A Geometric Representation of Integral Solutions of $x^2 + xy + y^2 = m^2$

Abstract

More than a century ago, Norman Anning conjectured that it is possible to arrange 48 points on a circle, such that all distances between the points are integer numbers and are all among the solutions of the diophantine equation

$$x^2 + xy + y^2 = 7^2 \cdot 13^2 \cdot 19^2 \cdot 31^2.$$

We shall obtain Anning's conjecture as a consequence of a far more general geometrical result.

key-words: quadratic diophantine equations, quadratic forms, plane integral point sets

2010 Mathematics Subject Classification: **11D09** 11H55 52C10

1 A conjecture of Anning

In 1915, Norman Anning presented in [2] (see Figure 1) an arrangement of 12 points on a circle whose mutual distances are all integer numbers and miraculously all among the solutions of the diophantine equation

$$x^2 + xy + y^2 = 7^2 \cdot 13^2. \tag{1}$$

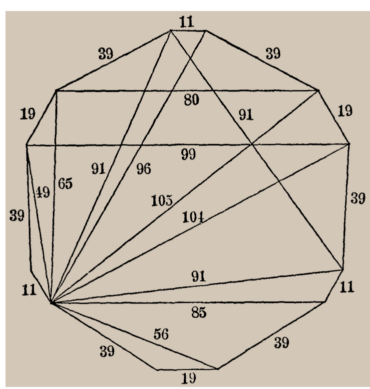

Figure 1: Anning's chordal dodecagon with integer sides and integer diagonals.

In fact, there are exactly 13 different distances which occur between vertices of Anning's chordal dodecagon, namely $11, 19, 39, 49, 56, 65, 80, 85, 91, 96, 99, 104, 105$. Surprisingly, these numbers all show up in the list of integer solutions of (1), which is, up to sign and order, $(49, 56)$, $(39, 65)$, $(19, 80)$, $(11, 85)$, $(0, 91)$, $(-11, 96)$, $(-85, 96)$, $(-19, 99)$, $(-80, 99)$, $(-39, 104)$, $(-65, 104)$, $(-49, 105)$, $(-56, 105)$. Similarly (see Figure 2), Anning gave a corresponding configuration of 24 points on a circle, whose 40 mutual distances appear as solutions of

$$x^2 \pm xy + y^2 = 7^2 \cdot 13^2 \cdot 19^2.$$

Observe, that it actually suffices to consider only the plus sign in the equation as we shall see later. Finally (see Figure 2), this led Anning to the conjecture, that it is possible to arrange 48 points on a circle, such that the distances between the points are all integral and among the solutions of the diophantine equation

$$x^2 + xy + y^2 = 7^2 \cdot 13^2 \cdot 19^2 \cdot 31^2.$$

In like manner 40 integers which occur among the solutions of

$$x^2 \pm xy + y^2 = 7^2 \cdot 13^2 \cdot 19^2$$

may be exhibited as the sides and diagonals of a cyclic 24-gon. The sides in order are: 96, 361, 299, 209, 249, 209, 299, 361, 96, 361, ...

That a study of

$$x^2 + xy + y^2 = 7^2 \cdot 13^2 \cdot 19^2 \cdot 31^2$$

would yield a similar 48-gon is probable.

Figure 2: Anning's conjecture.

At first glance, it is not clear how Anning found his geometric arrangments of points on a circle and why there is a relation to the integral solutions of $x^2 + xy + y^2 = \square$. The aim of this paper is to provide a geometrical proof of a very general result (Theorem 1), which covers in particular Anning's conjecture. Our proof is explicit and allows to actually construct such chordal polygons with $3 \cdot 2^n$ vertices. We will also show that not only all distances of the vertices occur as solutions of a corresponding diophantine equation, but also vice versa, that all positive integers which are solutions of the diophantine equation will occur as distances between the vertices of the polygon (see Corollary 10).

Before we start, we should add a few remarks about plane integral point sets in general: Configurations of points in the plane with integer mutual distance have been studied by numerous authors in the past. Such a set is called *plane integral point set*. The Erdős-Anning theorem states that an infinite number of points in the plane can have mutual integer distances only if all points lie on a straight line. This theorem has been proved in [3]. By using Pythagorean triangles it is easy to see that any *finite number* of points can be arranged in the plane such that all of them except one are collinear, and such that all distances are integers. In [11], a plane heptagon forming an integral point set is constructed such that, no three of its vertices lie on a line, and no four on a circle. The problem of the minimum diameter of n points in the plane in general position with integer mutual distances is discussed in [12]. Plane integral point sets of n points on a circle are considered in [9] and [8], the constructions, however, do not make contact to the diophantine equation $x^2 + xy + y^2 = \square$. Now, our main result is the following:

THEOREM 1. *For any integer $n \in \mathbb{N}$, one can arrange $3 \cdot 2^n$ points on a circle such that their mutual distances are among the solutions of the diophantine equation*

$$x^2 + xy + y^2 = p_1^2 \cdot p_2^2 \cdot \ldots \cdot p_n^2 \,, \tag{2}$$

where the p_i are different prime numbers of the form $6k+1, k \in \mathbb{N}$.

REMARK 2. Recall that by Dirichlet's theorem there are infinitely many primes in the arithmetic progression $6k+1, k \in \mathbb{N}$.

An algebraic proof of a generalisation of THEOREM 1, which, however, does not reveal the geometric content of the problem and does not connect the distances of the points on the circle with the solutions of the diophantine equation $x^2 + xy + y^2 = \square$, can be found in Bat-Ochir [4, Theorem 3], or in a less general form in Harborth, Kemnitz, Möller [10, Theorem 1]. Before we prove THEOREM 1, we consider the algebraic and geometric aspect of Anning's problem.

2 Algebraic point of view

In this section, we briefly discuss the diophantine equation $x^2 + xy + y^2 = m^2$. To keep the notation short, we introduce the following terminology: For a pair of integers (a, b) we write $(a, b)_q$ to denote that a and b satisfy the equation

$$a^2 + ab + b^2 = q. \tag{3}$$

Trivially, we have $(a, b)_q \implies (b, a)_q$ and $(a, b)_q \implies (-a, -b)_q$. Moreover, by Vieta's formulas we have $(a, b)_q \implies (a, -(a + b))_q$. This leads to the following observation:

REMARK 3. The alternating group A_4 operates on the set of solutions of (3). The orbit of a solution (a, b) is

$$\{\pm(a, b), \pm(b, a), \pm(a, -(a + b)), \pm(b, -(a + b)), \pm(-(a + b), a), \pm(-(a + b), b)\}.$$

Now, for two pairs of integers (a, b) and (c, d), we define

$$(a, b) * (c, d) := (ad - bc, ac + bc + bd).$$

LEMMA 4. *Let a, b, c, d, q_1, q_2 be integers such that $(a, b)_{q_1}$ and $(c, d)_{q_2}$. Then*

$$\big((a, b) * (c, d)\big)_{q_1 q_2},$$

in other words, we have

$$(ad - bc, ac + bc + bd)_{q_1 q_2}.$$

Proof. Let $A := ad - bc$ and $B := ac + bc + bd$. It is elementary to check the factorization

$$A^2 + AB + B^2 = (a^2 + ab + b^2) \cdot (c^2 + cd + d^2) = q_1 q_2.$$

q.e.d.

Notice that we can exchange a and b, or c and d, or both, which gives us

$$(bd - ac, ac + ad + bc)_{q_1 q_2}, \quad (ac - bd, ad + bc + bd)_{q_1 q_2}, \quad (bc - ad, ac + ad + bd)_{q_1 q_2}.$$

The following fact is just a consequence of Dickson [6, Exercises XXII.2, p. 80] (see also Cox [5, Chapter 1]).

FACT 5. *Let $p_1 < p_2 < \ldots < p_n$ be primes, where for $1 \leq i \leq n$ we have $p_i \equiv 1 \mod 6$, and let $m = \prod_{i=1}^{n} p_i$. Then the number of positive, integral solutions of*

$$x^2 + xy + y^2 = m^2$$

is $\frac{3^n - 1}{2}$ (where (x, y) and (y, x) are counted as one solution). In particular, if $n = 1$ and $p \equiv 1 \mod 6$, then the solution in positive integers $0 < x < y$ of

$$x^2 + xy + y^2 = p^2$$

is unique.

Notice that by LEMMA 4, if $p \equiv 1 \mod 6$ and $(a, b)_p$ with $a > b > 0$, then $(a^2 - b^2, 2ab + b^2)_{p^2}$, *i.e.*, $x = a^2 - b^2$ and $y = 2ab + b^2$ is the unique solution in positive integers of the equation $x^2 + xy + y^2 = p^2$.

EXAMPLES. In order to illustrate the previous results, we give a few examples:

- From $(2, 1)_7$ we obtain $(3, 5)_{7^2}$.
- From $(23, 120)_{(7 \cdot 19)^2}$ we obtain $(23 \cdot 13, 120 \cdot 13)_{(7 \cdot 13 \cdot 19)^2}$.
- From $(7, 8)_{13}$ and $(23, 120)_{(7 \cdot 19)^2}$ we obtain $(656, 1305)_{(7 \cdot 13 \cdot 19)^2}$.

3 Geometric point of view

Let ABC be an equilateral triangle with sides of length m, and let K be its circumcircle. Furthemore, let P be a point on the shorter arc over the chord $\overline{AB}$ (see Figure 3).

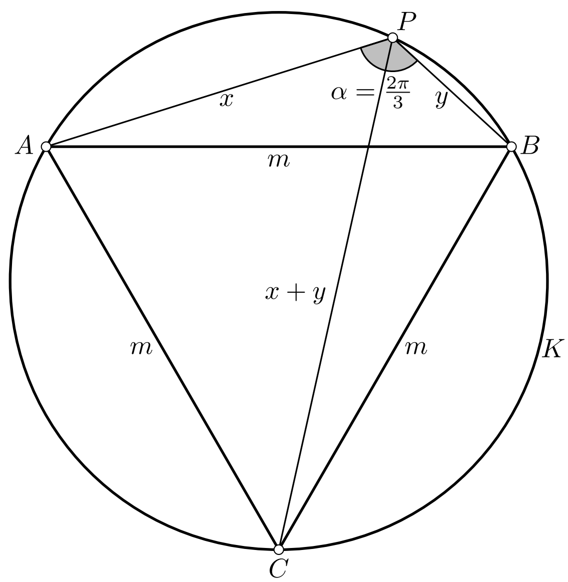

Figure 3: Geometric interpretation of the equation $x^2 + xy + y^2 = m^2$.

By the law of cosines we have

$$m^2 = x^2 + y^2 - 2xy\cos(\alpha) = x^2 + xy + y^2. \tag{4}$$

Vice versa, for each solution of $x^2 + xy + y^2 = m^2$ in positive real numbers x, y there is a point P on the shorter arc over $\overline{AB}$ with distances x and y from A and B, respectively. Moreover, by Ptolemy's theorem applied to the cyclic quadrilateral $ACBP$, we have that the length of $\overline{PC}$ is $x + y$. In this sense, we can geometrically read off from P the entire orbit of the solution (x, y) of (4) under A_4 (see Remark 3). We obtain:

Lemma 6.

(a) Let K be the circumcircle of the equilateral triangle ABC of side length $|AB| = m$. If P is a point on the smaller arc over $\overline{AB}$ (including A and B) such that $a = |PA| \in \mathbb{N}$, $b = |PB| \in \mathbb{N}$, then $(a, b)_{m^2}$. Moreover, $c := |PC| = a + b \in \mathbb{N}$ and $(\pm a, \mp c)_{m^2}$ and $(\pm b, \mp c)_{m^2}$.

(b) Vice versa, let a, b be integers with $(a, b)_{m^2}$. Then, if $ab \geq 0$, there exists a point P on the shorter arc over $\overline{AB}$ such that $|PA| = |a|$ and $|PB| = |b|$. If $a < 0 < b$ and $|a| < b$, then there exists a point P on the shorter arc over $\overline{AB}$ such that $|PC| = b$, $|PA| = -a$ and $|PB| = a + b$. If $a < 0 < b$ and $|a| > b$, then there exists a point P on the shorter arc over $\overline{AB}$ such that $|PC| = -a$, $|PB| = b$ and $|PA| = -(a + b)$.

We now give a geometric interpretation of Lemma 4 by interpreting the algebraic expressions there as lengths of chords which occur by concatenating two chords (see Figure 4).

Proposition 7. *Suppose that the triangle with side lengths a, b, q_1, where $a, b < q_1$, has circumradius $\frac{q_1}{\sqrt{3}}$ and that the triangle with side lengths c, d, q_2, where $c, d < q_2$, has circumradius $\frac{q_2}{\sqrt{3}}$ (see Figure 4). Then, the circumcircle of the triangle with side lengths*

aq_2, cq_1 and $s = ac+ad+bc$ has radius $\frac{q_1 q_2}{\sqrt{3}}$. Moreover, if $cq_1 < aq_2$, then the circumcircle of the triangle with side lengths aq_2, cq_1 and $s = ad - bc$ has the same radius $\frac{q_1 q_2}{\sqrt{3}}$.

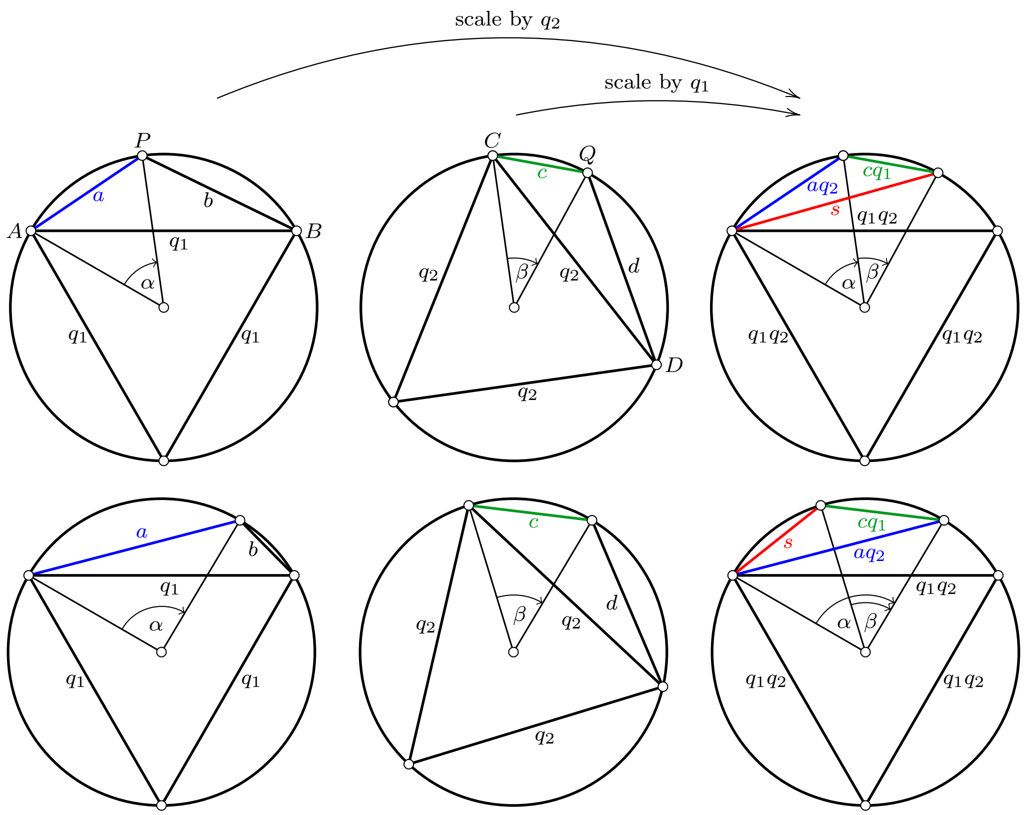

Figure 4: Adding solutions (top) and subtracting solutions (bottom).

Proof. The triangle with side lengths a, b, q_1 corresponds to $(a, b)_{q_1^2}$, and the triangle with side lengths c, d, q_2 corresponds to $(c, d)_{q_2^2}$ (see Figure 4, left and middle). By scaling the left configuration in Figure 4 by q_2, we get $(aq_2, bq_2)_{q_1^2 q_2^2}$, and by scaling the middle configuration in Figure 4 by q_1, we get $(cq_1, dq_1)_{q_1^2 q_2^2}$. In this way, we may consider the chords of length aq_2 and cq_1 in the circle of radius $r = \frac{q_1 q_2}{\sqrt{3}}$. By concatenating these chords in this circle we can "add" (top right in Figure 4) or "subtract" (bottom right in Figure 4) the chords. In order to determine the length s of the resulting chord, we use the angles

$$\alpha = 2 \arcsin \frac{aq_2}{2r} \quad \text{and} \quad \beta = 2 \arcsin \frac{cq_1}{2r}\,.$$

We find

$$\begin{aligned}
s &= 2r\sin\Big(\frac{\alpha\pm\beta}{2}\Big)\\
&= 2r\Big(\sin\frac{\alpha}{2}\cos\frac{\beta}{2}\pm\sin\frac{\beta}{2}\cos\frac{\alpha}{2}\Big)\\
&= aq_2\sqrt{1-\Big(\frac{c\sqrt{3}}{2q_2}\Big)^2}\pm cq_1\sqrt{1-\Big(\frac{a\sqrt{3}}{2q_1}\Big)^2}\\
&= \frac{a}{2}\sqrt{4q_2^2-3c^2}\pm\frac{c}{2}\sqrt{4q_1^2-3a^2}\\
&= \frac{a}{2}(c+2d)\pm\frac{c}{2}(a+2b).
\end{aligned}$$

For the plus sign, we obtain

$$s = ac + ad + bc$$

and for the minus sign

$$s = ad - bc.$$

q.e.d.

The length s of the resulting chord which we obtained by adding and subtracting chords of lengths aq_2 and cq_1 will be denoted by

$$aq_2 \oplus cq_1, \quad aq_2 \ominus cq_1.$$

Now we consider oriented angles α and β larger than $\frac{2\pi}{3}$. If, as in Figure 4, a and b continue to denote the distance from P to A and B, respectively, and c and b are the distances from Q to C and D, respectively, then the length of the resulting chord $s = aq_2 \oplus cq_1$ can be calculated in the same way as in the above proof. The result in the various cases is summarized in the diagram shown in Figure 5. In particular, we see that whenever a, b, c, d and q_1, q_2 are integers, s is a solution of the diophantine equation $x^2 + xy + y^2 = q_1^2 q_2^2$. For example, for $\frac{2\pi}{3} \le \alpha \le 2\pi$, $0 \le \beta \le \frac{2\pi}{3}$, $\alpha + \beta \le 2\pi$, we have by LEMMA 6 that $a^2 - ab + b^2 = q_1^2$ and $c^2 + cd + d^2 = q_2^2$. Then, indeed, for $s = ac + ad - bd$ and $t = -(ac + bd)$ we get $s^2 + st + t^2 = (a^2 - ab + b^2)(c^2 + cd + d^2) = q_1^2 q_2^2$.

DEFINITION 8. A chordal $(3 \cdot 2^n)$-gon which is symmetric with respect to a rotation with angle $2\pi/3$ about its center and whose vertices have integer mutual distances will be called *Anning polygon*. It is determined by a period of the sequence of the lengths $s_1, s_2, \ldots, s_{2^n}$ of consecutive chords. We will encode such an Anning polygon by $\mathscr{A}_n = \langle s_1, s_2, \ldots, s_{2^n}\rangle_m$, where m is the side length of the equilateral triangle with the same circumcircle as the polygon.

For example, the dodecagon in Figure 1 is an Anning polygon $\mathscr{A}_2 = \langle 11, 39, 19, 39\rangle_{91}$. Notice that this encoding is not unique.

4 Combining the algebraic and the geometric aspects

In this section, we first prove THEOREM 1 and then consider its refinements.

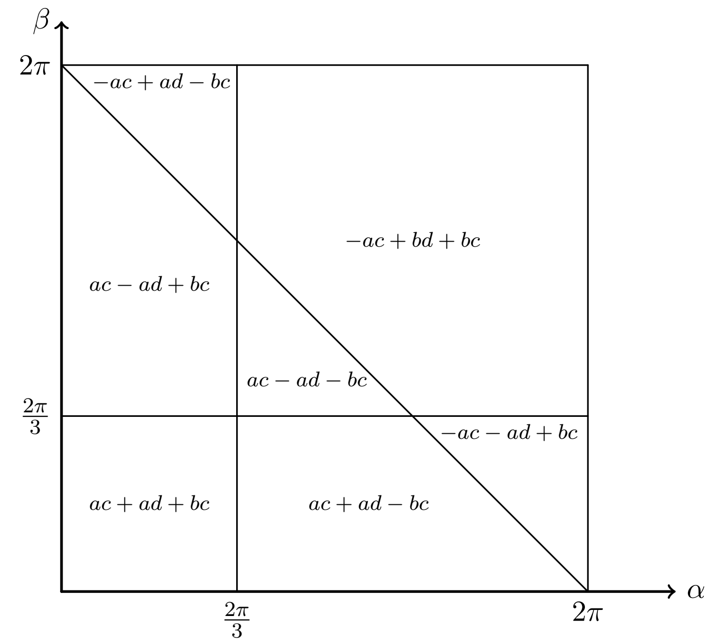

Figure 5: Length of the chord $s = aq_2 \oplus cq_1$.

Proof of Theorem 1. We have to show that for any integer $n \in \mathbb{N}$, one can arrange $3 \cdot 2^n$ points on a circle such that their mutual distances are among the solutions of the diophantine equation

$$x^2 + xy + y^2 = p_1^2 \cdot p_2^2 \cdot \ldots \cdot p_n^2\,,$$

where the p_i are different prime numbers of the form $6k+1$ (for some $k \in \mathbb{N}$).

The proof is by induction on n. For $n = 1$, we choose a prime number p_1 of the form $6k+1$ (for some $k \in \mathbb{N}$), for example, $p_1 = 7$. Then we choose positive integers s_1, s_2 such $s_1 < s_2 < p_1$ and $(s_1, s_2)_{p_1^2}$. Notice that by Fact 5, s_1 and s_2 are unique. For $p_1 = 7$ we have $s_1 = 3$ and $s_2 = 5$. Consider the circumcircle of the triangle with sides p_1, s_1, s_2. By rotating this triangle in its circumcircle by $2\pi/3$ and $4\pi/3$, we get an Anning Hexagon $\mathscr{A}_1 = \langle s_1, s_2\rangle_{p_1}$. In our example, shown in Figure 6, the occurring distances in $\mathscr{A}_1 = \langle 3, 5\rangle_7$ are $3, 5, 7, 8$ (see also Figure 3).

To illustrate the induction step, we first explicitly show the transition from $n = 1$ to $n = 2$: First, we choose a prime number p_2 of the form $6k+1$ (for some $k \in \mathbb{N}$) which is distinct from p_1, say $p_2 = 31$ (for $p_2 = 13$ we actually obtain Anning's original configuration shown in Figure 1). Then we choose the positive integers σ and τ such $\sigma < \tau < p_2$ and $(\sigma, \tau)_{p_2^2}$. For $p_2 = 31$ we have $\sigma = 11$ and $\tau = 24$. Now, for $i = 1, 2$ let $\bar{s}_i := s_i \cdot p_2$, and let $\bar{\sigma} := \sigma \cdot p_1$ and $\bar{\tau} := \tau \cdot p_1$. Notice that we have $(\bar{s}_1, \bar{s}_2)_{p_1^2 \cdot p_2^2}$ and $(\bar{\sigma}, \bar{\tau})_{p_1^2 \cdot p_2^2}$. Moreover, we obtain two Anning Hexagons $\mathscr{A}_1$ and $\mathscr{A}_1'$ with the same circumcircle where $\mathscr{A}_1$ is encoded by $\langle \bar{s}_1, \bar{s}_2\rangle_{p_1 \cdot p_2}$, and $\mathscr{A}_1'$ is obtained from $\mathscr{A}_1$ by a rotation through α, where

$$\alpha := 2 \arcsin \frac{\bar{\sigma}\sqrt{3}}{2p_1p_2} = 2 \arcsin \frac{\sigma\sqrt{3}}{2p_2}.$$

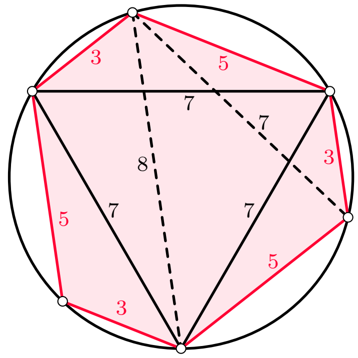

Figure 6: Anning Hexagon. Six points on a circle with integer mutual distances.

With a slight abuse of notation we encode $\mathscr{A}_1'$ by

$$\bar{\sigma} \oplus \langle \bar{s}_1, \bar{s}_2 \rangle_{p_1 \cdot p_2}.$$

For $p_1 = 7$ and $p_2 = 31$ we have $\bar{s}_1 = 3 \cdot 31$, $\bar{s}_2 = 5 \cdot 31$, and $\bar{\sigma} = 11 \cdot 7$. The two Anning Hexagons $\mathscr{A}_1$ and $\mathscr{A}_1'$ are illustrated in Figure 7:

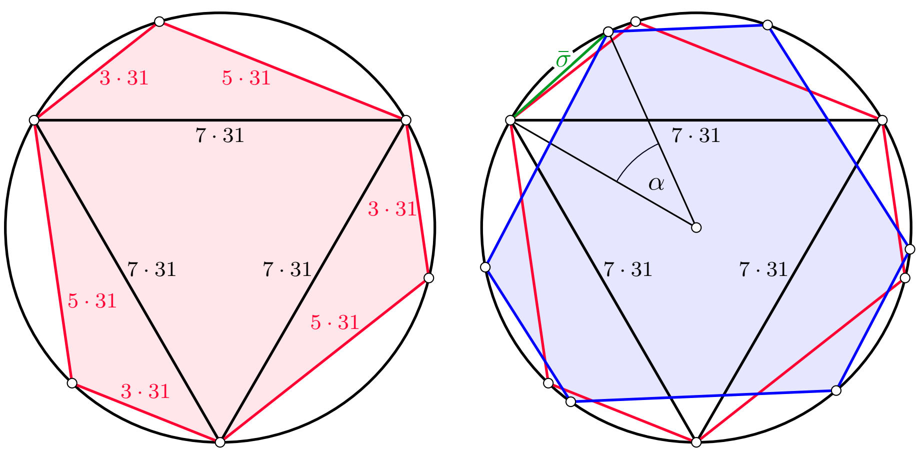

Figure 7: On the left: Anning Hexagon $\mathscr{A}_1$. On the right: Anning Hexagon $\mathscr{A}_1$ (red) and Anning Hexagon $\mathscr{A}_1'$ (blue) obtained from $\mathscr{A}_1$ by rotation angle α. Together, the vertices of $\mathscr{A}_1$ and $\mathscr{A}_1'$ form an Anning Dodecagon $\mathscr{A}_2$.

Claim 1. *The* 12 *vertices of the two hexagons* $\mathscr{A}_1$ *and* $\mathscr{A}_1'$ *are pairwise distinct.*

Otherwise, there would be two points of $\mathscr{A}_1$ such that the distance between these two points is $\bar{\sigma} = \sigma p_1 < p_1 p_2$. We show that this is impossible: Let $\bar{s}$ with $0 < \bar{s} < p_1 p_2$ be the distance between two points of $\mathscr{A}_1$. Then $\bar{s} = s p_2$ and there exists an integer t such that $0 < t < p_1$ and $(s,t)_{p_1^2}$. In particular, we have $p_1 \nmid s$, and since the primes p_1 and p_2 are distinct, $p_1 \nmid s p_2 = \bar{s}$. But since $p_1 \mid \bar{\sigma}$, this shows that $\bar{s} \neq \bar{\sigma}$.

Claim 2. *The distance x between any two of the 12 vertices is among the integral solutions of $x^2+xy+y^2=p_1^2p_2^2$.*

To see this, let P and Q be two of the 12 points. If P and Q both belong to the same Anning Hexagon, then, by construction, the distance between P and Q is an integral solutions of $x^2+xy+y^2=p_1^2p_2^2$. If P is a vertex of $\mathscr{A}_1$ and Q a vertex of $\mathscr{A}_1'$, then there is a vertex P' on $\mathscr{A}_1$ which, when rotated through α, becomes Q. In particular, the distance between P' and Q is $\bar\sigma=\sigma p_1$. The distance between P' and P is an integer ap_2. Thus, we get that the distance x between P and Q is $ap_2\oplus\sigma p_1$, and hence among the integral solutions of $x^2+xy+y^2=p_1^2p_2^2$.

The Anning Dodecagon which we obtain in this way can be encoded by $\langle s_1,s_2,s_3,s_4\rangle_{p_1\cdot p_2}$, where the s_i's are the lengths of the chords between the consecutive vertices of $\mathscr{A}_2$ over the chord of length p_1p_2.

For the general induction step, assume that for some pairwise distinct primes $p_1,\dots,p_n$ of the form $6k+1$ we have already constructed an Anning $(3\cdot 2^n)$-gon $\mathscr{A}_n$, which is encoded by $\langle s_1,s_2,\dots,s_{2^n}\rangle_{p_1\cdot\ldots\cdot p_n}$. Now, let p_{n+1} be a prime of the form $6k+1$ (for some $k\in\mathbb{N}$) which is distinct from $p_1,\dots,p_n$, and choose the positive integers σ and τ such $\sigma<\tau<p_{n+1}$ and $(\sigma,\tau)_{p_{n+1}^2}$. For $1\le i\le 2^n$, let $\bar s_i:=s_i\cdot p_{n+1}$ and let $\bar\sigma:=\sigma\cdot p_1\cdot\ldots\cdot p_n$. Then we consider the two Anning $(3\cdot 2^n)$-gons

$$\langle \bar s_1,\bar s_2,\dots,\bar s_{2^n}\rangle_{p_1\cdot\ldots\cdot p_{n+1}} \quad\text{and}\quad \bar\sigma\oplus\langle \bar s_1,\bar s_2,\dots,\bar s_{2^n}\rangle_{p_1\cdot\ldots\cdot p_{n+1}}.$$

As above, it follows that the vertices of these two Anning $(3\cdot 2^n)$-gons are distinct. Their union is therefore a set of $3\cdot 2^{n+1}$ points on a circle, forming an Anning $(3\cdot 2^{n+1})$-gon. Indeed, as before, it follows that mutual distances of the points are among the solutions of the diophantine equation

$$x^2+xy+y^2=p_1^2\cdot\ldots\cdot p_{n+1}^2\,,$$

which completes the proof. *q.e.d.*

The concrete calculation yields the following Anning 48-gon with $p_1=7$, $p_2=13$, $p_3=19$, $p_4=31$, which is encoded by

$$\begin{aligned}\langle &2976, 5096, 6141, 5096, 2976, 1225, 6479, 3535,\\ &\qquad 4199, 5096, 1389, 5096, 4199, 3535, 6479, 1225\rangle_{7\cdot13\cdot19\cdot31}.\end{aligned}$$

This proves Anning's original conjecture.

We can also compute the Anning 96-gon with $p_1=7$, $p_2=13$, $p_3=19$, $p_4=31$, $p_5=37$, which is encoded by

$$\begin{aligned}\langle &5863, 39463, 91377, 18753, 188552, 32643, 45325, 110112,\\ &\quad 39463, 149195, 39463, 110112, 45325, 32643, 188552, 18753,\\ &\qquad 91377, 39463, 5863, 149513, 90520, 98192, 32643, 18753,\\ &\qquad\quad 136648, 52032, 136648, 18753, 32643, 98192, 90520, 149513\rangle_{7\cdot13\cdot19\cdot31\cdot37}.\end{aligned}$$

In an Anning polygon, one can actually read off *all positive*, and hence, by LEMMA 6, *all* solutions of the corresponding diophantine equation. First we consider the case of positive solutions:

PROPOSITION 9. *Let $m = p_1 \cdot \ldots \cdot p_n$ be a product of pairwise distinct primes of the form $6k+1$ and let $\langle s_1, \ldots, s_{2^n} \rangle_m$ be the code of an Anning $(3 \cdot 2^n)$-gon $\mathscr{A}$ constructed in the proof of THEOREM 1. Then for any integers a, b with $0 < a, b < m$ such that $a^2 + ab + b^2 = m^2$ there are three points P, Q, R on $\mathscr{A}$ such that a, b are the distances $\overline{PQ}$ and $\overline{QR}$, respectively.*

Proof. By FACT 5, there are $\frac{3^n - 1}{2}$ positive, integral solutions $a < b$ of $a^2 + ab + b^2 = m^2$. For positive integers n, let $S_n^+ := \frac{3^n-1}{2}$. Then $S_1^+ = 1$, and with an easy calculation we obtain

$$S_{n+1}^+ = 3 \cdot S_n^+ + 1 \,.$$

The proof is now by induction on n: For $n = 1$, $S_1^+ = 1$, *i.e.*, there is a unique integral solution $0 < a < b < m$ of $a^2 + ab + b^2 = m^2$. Now, a and b are the lengths of two sides of the Anning Hexagon constructed in the proof of THEOREM 1.

For the induction step, let $P_0, \ldots, P_{2^n}$ be $2^n + 1$ consecutive points of an Anning $(3 \cdot 2^n)$-gon $\mathscr{A}_n$, and for $0 \le i < j \le 2^n$ let

$$s_{i,j} := \overline{P_i P_j} \,.$$

Let $A_n := \{s_{i,j} < m : 0 \le i < j \le 2^n\}$ and assume that $\mathrm{card}(A_n) = S_n^+$ and that for any integers a, b with $0 < a, b < m$ and $a^2 + ab + b^2 = m^2$ we have $\{a, b\} \subseteq A_n$. Furthermore, let p_{n+1} be a prime of the form $6k+1$ such that $p_{n+1} \nmid m$. As in the proof of THEOREM 1, let $0 < \sigma, \tau < p_{n+1}$ be such that $(\sigma, \tau)_{p_{n+1}^2}$, let $\bar{\sigma} := \sigma \cdot m$, and for $0 \le i < j \le 2^n$ let

$$\bar{s}_{i,j} := s_{i,j} \cdot p_{n+1}.$$

Scaling $\mathscr{A}_n$ by the factor p_{n+1}, we obtain a $(3 \cdot 2^n)$-gon $\mathscr{A}_n'$, where $P_0', \ldots, P_{2^n}'$ are the $2^n + 1$ consecutive points of $\mathscr{A}_n'$ which correspond to $P_0, \ldots, P_{2^n}$, and by a rotation of $\mathscr{A}_n'$ through $\alpha = 2 \arcsin \frac{\sigma\sqrt{3}}{2p_{n+1}}$, we obtain a $(3 \cdot 2^n)$-gon $\mathscr{A}_n''$ with $2^n + 1$ consecutive points $Q_0, \ldots, Q_{2^n}$, where for all $0 \le i \le 2^n$ we have

$$\overline{P_i' Q_i} = \bar{\sigma}$$

(see Figure 8).

Let us define

$$\bar{A}_n := \{s \cdot p_{n+1} : s \in A_n\}, \quad \bar{A}_n \oplus \bar{\sigma} := \{\bar{s} \oplus \bar{\sigma} : \bar{s} \in \bar{A}_n\}, \quad \bar{A}_n \ominus \bar{\sigma} := \{\bar{s} \ominus \bar{\sigma} : \bar{s} \in \bar{A}_n\}.$$

By a similar argument as in the proof of THEOREM 1, it follows that

$$\mathrm{card}(\bar{A}_n) = \mathrm{card}(\bar{A}_n \oplus \bar{\sigma}) = \mathrm{card}(\bar{A}_n \ominus \bar{\sigma}),$$

and that the sets $\bar{A}_n$, $\bar{A}_n \oplus \bar{\sigma}$, $\bar{A}_n \ominus \bar{\sigma}$, and $\{\bar{\sigma}\}$ are pairwise disjoint. For the sake of simplicity, let us assume that $\bar{\sigma} < \min(\bar{A}_n)$ — the general case can be handled similarly. Now, we compute the distances between any two distinct points of $\{P_0', \ldots, P_{2^n}', Q_0, \ldots, Q_{2^n}\}$: We already know that for $0 \le i \le 2^n$, $\overline{P_i' Q_i} = \bar{\sigma}$. Furthermore, for $0 \le i < j \le 2^n$ we have

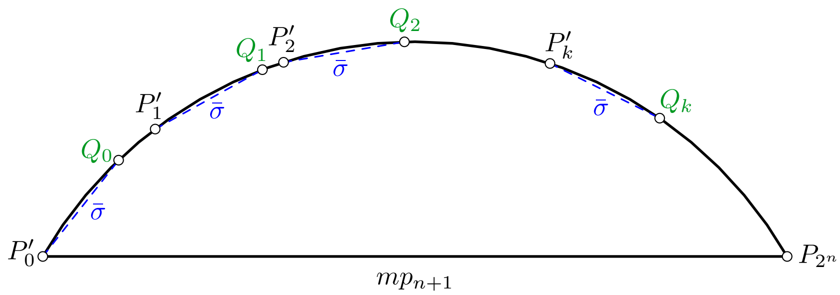

Figure 8: The points P_k' and Q_k.

- either $\overline{P_i'P_j'} = m$ or $\overline{P_i'P_j'} \in \bar{A}_n$,
- either $\overline{Q_iQ_j} = m$ or $\overline{Q_iQ_j} \in \bar{A}_n$,
- either $\overline{P_i'Q_j} \geq m$ or $\overline{P_i'Q_j} \in \bar{A}_n \oplus \bar\sigma$,
- either $\overline{P_j'Q_i} \geq m$ or $\overline{P_j'Q_i} \in \bar{A}_n \ominus \bar\sigma$.

Finally, we have that

$$\mathscr{S} := \left\{\overline{AB}:\ A, B \in \{P_0', \ldots, P_{2^n}', Q_0, \ldots, Q_{2^n}\} \text{ and } \overline{AB} < m\right\} = \bar{A}_n \cup (\bar{A}_n \oplus \bar\sigma) \cup (\bar{A}_n \ominus \bar\sigma) \cup \{\bar\sigma\},$$

which shows that $\operatorname{card}(\mathscr{S}) = 3 \cdot \operatorname{card}(A_n) + 1$, and therefore,

$$\operatorname{card}(\mathscr{S}) = 3 \cdot S_n^+ + 1 = S_{n+1}^+.$$

This completes the induction step and the proof. *q.e.d.*

COROLLARY 10. *Let $m = p_1 \cdot \ldots \cdot p_n$ be a product of pairwise distinct primes of the form $6k+1$ and let $\langle s_1, \ldots, s_{2^n}\rangle_m$ be the code of an Anning $(3 \cdot 2^n)$-gon $\mathscr{A}$ constructed in the proof of* THEOREM *1. Then there are $\frac{3^{n+1}-1}{2}$ positive integers a which occur as a solution of the diophantine equation $a^2 + ab + b^2 = m^2$. For every such integer a, there are two vertices P, Q of $\mathscr{A}$ with distance a, and no other distances occur. More precisely, if (a, b) is an integer solution of $a^2 + ab + b^2 = m^2$, then there are three vertices P, Q, R on $\mathscr{A}$ such that $|a|, |b|$ are the distances $\overline{PQ}$ and $\overline{QR}$, respectively, and $\overline{PR} = m$.*

Proof. According to FACT 5, there are $\frac{3^n-1}{2}$ positive integer solutions (x, y) with $0 < x < y < m$ of $a^2+ab+b^2 = m^2$. With each such pair (x, y) there is also the solution $(-x, x+y)$ with $x + y > m$. If, on the other hand, for $x > m$ we have $a^2 + ab + b^2 = m^2$, then also $(-y, x + y)$ is a solution, where $0 < -y < m$, $0 < x + y < m$. Hence, with each pair of integer solutions (x, y) with $0 < x < y < m$ of $a^2 + ab + b^2 = m^2$, there are exactly three positive integer values $x, y, x + y$ occurring as solutions of the equation, hence a total of

$3 \cdot \frac{3^n-1}{2}$. Last but not least, there is the trivial solution $(m, 0)$, hence m is also a positive value occurring as a solution, which gives a final total of $3 \cdot \frac{3^n-1}{2} + 1 = \frac{3^{n+1}-1}{2}$.

The fact that for every integer solution (x, y) of $a^2 + ab + b^2 = m^2$ we have a triangle in $\mathscr{A}$ with side lengths $|x|, |y|, m$ follows from PROPOSITION 9 together with LEMMA 6.

q.e.d.

We close this discussion with the following observation.

PROPOSITION 11. *Let x, y be a positive integer solution of $x^2+xy+y^2 = m^2$, $m \in \mathbb{N}$, and K a circle with radius $\frac{m^{n-1}}{\sqrt{3}}$, $2 \leq n \in \mathbb{N}$. Then the n endpoints $A_1, \ldots, A_n$ of a chain of $n-1$ chords of length xm^{n-2} in K are pairwise distinct and have integer mutual distances which are solutions of $x^2 + xy + y^2 = m^{2n-2}$.*

Figure 9 shows the construction with $m = 7, x = 5$ for $n = 5$ points in a circle of radius $\frac{7^4}{\sqrt{3}}$. The length of the four chords is $5 \cdot 7^3$.

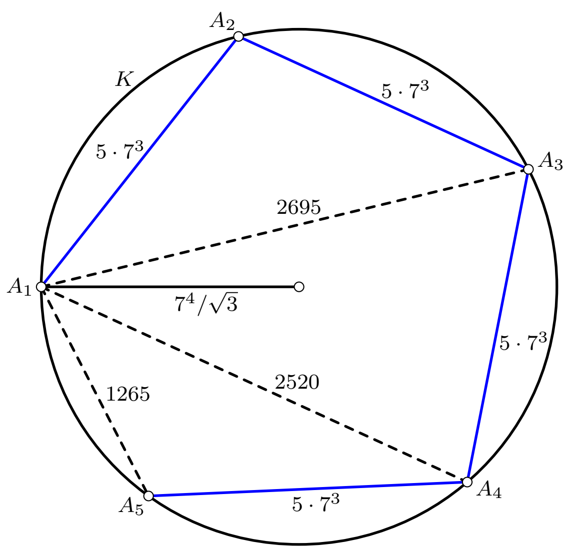

Figure 9: Five points on a circle with integer mutual distance.

Proof of Proposition 11. By construction, the n endpoints in the chain of chords have integer mutual distances

$$xm^{n-2},\ xm^{n-2} \oplus xm^{n-2},\ \ldots,\ \underbrace{xm^{n-2} \oplus \ldots \oplus xm^{n-2}}_{n-1 \text{ summands}}.$$

It remains to show that the chain can never close. In particular, we have to show that $\alpha = \arcsin \frac{x\sqrt{3}}{2m}$ is incommensurable with respect to π. We have $\alpha = \arcsin(\sqrt{r})$ for $r = \frac{3x^2}{4m^2} = \frac{3x^2}{4(x^2+xy+y^2)} \in \mathbb{Q}$. It is known (see [13]) that for $0 \leq r \leq 1$ rational, α is a rational multiple of π if and only if $r \in \{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1\}$. Since in our case we have

$0 < r < \frac{3}{4}$ we only need to check the values $r \in \{\frac{1}{4}, \frac{1}{2}\}$. From $\frac{3x^2}{4(x^2+xy+y^2)} = \frac{1}{4}$, it follows that $y = -2x$ or $y = x$, which is both not possible. From $\frac{3x^2}{4(x^2+xy+y^2)} = \frac{1}{2}$ it follows that $y = \frac{1}{2}(-x \pm \sqrt{3}x) \notin \mathbb{N}$, which is also excluded. *q.e.d.*

We can extend the finite chain of points A_i in PROPOSITION 11 to an infinite sequence $A_1, \ldots, A_n, \ldots$ As we have seen in the proof of PROPOSITION 11, the central angle α over the chord of length xm^{n-2} is incommensurable with respect to π. Hence, by Weyl's Equidistribution Theorem [14], the points A_i are uniformly distributed on the circle. The mutual distance of points A_i and A_j, $i < j$, is an integer by PROPOSITION 11 if $j - i < n$. If, on the other hand $n \leq j - i$, then $|A_i - A_j| m^{j-i-n+1}$ is an integer, again by PROPOSITION 11. Thus, the mutual distance of points A_i in the sequence is always rational. Hence, if $q \in \mathbb{Q}$, we can rescale the circle K of radius $m^{n-1}/\sqrt{3}$ by the factor q/m^{n-1} and obtain a final corollary (see also [7, Theorem 65, p. 229] and [1]):

COROLLARY 12. *Let C be a circle with radius $\frac{q}{\sqrt{3}}$ for some $q \in \mathbb{Q}$. Then, C contains a dense set of points with rational mutual distances.*

Acknowledgement

We would like to thank the referee for his or her valuable remarks which greatly helped to improve this article.

References

[1] WILLIAM ANDERSON, WILLIAM SIMONS, J. G. MAULDON, AND JAMES C. SMITH, *Problems and Solutions: Solutions of Elementary Problems: E2697*, ***Amer. Math. Monthly***, vol. 86 (1979), no. 3, 225.

[2] NORMAN ANNING, *Questions and Discussions: Relating to a Geometric Representation of Integral Solutions of Certain Quadratic Equations*, ***American Mathematical Monthly***, vol. 22 (1915), no. 9, 321.

[3] NORMAN ANNING AND PAUL ERDŐS, *Integral distances*, ***Bull. Amer. Math. Soc.***, vol. 51 (1945), 598–600.

[4] GANBILEG BAT-OCHIR, *On the number of points with pairwise integral distances on a circle*, ***Discrete Applied Mathematics*** (2018).

[5] DAVID A. COX, ***Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication***, 2nd ed., John Wiley & Sons, Hoboken (NJ), 2013.

[6] LEONARD EUGENE DICKSON, ***Introduction to the theory of numbers***, 7th ed., The University of Chicago Press, Chicago (IL), 1951.

[7] Leonhard Euler, *Opera postuma, vol. I.*, ch. Fragmenta arithmetica ex Adversariis mathematicis depromta, C: Analysis Diophantea, pp. 204–263, Petropolis: Eggers, 1862.

[8] Jean-Pierre Friedelmayer, *Points à distances entières sur un cercle*, ***Bulletin de l'APMEP*** (2017), no. 522, 92–104.

[9] Heiko Harborth, *Karl der Grosse und sein Nachwirken. 1200 Jahre Kultur und Wissenschaft in Europa*, ch. Integral Distances in Point Sets, pp. 213–224, Brepols Publishers, 1998.

[10] Heiko Harborth, Arnfried Kemnitz, and Meinhard Möller, *An upper bound for the minimum diameter of integral point sets*, ***Discrete & Computational Geometry***, vol. 9 (1993), 427–432.

[11] Tobias Kreisel and Sascha Kurz, *There are integral heptagons, no three points on a line, no four on a circle*, ***Discrete Comput. Geom.***, vol. 39 (2008), no. 4, 786–790.

[12] Sascha Kurz and Alfred Wassermann, *On the minimum diameter of plane integral point sets*, ***Ars Combin.***, vol. 101 (2011), 265–287.

[13] Juan L. Varona, *Rational values of the arccosine function*, ***Cent. Eur. J. Math.***, vol. 4 (2006), no. 2, 319–322.

[14] Hermann Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, ***Math. Ann.***, vol. 77 (1916), no. 3, 313–352.