roles and $u+iv$ and $x+iy$ give congruent packings. □.

4. Strongly Integral Apollonian Packings

Given a circle in the complex plane, we call the product of curvature and the center the *curvature-center*. We say that a circle packing is "strongly integral" if every circle in it has curvature-center a Gaussian integer. A remarkable fact, first noted in [1], is that Descartes formula holds true for curvature-centers of four mutually tangent circles just as it does for just the curvatures. Hence, if three mutually tangent circles in a circle packing have integral curvature-centers, then all circles in that packing do.

A packing constructed in the previous section is, generally, not strongly integral. However, a translation of the packing is. Assuming $z \perp n$, there exists an integer a such that $a|z|^2 \equiv 1$ and thus, if $w = -az^2$, then the curvature-center of $C_z + \frac{w}{n}$ is $w + \frac{z^2 + w|z|^2}{n}$, a Gaussian integer. This motivates the definition of $f(z)$ as $Res_n(-az^2)$ unless $2xy/n$ is an odd integer in which case we let $f(z) = Res_n(-az^2) + in$. The reason for this technical detail will become apparent later. In any case, for all $z \perp n$,

$$z^2 + f(z)|z|^2 \equiv 0.$$

We now determine a condition which implies $f(z) = f(w)$.

Lemma 7. *Let $z, w \perp n$. $f(z) \equiv f(w)$ if and only if $n|2Im(\overline{z}w)$. If $n|Im(\overline{z}w)$ then $f(z) = f(w)$.*

Proof. $f(z) \equiv f(w)$ if and only if $z + f(w)\overline{z} \equiv 0$ if and only if $z\overline{w} + f(w)\overline{z}\overline{w} \equiv 0 \equiv \overline{z}(w + f(w)\overline{w})$ if and only if $z\overline{w} \equiv w\overline{z}$.

Let $n|Im(\overline{z}w)$, then $f(z) \equiv f(w)$ and thus, if $n \nmid xy$, then $f(z) = f(w)$. Let $x+iy = z$ and $u+iv = w$. Then $xv \equiv yu$ and, if $n|xy$, then $n|(x^2+y^2)uv$ and thus $n|uv$. Therefore, in this case, $f(z) = f(w)$. □

Proposition 5. *For $z \perp n$, $\mathcal{C}(z) + \frac{f(z)}{n}$ is strongly integral.*

Proof. Let $g = gcd(Re(z), Im(z))$ and $z' = z/g$. By Lemma 7, $f(z) = f(z')$. By the complex Descartes formula, since $\mathcal{C}(z) = \mathcal{C}(z', \rho(z'))$,it is enough to show that $C_w + \frac{f(z)}{n}$ is strongly integral where $w = 0, z', \rho(z')$. The first two are trivial; let $w = \rho(z')$. Since $C_w||C_{z'}$, $Im(\overline{z}'w) = n$ and, by Lemma 7, $f(z) = f(w)$. The result follows. □.

The complex number $f(z)/n$ is the center of the largest circle in the circle packing $\mathcal{C}(z)$ shifted so as to be strongly integral. We call it the "center" of the circle packing $\mathcal{C}(z)$.

The definition of f depends on n and, if necessary, we will write f_n for f if n is not clear from the context. It turns out that the centers 'almost' uniquely define the circle packings.

Proposition 6. *If for some $z \perp n$ and $w \perp m$, $\frac{f_n(z)}{n} = \frac{f_m(w)}{m}$ then $m = n$.*

Proof. By the hypothesis,

$$n^2|f_m(w)|^2 = m^2|f_n(z)|^2.$$

Since $|f_m(w)|^2 \equiv 1(\mod m)$ and $|f_n(z)|^2 \equiv 1(\mod n)$, there exist integers k_1, k_2 such that $n^2(1+k_1m) = m^2(1+k_2n)$ and so $n^2 - m^2 = (k_2n - k_1m)nm$. Let $g = gcd(m,n)$. Then $gmn|(n^2-m^2)$ from which it follows that $gm|n^2$ and $gn|m^2$ and, therefore, $m = n$. □

It is possible, however, for $f(z) = f(w)$ but $\mathcal{C}(z) \neq \mathcal{C}(w)$. That is, by Proposition 3, the converse of the second part of Lemma 7 is not true. For example, $n = 10$, $z = 1$, and $w = 2+5i$ has $f(z) = f(w) = 9$ but $Im(\overline{z}w) = 5$. Such examples necessarily have n even.

Following [2], we define the integral Apollonian super-gasket to be the set of all primitive strongly integral Descartes configurations. An element of the gasket can be thought of as a 4-by-2 matrix where each row represents one of four mutually tangent circles and is of the form

$$(c \; a+ib)$$

where c is the curvature and $a+ib$ the curvature-center of the circle. Hence, the first column forms a Descartes quadruple and the second column forms a complex Descartes quadruple. Given n and $z, w \perp n$ where $|Im(\overline{z}w)| = n$, an example of such a matrix is

$$M(z,w) = \begin{pmatrix} -n & -f(z) \\ n+|z|^2 & f(z)+g(z) \\ n+|w|^2 & f(z)+g(w) \\ n+|z+w|^2 & f(z)+g(z+w) \end{pmatrix} \tag{4}$$

where

$$g(z) = \frac{z^2 + f(z)|z|^2}{n}.$$

We say that a Gaussian integer z is *oe* if $Re(z)$ is odd and $Im(z)$ is even. We define ee, eo, and oo similarly.

Of special interest is the *standard super-gasket* which is the set of elements in the integral super-gasket for which all the row sums are *oe*. An example of such a matrix is:

$$\begin{pmatrix} -15 & -10-6i \\ 28 & 19+12i \\ 33 & 22+12i \\ 40 & 25+16i \end{pmatrix}.$$

We say that two elements of the super-gasket are *equivalent* if the circle packings determined by the two elements are the same. We say that w is the *curvature-center* of an element M of the super-gasket if w is the curvature-center of the corresponding circle packing. Given three mutually tangent circles, there are exactly two other circles each tangent to the three. Given a Descartes quadruple, one can 'reduce' it by replacing the curvature of one circle by the (smaller) curvature of the dual circle. If sufficiently reduced so that one of the curvatures is negative, then the curvature-center corresponding to that negative curvature is the center of the packing.

We say that $M(z, w)$ is *proper* if every row sum is *oe*. The first two rows of the matrix $M(z, w)$ depend only on z and n and themselves form a matrix. We define

$$m(z) = \begin{pmatrix} n & f(z) \\ n + |z|^2 & f(z) + g(z) \end{pmatrix}.$$

We say that $m(z)$ is proper if and only its row sums are *oe*. Let

$$S = \{f(z) : z \perp n \text{ and } m \text{ is proper}\}.$$

Lemma 8. *If n is odd, then $m(z)$ is proper if and only if $f(z)$ is ee. If n is even, then $m(z)$ is proper if and only if $g(z)$ is oe.*

Proof. Suppose n is odd. If $m(z)$ is proper, then $n + f(z)$ is *oe* and so $f(z)$ is *ee*. Conversely, if $f(z)$ is *ee*, then $n + f(z)$ is *oe* and, since $|z|^2 + g(z) = (z^2 + (n + f(z))|z|^2)/n$ is *ee*, $n + |z|^2 + f(z) + g(z)$ is *oe*.

Suppose n is even. Then $|z|^2$ is odd (since $z \perp n$). If $m(z)$ is proper, then $f(z)$ is *oe*, $f(z) + g(z)$ is *ee*, and thus $g(z)$ is *oe*. Conversely, if $g(z)$ is *oe*, then $f(z)$ is *oe* since $z^2 + f(z)|z|^2 = ng(z)$ is *ee*, z^2 is *oe*, and $|z|^2$ is odd. Hence, $n + f(z)$ and $n + |z|^2 + f(z) + g(z)$ are *oe*. □

Lemma 9. *If $z, w \perp n$, $m(z)$ is proper, and $n|Im(\overline{z}w)$, then $m(w)$ is proper.*

Proof. Suppose n is odd. Since $f(z) = f(w)$, then, by Lemma 8, $m(w)$ proper.

Suppose n is even. By Proposition 3, $\exists k \perp n : w \equiv kz$ and thus $w = kz + nz_0$ for some Gaussian integer z_0. Since $f(w) = f(z)$,

$$g(w) \equiv k^2 g(z) (\mod 2).$$

Hence, if $m(z)$ is proper, then $g(z)$ is *oe* and thus, since k is odd, $g(w)$ is *oe* and $m(w)$ is proper. □

Proposition 7. *S coincides with the set C of curvature-centers of the standard super-gasket which have coordinates between 0 and n inclusive.*

Proof. We first show $S \subset C$. Suppose $z \perp n$ with $m(z)$ proper. Since $f(z) = f(\frac{z}{g})$, we may assume, without loss of generality, that $z \in \mathbb{Z}[i]^*$ and there exists w $(=\rho(z))$ such that $\mathcal{C}(z) = \mathcal{C}(z, w)$. Then the 4x3 matrix in (4) is in the integral super-gasket and, by Lemma 9, is in the standard super-gasket.

Now we show $C \subset S$. Given curvature-center w of an element of the standard super-gasket, let $\mathcal{C}$ denote the circle packing that element determines. It is enough to show that $w = f(z)$ for some $z \perp n$. By Proposition 2, every Descartes quadruple is represented by some $\mathcal{C}(z_0)$ where $z_0 \perp n$. Let $a = n + |z_0|^2$. Then a is in the first column of some element of the super-gasket equivalent to the given element. Necessarily, $a \perp n$.

Let $\frac{w}{n}$ be the center of $\mathcal{C}$. The circle corresponding to a then has center $\frac{w}{n} + (\frac{1}{n} - \frac{1}{a})e^{i\theta}$ for some θ. Hence

$$\frac{aw}{n} + \frac{a-n}{n}e^{i\theta}$$

is a Gaussian integer. Since $e^{i\theta} \in \mathbb{Q}[i]$,

$$e^{i\theta} = z_1^2/|z_1|^2$$

for some $z_1 \in \mathbb{Z}[i]$. Since

$$0 \equiv aw + (a-n)e^{i\theta} \equiv |z_0|^2 w + |z_0|^2 \frac{z_1^2}{|z_1|^2}, \tag{5}$$

it follows that

$$z_1^2 + w|z_1|^2 \equiv 0. \tag{6}$$

It remains to show that $z_1 \perp n$ since then (6) implies

$$z_1 + w\overline{z_1} \equiv 0 \equiv z_1 + f(z_1)\overline{z_1}$$

and thus $w = f(z_1)$.

If n is even, then w is *oe*. Let $r + is = z_1$. We may assume that r and s are not both even. If they are both odd, then 4 divides $r^2 - s^2$ but not $r^2 + s^2$ and thus $Re(z_1^2|z_0|^2/|z_1|^2)$ is even which contradicts (5). Hence $|z_1|^2$ is odd and it follows that $2rs \perp r^2 + s^2$ and thus $|z_1|^2$ divides $|z_0|^2$ and, because $z_0 \perp n$, $z_1 \perp n$.

If n is odd, then w is *ee*. Arguing as above, $\gcd(2rs, r^2 + s^2)$ is either 1 or 2 and therefore $|z_1|^2$ divides $2|z_0|^2$ and thus $z_1 \perp n$. □

It turns out, though we won't prove it here, that the set S is in one-to-one correspondence with the set of primitive reduced Descartes quadruples with least curvature $-n$.

5. Symmetries.

Mallows conjectured [5] that the centers of the circle packings corresponding to the standard super gasket obey the following symmetries:

a) around $y = x$ when n is odd,

b) around $x = \frac{1}{2}$ when n is an odd multiple of 2,

c) around $y = \frac{1}{2}$ when n is a multiple of 4.

We shall prove this (i.e., Theorem 2) through three propositions. As above, let

$$S = \{f(z) : m(z) \text{ proper}\}$$

.

Proposition 8. *For n odd, if $z \in S$, then $i\overline{z} \in S$.*

Proof. if $m(z)$ is proper, then $m((1+i)\overline{z})$ is proper. Note that

$$[(1+i)\overline{z}]^2 + i\overline{f(z)}|(1+i)\overline{z}|^2 = 2i\overline{z^2 + f(z)|z|^2} \equiv 0$$

and thus

$$f((1+i)\overline{z}) = i\overline{f(z)}.$$

Assuming $m(z)$ is proper, then by Lemma 8, $f(z)$ is ee. Then $f((1+i)\overline{z})$ is ee and, again by Lemma 8, $m((1+i)\overline{z})$ is proper. □

Suppose now that n is even. If $z \perp n$, then, necessarily, $Re(z) \not\equiv Im(z)(\mod 2)$ and thus $|z|^2$ is odd and both z^2 and $f(z)$ are oe.

Let $w = \frac{n}{2}(1+i)$. If $u + iv = f(z)$ then, since $1 + v \pm u$ is even,

$$w + f(z)\overline{w} \equiv \frac{n}{2}((1+v+u) + i(1+v-u)) \equiv 0.$$

Hence,

$$(w+z) + f(z)(\overline{w} + \overline{z}) \equiv 0$$

and thus $f(z) \equiv f(z+w)$. Since $2xy/n$ is an odd integer (and, necessarily, $4|n$) if and only if $2(x+\frac{n}{2})(y+\frac{n}{2})/n$ is an odd integer, $f(z) = f(w+z)$. Since, if $x+iy = z$,

$$\frac{(z+w)^2 + f(z+w)|z+w|^2}{n} = \frac{z^2 + f(z)|z|^2}{n} + (x-y) + (f(z)+i)(x+y) + w,$$

$g(z+w) - g(z) - w$ is eo.

Proposition 9. *If n is an odd multiple of 2 and $z \in S$, then $n - \overline{z} \in S$.*

Proof. Since $z + f(z)\overline{z} \equiv 0$,

$$i\overline{z} + f(i\overline{z})\overline{i\overline{z}} \equiv 0 \equiv i\overline{(z + f(z)\overline{z})}$$

and so $f(i\overline{z}) \equiv -\overline{f(z)}$. Since $Re(f(z))$ is odd,

$$f(i\overline{z} + w) = f(i\overline{z}) = n - \overline{f(z)}.$$

Then

$$g(i\overline{z}) = \frac{(i\overline{z})^2 + f(i\overline{z})|i\overline{z}|^2}{n} = \frac{-\overline{z}^2 + (n - \overline{f(z)})|z|^2}{n} = |z|^2 - \overline{g(z)}.$$

If $g(z)$ is oe, then $g(i\overline{z})$ is ee and thus, since w is oo, $g(i\overline{z}+w)$ is oe. By Lemma 8, if $m(z)$ is proper, then so is $m(i\overline{z}+w)$. □

Proposition 10. *If n is a multiple of 4 and $z \in S$, then $in + \overline{z} \in S$.*

Proof. Since $z + f(z)\overline{z} \equiv 0$,

$$\overline{z} + \overline{f(z)}z \equiv 0 \equiv \overline{z} + f(\overline{z})z$$

and so $f(\overline{z}) \equiv \overline{f(z)}$. Since, when $n|2xy$,

$$\frac{1}{n}Im((\overline{z}+w)^2) \not\equiv \frac{1}{n}Im(z^2)(\mod 2)$$

,

$$f(\overline{z}+w) = f(\overline{z}) = in + \overline{f(z)}.$$

Then

$$g(\overline{z}) = \frac{\overline{z}^2 + f(\overline{z})|\overline{z}|^2}{n} = i|z|^2 + \overline{g(z)}.$$

If $g(z)$ is oe, then $g(\overline{z})$ is ee and thus, since w is ee, $g(\overline{z}+w)$ is oe. By Lemma 8, if $m(z)$ is proper, then so is $m(\overline{z}+w)$. □

REFERENCES

[1] J.C. Lagarias, C.L. Mallows, A.R. Wilks, *Beyond the Descartes Circle Theorem*, American Math. Monthly 109 (2002), no. 4, 338–361.
[2] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.R. Yan, *Apollonian Circle Packings: Geometry and Group Theory II. Super-Apollonian Group and Integral Packings*, preprint, 1/24/01.
[3] G.H.Hardy, E.M Wright, "An introduction to the theory of numbers, Fifth edition", Oxford University Press, New York, 1979.
[4] L.K. Hua, "Introduction to number theory", Springer, New York, 1982.
[5] C.L. Mallows, personal communication.

E-mail address : samuel.northshield@plattsburgh.edu