Configurations on Elliptic Curves

Dedicated to the memory of Branko Grünbaum

Andrin Halbeisen

8400 Winterthur, Switzerland

andrin.halbeisen@gmx.ch

Lorenz Halbeisen

Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland

lorenz.halbeisen@math.ethz.ch

Norbert Hungerbühler

Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland

norbert.hungerbuehler@math.ethz.ch

key-words: configuration, elliptic curve

2020 Mathematics Subject Classification: **51A20** 51A05

Abstract

An elliptic configuration is a configuration with all its points on a cubic curve, or more precisely, all points are in the torsion group of an elliptic curve. We investigate the existence of elliptic $(3r_4, 4r_3)$ configurations for $r \geq 5$. In particular, we construct elliptic $((p-1)_3)$ configurations for every prime $p > 7$ and show that there are $(3r_4, 4r_3)$ configurations whenever $3r = p-1$ for some prime $p > 7$. Furthermore, we show that for every $k \geq 2$ there is an elliptic $(9k_4, 12k_3)$ configuration with a rotational symmetry of order 3, where we introduce a new normal form for D_3-symmetric elliptic curves.

1 Terminology

A (p_λ, l_π)*configuration* consists of p points and l lines in the real affine plane such that each point belongs to λ lines and each line goes through π points. If $p = l$ and consequently $\lambda = \pi$, we just write (p_λ) instead of (p_λ, l_π). A configuration is called an *elliptic configuration* if there is a cubic curve which passes through all points of the configuration (see also the discussion of elliptic configurations in Grünbaum [19, p. 247 ff.]). Examples of elliptic $(12_4, 16_3)$ configurations can be found in Grünbaum [19, p. 249], Coxeter [16, p. 440], and Feld [17] (where one can find also an example of an elliptic $(36_7, 84_3)$ configuration, and for an elliptic $(24_6, 48_3)$ configuration see [21]. In [25] Metelka identified 8 elliptic $(12_4, 16_3)$ configurations.

For a finite group G, a configuration is called G-*symmetric* if G is a subgroup of the symmetry group of the configuration. There exists an extensive literature on configurations with various types of symmetry (rotational, dihedral, point, chiral, floral): see,

e.g., [1–14]. Finally, an *elliptic G-symmetric configuration* is a configuration which is both elliptic and G-symmetric.

Since a line intersects a cubic curve in at most 3 different points, the maximum value for π of an elliptic (p_λ, l_π) configuration is $\pi = 3$, and therefore, natural candidates for elliptic configurations are $(3r_3)$ configurations and $(3r_4, 4r_3)$ configurations for $r \geq 1$ (for $(12_4, 16_3)$ configurations see, for example, Gropp [18] or Metelka [26]). On page 293 of Grünbaum [19], *Open Problem 4* asks to decide for which $r \geq 5$ elliptic $(3r_4, 4r_3)$ configurations exist.

Of particular interest are elliptic configurations with C_3 or D_3 symmetry. Here, D_3 is the dihedral group of the regular triangle, and C_3 its subgroup of of elements of odd order. For $G = D_3$ or $G = C_3$ the number of lines of a G-symmetric configuration must be a multiple of 3. Hence, since $3 \mid 4r$ implies $3 \mid r$, the possible elliptic D_3 or C_3-symmetric $(3r_4, 4r_3)$ configurations are $(9k_4, 12k_3)$ configurations for $k \geq 1$.

After introducing a normal form of cubic curves which are D_3-symmetric, we give a construction of elliptic D_3-symmetric $(9k_4, 12k_3)$ configurations for every $k \geq 2$. Finally, we show the existence of elliptic $(3r_4, 4r_3)$ configurations for some $r \geq 5$. The constructions of elliptic configurations are motivated by Schroeter's ruler construction of cubic curves (see [21]).

2 A D_3-symmetric normal form for cubic curves

In this section, we will introduce a normal form of cubic curves which are D_3-symmetric and show that every non-singular cubic curve can be transformed into this form by a projective transformation. This normal form of cubic curves will be used later in order to construct elliptic D_3-symmetric configurations.

It is well-known that every non-singular cubic curve in the real projective plane can be transformed into Weierstrass Normal Form

$$y^2 = x^3 + ax^2 + bx.$$

Without loss of generality, we may require that the x-coordinate of an inflection point is 1. In this case we get (see [20, Fact 2.3])

$$b \neq 1 \quad \text{and} \quad a = \frac{b^2 - 6b - 3}{4}. \tag{1}$$

Now, by computing the polar conic at the point $(0, 1, 0)$ in the projective extension of the plane as well as the intersection points of the tangents at the inflections points, we find the projective transformation

$$\begin{pmatrix} 1 & 0 & -2b \\ 0 & \frac{\sqrt{3}(b-1)}{2} & 0 \\ 1 & 0 & b-3 \end{pmatrix}$$

which transforms the affine curve $y^2 = x^3 + ax^2 + bx$ (with a, b as in (1)) into the curve

$$\Gamma_{D_3} : \; x^3 - 3xy^2 - 3(b-3)(x^2+y^2) + 4b^2(b-9) \; = \; 0.$$

To see that the latter curve is D_3-symmetric, notice first that the curve is symmetric with respect to the x-axis. To see that the curve is also symmetric with respect to rotations about the origin with angle $\frac{2\pi}{3}$, notice that if (x_0, y_0) is a point on the curve Γ_{D_3}, then also

$$\begin{pmatrix} \cos(\frac{2\pi}{3}) & \sin(\frac{2\pi}{3}) \\ -\sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

is a point on Γ_{D_3}. Figure 1 shows two D_3-symmetric curves Γ_{D_3}.

Conic sections have a natural reflection symmetry along their axes. It is quite natural to look at cubic curves in a D_3-symmetric form. In this regard, we now have:

Proposition 1. *Every regular cubic curve can be brought, by a projective transformation, into the D_3-symmetric normal form*

$$\Gamma_{D_3} : \; x^3 - 3xy^2 - 3(b-3)(x^2+y^2) + 4b^2(b-9) \; = \; 0$$

with $b \in \mathbb{R} \setminus \{1\}$.

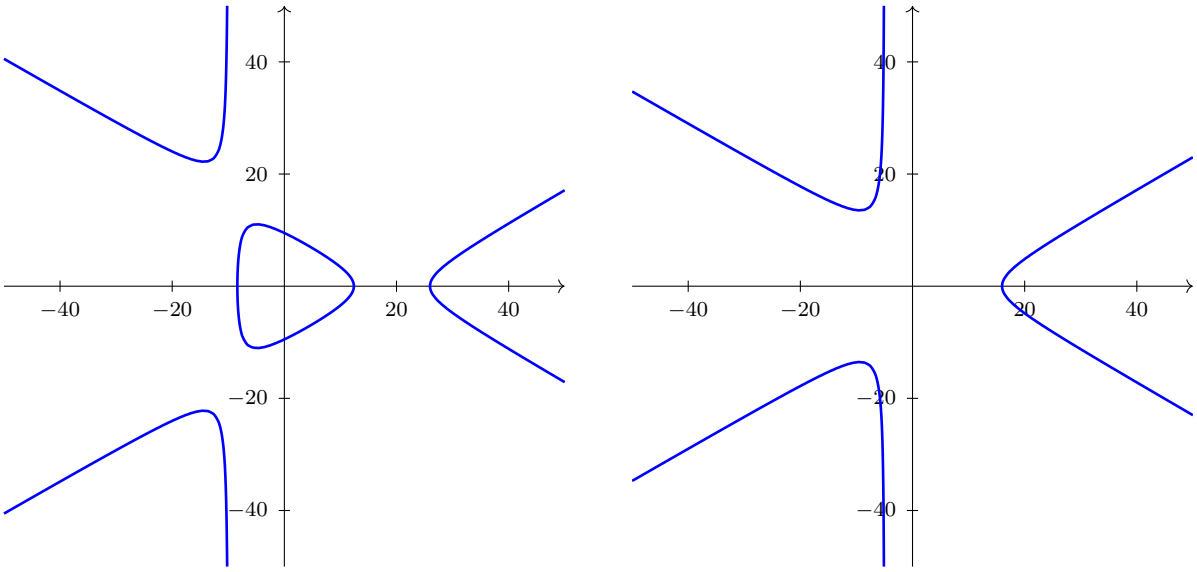


Figure 1: Elliptic D_3-symmetric curves for $b = 13$ (left), and $b = 8$ (right).

Remarks. Since the three points at infinity of an elliptic D_3-symmetric curve are the three inflection points of the curve, the projective transformation which transforms a curve in Weierstrass Normal Form into our D_3-symmetric normal form is in general not rational (*e.g.*, in the case when the parameter b is rational).

Concerning the arithmetic on elliptic D_3-symmetric curves it turns out that the formulae to add or to double points are somewhat more involved than the corresponding formulae for curves in Weierstrass Normal Form.

3 Elliptic D_3-symmetric $(9k_4, 12k_3)$ configurations

In order to construct an elliptic D_3-symmetric $(9k_4, 12k_3)$ configuration for some $k \geq 2$, we take an arbitrary D_3-symmetric elliptic curve Γ_0 with neutral element $\mathscr{O} = (0, 1, 0)$ and choose a point Q on Γ_0 of order $9k + 3$. This can be achieved by considering a p-periodic parametrization of the curve by the Weierstrass $\wp$-function and taking the point Q as the image of the parameter value $\frac{pq}{9k+3}$ for some q with $\gcd(q, 9k + 3) = 1$. See [27, Chapter VI, §3] for details. As a matter of fact, we would like to mention that the points which are constructed in this way are in general irrational. Mazur's classification theorem (see [23], [24]) limits the possibility for elliptic configurations with rational points: See Figure 8 for an example of a configuration which cannot have only rational points.

Notice that $k \geq 2$ is necessary, since $k = 1$ corresponds to the Hesse configuration $(9_4, 12_3)$ which can be realized in the complex projective plane as the set of inflection points of an elliptic curve, but which has no realization with straight lines in the Euclidean plane because of the Sylvester-Gallai theorem. In fact our construction, which we present below, works only for $k \geq 2$.

The group G_k on Γ_0, generated by the point Q, is isomorphic to the group $\mathbb{Z}/(9k + 3)\mathbb{Z}$. For $1 \leq i \leq 9k + 3$, let

$$P_i := i * Q := \underbrace{Q + Q + \ldots + Q}_{i \text{ terms}},$$

where we denote the group operation on Γ_0 by $+$. We define the following three sets of points:

$$S_0 := \{P_1, \ldots, P_{3k}\}, \qquad S_1 := \{P_{3k+2}, \ldots, P_{6k+1}\}, \qquad S_2 := \{P_{6k+3}, \ldots, P_{9k+2}\}$$

Then each S_j (for $j \in \{0, 1, 2\}$) contains $3k$ pairwise distinct points, and since the sets S_j are pairwise disjoint, the set $S := S_0 \cup S_1 \cup S_2$ contains $9k$ pairwise distinct points on the curve Γ_0. Notice that since the points P_{3k+1}, P_{6k+2} of order three, and P_{9k+3} are the only points of Γ_0 at infinity and none of them belongs to S, all points of S belong to the real affine plane. The goal is now to construct a D_3-symmetric, $(9k_4, 12k_3)$ configuration on the set of points S. Before we start with the construction, let us introduce some notation.

- We identify the group G_k with the group $\mathbb{Z}/(9k + 3)\mathbb{Z}$, and for $1 \leq u \leq 9k + 3$, we identify the point P_u with $u \in G_k$ (*i.e.*, with an element in $\mathbb{Z}/(9k + 3)\mathbb{Z}$). Similarly, we identify S with a subset of G_k.
- If three distinct points P_u, P_v, P_w are collinear (*i.e.*, lie on a line), then the line is denoted by $[u, v, w]$. Notice that by the group law of an elliptic curve, we have that three distinct points P_u, P_v, P_w are collinear if and only if $u + v + w \equiv 0 \pmod{9k + 3}$. In other words, each line through three different points is of the form $[u, v, w]$ for some pairwise distinct $u, v, w \in G_k$.

- If $[u,v,w]$ is a line, then $-[u,v,w] := [-u,-v,-w]$ is the *inverse line* of $[u,v,w]$. Notice that if $[u,v,w]$ is a line in S (*i.e.*, $u,v,w \in S$), then $-[u,v,w]$ is a line in S with $-[u,v,w] \neq [u,v,w]$, namely the line mirrored at the x-axis.

- For $u \in G_k$, we define $\rho(u) := u + (3k+1)$. Notice that if, for example, $u \in S_0$, then $\rho(u) \in S_1$ and $\rho^2(u) := (\rho \circ \rho)(u) \in S_2$.

- If $[u,v,w]$ is a line, then $\rho[u,v,w] := [\rho(u), \rho(v), \rho(w)]$ is the corresponding *rotated line*. Notice that if $[u,v,w]$ is a line in S, then $\rho[u,v,w]$ and $\rho^2[u,v,w]$ are lines in S, where $[u,v,w]$, $\rho[u,v,w]$, and $\rho^2[u,v,w]$ are pairwise distinct (but not necessarily disjoint) lines.

The following fact is an immediate consequence of the preceding definitions.

Fact 2. *Any $(9k_4, 12k_3)$ configuration on the point set S which contains with any line $[u,v,w]$ also the lines $\rho[u,v,w]$ and $\rho^2[u,v,w]$, is an elliptic C_3-symmetric $(9k_4, 12k_3)$ configuration, where C_3 is the cyclic group of order 3. If the configuration contains in addition with any line $[u,v,w]$ also the line $-[u,v,w]$, then it is an elliptic D_3-symmetric configuration.*

So, by Fact 2, to construct an elliptic D_3-symmetric $(9k_4, 12k_3)$ configuration it suffices to find $2k$ lines $[u_i,v_i,w_i]$ such that for $1 \leq i \leq 2k$, the lines $\pm[u_i,v_i,w_i]$, $\pm\rho[u_i,v_i,w_i]$, and $\pm\rho^2[u_i,v_i,w_i]$ are pairwise distinct. Before we start constructing such lines, we show how we construct lines in S from "proto-lines" in S_0:

For any $u,v,w \in S$, let

$$u_0 := u \pmod{3k+1}, \quad v_0 := v \pmod{3k+1}, \quad w_0 := w \pmod{3k+1}.$$

Then $u_0, v_0, w_0 \in S_0$ and if $[u,v,w]$ is a line, then $u_0 + v_0 + w_0 \equiv 0 \pmod{3k+1}$. If, on the other hand, $u,v,w \in S_0$ are such that $u+v+w \equiv 0 \pmod{3k+1}$, then the triple (u,v,w) is called a *proto-line* in S_0. Notice that we do not require that the three points u,v,w of a proto-line (u,v,w) are pairwise distinct.

The following lemma will be crucial in the construction of $(9k_4, 12k_3)$ configurations.

Reduction Lemma 3. *If $u,v,w \in S_0$ are such that (u,v,w) is a proto-line, then there are $\bar{u},\bar{v},\bar{w} \in S$ such that $u = \bar{u}'$, $v = \bar{v}'$, $w = \bar{w}'$ and $[\bar{u},\bar{v},\bar{w}]$ is a line.*

Proof. Let $u,v,w \in S_0$ be such that (u,v,w) is a proto-line. Notice that since $u + v + w \equiv 0 \pmod{3k+1}$ and $3 \nmid 3k+1$, at most two of the three points u,v,w can be equal. Without loss of generality assume $u \neq v$. Then, for $\bar{u} := u$, $\bar{v} := v$, and $\bar{w} := w + (6k+2)$, $[\bar{u},\bar{v},\bar{w}]$ is a line. *q.e.d.*

In order to construct an elliptic C_3-symmetric $(9k_4, 12k_3)$ configuration, by Reduction Lemma 3 and by rotating the lines with ρ and ρ^2, respectively, it suffices to find a set

L of $4k$ proto-lines in S_0 such that each point of S_0 belongs to exactly 4 proto-lines in L. In order to construct an elliptic D_3-symmetric $(9k_4, 12k_3)$ configuration, we have to make sure in addition that for each proto-line $(u, v, w) \in L$, also $(-u, -v, -w) \in L$.

Theorem 4. *For every integer $k \geq 2$ there exists an elliptic D_3-symmetric $(9k_4, 12k_3)$ configuration.*

The proof of this theorem will be carried out in the following sections by explicit constructions of the corresponding configurations. In particular, we will construct elliptic $(9k_4, 12k_3)$ configurations for $k \equiv 3 \pmod 4$, for $k \equiv 1 \pmod 4$, and for k even, respectively.

3.1 D_3-symmetric $(9k_4, 12k_3)$ configurations for $k \equiv 3 \pmod 4$

Let $k \geq 3$ be a positive integer with $k \equiv 3 \pmod 4$, and let $n_k := 3k + 1$. The first step in the construction of a $(9k_4, 12k_3)$ configuration is the construction of $4k$ proto-lines. For this, we start with a triple (a_0, b_0, c_0) with $a_0 + b_0 + c_0 \equiv 0 \pmod{n_k}$, where a_0, b_0, c_0 are not necessarily non-zero. Then, we build successively the n_k triples $(a_{i+1}, b_{i+1}, c_{i+1}) := (a_i - 2, b_i + 1, c_i + 1)$ in $\mathbb{Z}/n_k\mathbb{Z}$. Among these triples, there will be two triples which are not proto-lines because one of the numbers is 0. We then replace these two triples by two proto-lines and construct additional $k - 1$ proto-lines in order to obtain $4k$ proto-lines.

We construct the $4k$ proto-lines as follows: Firstly, let

$$m_1 := \frac{k+1}{2}\,, \qquad m_2 := n_k - m_1\,,$$

and let

$$t_1 := \begin{cases} \frac{m_1}{2} & \text{if } m_1 \equiv 2 \pmod 4, \\ \frac{n_k + m_1}{2} & \text{otherwise,} \end{cases} \qquad t_2 := n_k - t_1.$$

Since $k \equiv 3 \pmod 4$, we have that $k + 1 \equiv 0 \pmod 4$ and therefore, n_k, m_1 and m_2 are even. Moreover, since $m_1 \equiv 0$ or $2 \pmod 4$, and since $n_k \equiv 2 \pmod 4$, we have either $m_1 \equiv 2 \pmod 4$ or $n_k + m_1 \equiv 2 \pmod 4$, which implies that t_1 and t_2 are both odd, in fact $t_1, t_2 \equiv 1 \pmod 4$.

Let $S_0^* := S_0 \cup \{0\}$ and define the following sequence of triples $\langle (a_i, b_i, c_i) : 0 \leq i < n_k \rangle$ in $S_0^* \times S_0^* \times S_0^*$: Let

$$(a_0, b_0, c_0) := (t_1, 0, t_2)$$

and for $0 \leq i < n_k$ let

$$(a_i, b_i, c_i) := (t_1 - 2i,\ i,\ t_2 + i) \pmod{n_k}\,.$$

Then, the sequence has the following properties:

(a) For all $0 \le i < n_k$, $a_i + b_i + c_i \equiv 0 \pmod{n_k}$ and a_i is odd. For the latter, recall that t_1 is odd and that n_k is even.

(b) $(a_{t_1}, b_{t_1}, c_{t_1}) = (t_2, t_1, 0) \pmod{n_k}$, *e.g.*, $a_{t_1} = t_1 - 2t_1 = -t_1 \equiv t_2 \pmod{n_k}$.

(c) For all $0 \le i < j < n_k$ we have $\{a_i, b_i, c_i\} \neq \{a_j, b_j, c_j\}$.

(d) For all $0 \le i < n_k$ we have

$$-(a_i, b_i, c_i) = -(t_1 - 2i,\ i,\ t_2 + i) = (t_2 + 2i,\ -i,\ t_1 - i) = (a_{t_1-i},\ c_{t_1-i},\ b_{t_1-i}).$$

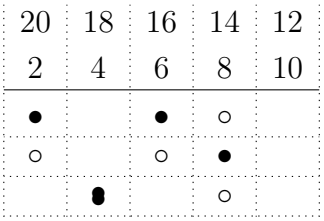
Property (a) shows that every triple in the sequence is a proto-line in S_0^*. Property (c) shows that the sequence contains exactly n_k pairwise different proto-lines; let L^* be the set of these n_k proto-lines. Property (d) shows that a proto-line (u, v, w) is in L^* if and only if the proto-line $-(u, v, w)$ is in L^*.

Every even number $0 \le \ell < n_k$ appears in exactly 2 proto-lines in L^*, and every odd number $0 < \ell < n_k$ appears in exactly 4 proto-lines in L^*. Now, we remove the two proto-lines $(t_1, 0, t_2)$ and $(t_2, t_1, 0)$ from L^*, and introduce the two proto-lines (m_1, t_2, t_2) and (m_2, t_1, t_1) to L^*; the resulting set of proto-lines is denoted L_0. Notice that $(m_2, t_1, t_1) = -(m_1, t_2, t_2)$, that the two proto-lines (m_1, t_2, t_2) and (m_2, t_1, t_1) are not in L^*, and that every proto-line in L_0 is a proto-line in S_0. In L_0, every odd number $0 < \ell < n_k$ appears in exactly 4 proto-lines in L_0, and every even number $0 < \ell < n_k$, except m_1 and m_2, appears in exactly 2 proto-lines in L_0, whereas m_1 and m_2 appear in exactly 3 proto-lines in L_0.

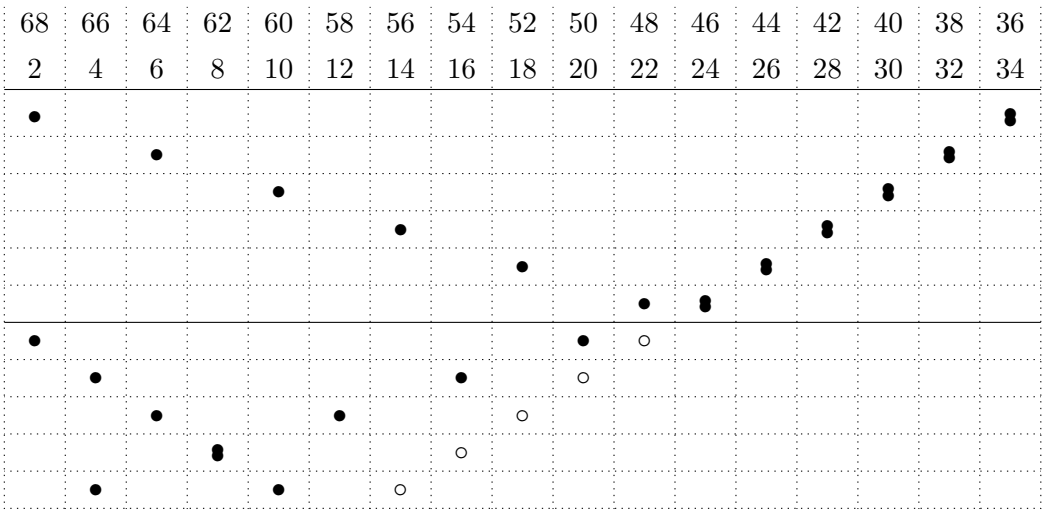
Example 1. For $k = 3$ (*i.e.*, $n_k = 10$), we start with the triple $(1, 0, 9)$ and get successively the triples $(9, 1, 0)$, $(7, 2, 1)$, $(5, 3, 2)$, $(3, 4, 3)$, $(1, 5, 4)$, $(9, 6, 5)$, $(7, 7, 6)$, $(5, 8, 7)$, $(3, 9, 8)$. We now replace the two triples $(1, 0, 9)$ and $(9, 1, 0)$ by the two proto-lines $(2, 9, 9)$ and $(8, 1, 1)$. This way, each odd number appears in a proto-line exactly 4 times, and each even number, except 2 and 8, appears in a proto-line exactly twice, whereas 2 and 8 appear 3 times. The additional $k - 1 = 2$ proto-lines will then be $(2, 4, 4)$ and $(8, 6, 6)$.

In order to complete the construction of a $(9k_4, 12k_3)$ configuration, we consider the set T_k consisting of the $\frac{n_k}{2} - 1$ even numbers $2, 4, \ldots n_k - 2$. It remains to find $k - 1$ proto-lines in S_0 with points in T_k, where every number in T_k except m_1 and m_2 appears in exactly 2 proto-lines, whereas m_1 and m_2 appear in exactly 1 proto-line. Together with the $n_k = 3k + 1$ proto-lines of L_0, this gives us $4k$ proto-lines, and after extending them to lines of S by Reduction Lemma 3 and by rotating them with ρ and ρ^2, we finally obtain $12k$ lines. For the remaining $k - 1$ proto-lines with points in T_k, by trial and error we have found the following pattern, which is obtained in the following way: First, we write the points of T_k in two rows, where the first row contains the numbers $n_k - 2$ to $\frac{n_k-2}{2} + 1$ in reverse order, and the second row contains the numbers 2 to $\frac{n_k-2}{2}$ in the natural order. Below the numbers of these two rows, we write $\bullet$ and $\circ$ for the

three points of the proto-lines, where • denotes a number from the second row, and ∘ denotes a number from the first row. Finally, ⬮ means the same number is listed twice. The following figure gives an example of three proto-lines for $k = 7$ (*i.e.*, $n_k = 22$), according to the construction described above:



The first proto-line is $(2, 6, 14)$, the second is $(20, 16, 8) = -(2, 6, 14)$, and the third is $(4, 4, 14)$. Notice that $-(u, v, w)$ is obtained from (u, v, w) by exchanging • and ∘. Now, instead of writing both proto-lines (u, v, w) and $-(u, v, w)$, we just write the one which uses the greater number of •'s — having in mind that each proto-line (u, v, w) represents also the proto-line $-(u, v, w)$. This way, we just have to find $\frac{k-1}{2}$ proto-lines. The following figure illustrates the 11 proto-lines for $k = 23$ (*i.e.*, $n_k = 70$), given in two parts:



First, notice that the proto-lines given in the diagram contain only even numbers and are therefore different from the proto-lines in L_0. Furthermore, we see that each point, except the points 12 and 58, appears in exactly 2 proto-lines, whereas the points 12 and 58 appear in exactly 1 proto-line. Notice that for $k = 23$, $m_1 = \frac{k+1}{2} = 12$ and $m_2 = n_k - m_1 = 58$.

Now, we give a more formal construction of the remaining $\frac{k-1}{2}$ proto-lines: Let $\tilde{n}_k := \frac{n_k}{2}$. The $\frac{k+1}{4}$ proto-lines in the first part are

$$\big(2 + 4i, (\tilde{n}_k - 1) - 2i, (\tilde{n}_k - 1) - 2i\big) \quad \text{where } 0 \le i \le \tfrac{k-3}{4}.$$

In particular, for $i = 0$ we obtain $(2, \tilde{n}_k - 1, \tilde{n}_k - 1)$, and for $i = \frac{k-3}{4}$ we obtain $(k-1, k+1, k+1)$ (notice that $2 + 4 \cdot \frac{k-3}{4} = k-1$ and $(\frac{3k+1}{2} - 1) - 2 \cdot \frac{k-3}{4} = k+1$). Furthermore, the $\frac{k-3}{4}$ proto-lines in the second part are

$$\big(2 + 2i,\ (k-3) - 4i,\ -(k-1) + 2i\big) \quad \text{where } 0 \le i \le \tfrac{k-7}{4}.$$

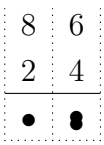
In particular, for $i = 0$ we obtain $(2, k-3, -(k-1))$, and for $i = \frac{k-7}{4}$ we obtain $(\frac{k-3}{2}, 4, -\frac{k+5}{2})$. Notice that $2+2\cdot\frac{k-7}{4} = \frac{k-3}{2}$, $(k-3)-4\cdot\frac{k-7}{4} = 4$, and $-(k-1)+2\cdot\frac{k-7}{4} = -\frac{k+5}{2}$. Now, since $\frac{k-3}{2} + 2 = m_1$ and $-(\frac{k+5}{2} - 2) = m_2$, we see that the only numbers which appear in exactly one proto-line are m_1 and m_2.

Example 2. We illustrate the construction described above for the parameter $k = 3$. This leads to an elliptic D_3-symmetric $(27_4, 36_3)$ configuration. The underlying group is $\mathbb{Z}_{30}$ on Γ_0. We obtain:

- $k = 3$, $n_k = 10$, $m_1 = 2$, $m_2 = 8$, $t_1 = 1$, $t_2 = 9$.
- The proto-lines in L^* given in Example 1 are

  $(1,0,9), (9,1,0), (7,2,1), (5,3,2), (3,4,3), (1,5,4), (9,6,5), (7,7,6), 5,8,7), (3,9,8)$.

- Remove $(1,0,9)$ and $(9,1,0)$, and introduce $(2,9,9)$ and $(8,1,1)$. This gives us the 10 proto-lines of L_0.
- The diagram, which yields the additional $\frac{k-1}{2} = 1$ line consists just of a single line:

  This gives us the lines $(2,4,4)$ and $(8,6,6)$.

- Together with the 10 proto-lines in L_0, we have now 12 proto-lines which we extend to proper lines in S and rotate them.

Observe that depending on how we extend the proto-lines to proper lines, and depending on the choice of the generator of $\mathbb{Z}_{30}$, we obtain different resulting configurations. One version is shown in Figure 2.

3.2 D_3-symmetric $(9k_4, 12k_3)$ configurations for $k \equiv 1 \pmod 4$

Let $k \ge 3$ be a positive integer with $k \equiv 1 \pmod 4$. Furthermore, let $n_k := 3k+1$ and let $m := \frac{n_k}{2}$. Notice that since $n_k \equiv 0 \pmod 4$, m is even.

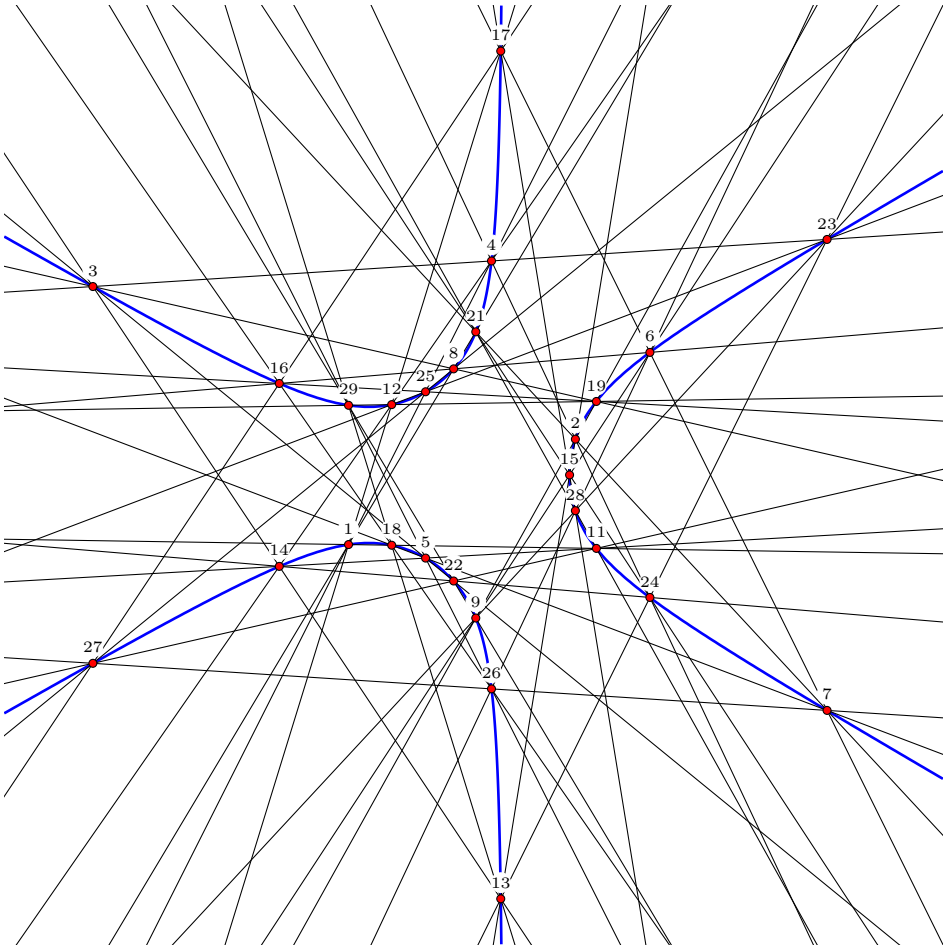


Figure 2: An elliptic D_3-symmetric $(27_4, 36_3)$ configuration.

As above, let $S_0^* := S_0 \cup \{0\}$ and define the following sequence of triples $\langle (a_i, b_i, c_i) : 0 \le i < n_k \rangle$ in $S_0^* \times S_0^* \times S_0^*$: Let

$$(a_0, b_0, c_0) := (0,\, n_k - 1,\, 1) \quad \text{and} \quad (a_1, b_1, c_1) := (2,\, n_k - 1,\, n_k - 1),$$

and for all $0 \le i < n_k - 2$ let

$$(a_{i+2}, b_{i+2}, c_{i+2}) := (a_i + 4,\, b_i - 2,\, c_i - 2) \pmod{n_k}.$$

Then, the sequence has the following properties:

(a) For all $0 \le i < n_k$, $a_i + b_i + c_i \equiv 0 \pmod{n_k}$, a_i is even, and b_i and c_i are both odd.

(b) $(a_m, b_m, c_m) = (0, m-1, m+1)$.

(c) For all $0 \le i < j < n_k$, $\{a_i, b_i, c_i\} \ne \{a_j, b_j, c_j\}$.

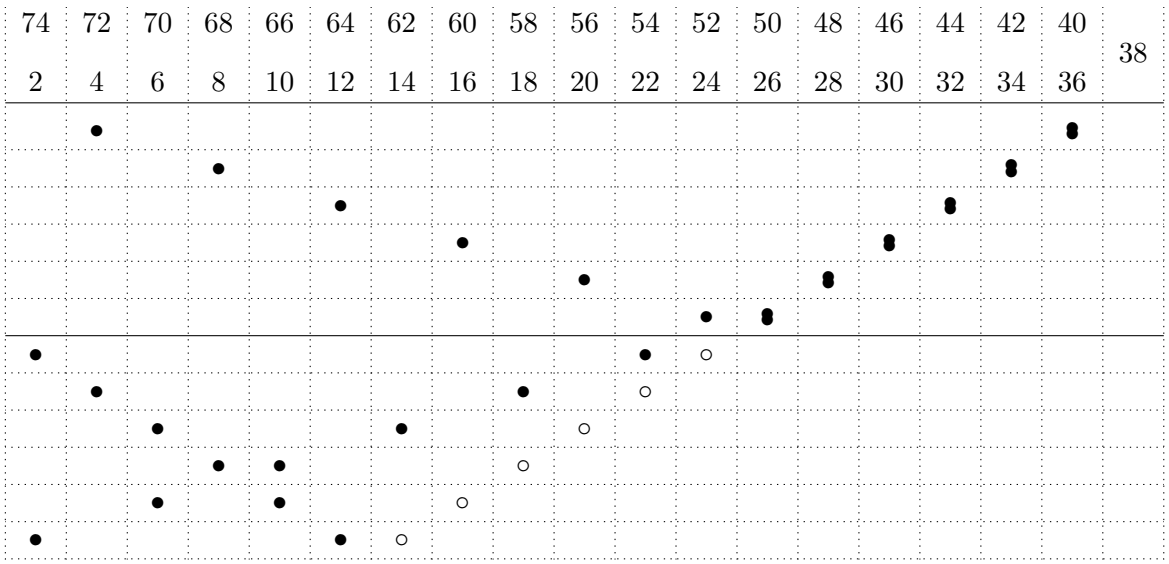
(d) For all $s \in \mathbb{Z}/n_k\mathbb{Z}$ we have $-(a_s, b_s, c_s) = (a_{-s}, b_{-s}, c_{-s})$.

Property (a) shows that every triple in the sequence is a proto-line in S_0^*. Property (c) shows that the sequence contains exactly n_k pairwise different proto-lines; let L^* be the set of these n_k proto-lines. Property (d) shows that a proto-line (u, v, w) is in L^* if and only if the proto-line $-(u, v, w)$ is in L^*.

Every even number $0 \leq \ell < n_k$ appears in exactly 2 proto-lines in L^*, and every odd number $0 < \ell < n_k$ appears in exactly 4 proto-lines in L^*. Now, we remove the two proto-lines $(0, n_k - 1, 1)$ and $(0, m - 1, m + 1)$ from L^*, and introduce the two proto-lines $(m, n_k - 1, m + 1)$ and $(m, 1, m - 1)$ to L^*; the resulting set of proto-lines is denoted L_0. Notice that $(m, n_k - 1, m + 1) = -(m, 1, m - 1)$, that the two proto-lines $(m, n_k - 1, m + 1)$ and $(m, 1, m - 1)$ are not in L^*, and that every proto-line in L_0 is a proto-line in S_0. In L_0, every odd number $0 < \ell < n_k$ appears in exactly 4 proto-lines in L_0, and every even number $0 \leq \ell < n_k$, except m, appears in exactly 2 proto-lines in L_0, whereas m appears in exactly 4 proto-lines in L_0.

In order to complete the construction of a $(9k_4, 12k_3)$ configuration, we consider the set T_k consisting of the $\frac{n_k}{2} - 1$ even numbers $2, 4, \ldots n_k - 2$. It remains to find $k - 1$ proto-lines in S_0 with points in T_k, where every number in T_k except m appears in exactly 2 proto-lines, whereas m does not appear in any proto-line.

For the construction of the remaining $k-1$ proto-lines with points in T_k, by trial and error we have found again a pattern, which is obtained in the following way: As above, we write just the proto-line with the greater number of •'s — having in mind that each proto-line (u, v, w) represents also the proto-line $-(u, v, w)$. This way, we just have to find $\frac{k-1}{2}$ proto-lines. The following figure illustrates the 12 proto-lines for $k = 25$ (*i.e.*, $n_k = 76$), given in two parts:



First, notice that the proto-lines given in the diagram are different from the proto-lines constructed above. Furthermore, we see that each point, except the point 38,

appears in exactly 2 proto-lines, whereas the point 38 does not appear in a proto-line. Notice that for $k = 25$, $m = 38$.

Now, we give a more formal construction of the remaining $\frac{k-1}{2}$ proto-lines: The $\frac{k-1}{4}$ proto-lines in the first part are

$$\big(4 + 4i, (m-2) - 2i, (m-2) - 2i\big) \quad \text{where } 0 \le i \le \tfrac{k-5}{4}.$$

In particular, for $i = 0$ we obtain $(4, m-2, m-2)$, and for $i = \frac{k-5}{4}$ we obtain $(k-1, k+1, k+1)$ (recall that $m = \frac{3k+1}{2}$). Furthermore, the $\frac{k-1}{4}$ proto-lines in the second part are

$$\big(2 + 2i, (k-3) - 4i, -(k-1) + 2i)\big) \quad \text{where } 0 \le i \le \tfrac{k-5}{4}.$$

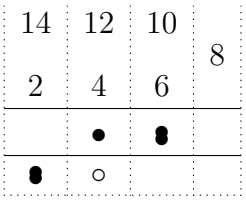
In particular, for $i = 0$ we obtain $(2, k-3, -(k-1))$, and for $i = \frac{k-5}{4}$ we obtain $(\frac{k-1}{2}, 2, -\frac{k+3}{2})$. Notice that the only number which does not appear in a proto-line is m, as required.

Example 3. We illustrate this construction for the parameter $k = 5$. This leads to an elliptic D_3-symmetric $(45_4, 60_3)$ configuration. The construction gives the following:

- $k = 5$, $n_k = 16$, $m = 8$.
- The proto-lines in L^* are:

  $(0, 15, 1), (2, 15, 15), (4, 13, 15), (6, 13, 13), (8, 11, 13), (10, 11, 11), (12, 9, 11),$
  $(14, 9, 9), (0, 7, 9), (2, 7, 7), (4, 5, 7), (6, 5, 5), (8, 3, 5), (10, 3, 3), (12, 1, 3), (14, 1, 1)$

- Remove $(0, 15, 1)$ and $(0, 7, 9)$ (*i.e.*, the two triples which contain 0), and introduce $(8, 15, 9)$ and $(8, 1, 7)$. This gives us the 16 proto-lines of L_0.
- The diagram, which gives us additional $\frac{k-1}{2} = 2$ lines consists of just two lines, one line in each part:



  This gives us the $k - 1 = 4$ lines $(4, 6, 6)$, $(12, 10, 10)$, $(2, 2, 12)$, $(14, 14, 4)$.

- Together with the 16 proto-lines in L_0, we have now 20 proto-lines which we extend to proper lines in S and rotate them.

Again, depending on how we extend the proto-lines to proper lines, and depending on the choice of the generator of $\mathbb{Z}_{48}$, we obtain different resulting configurations. One version is shown in Figure 3.

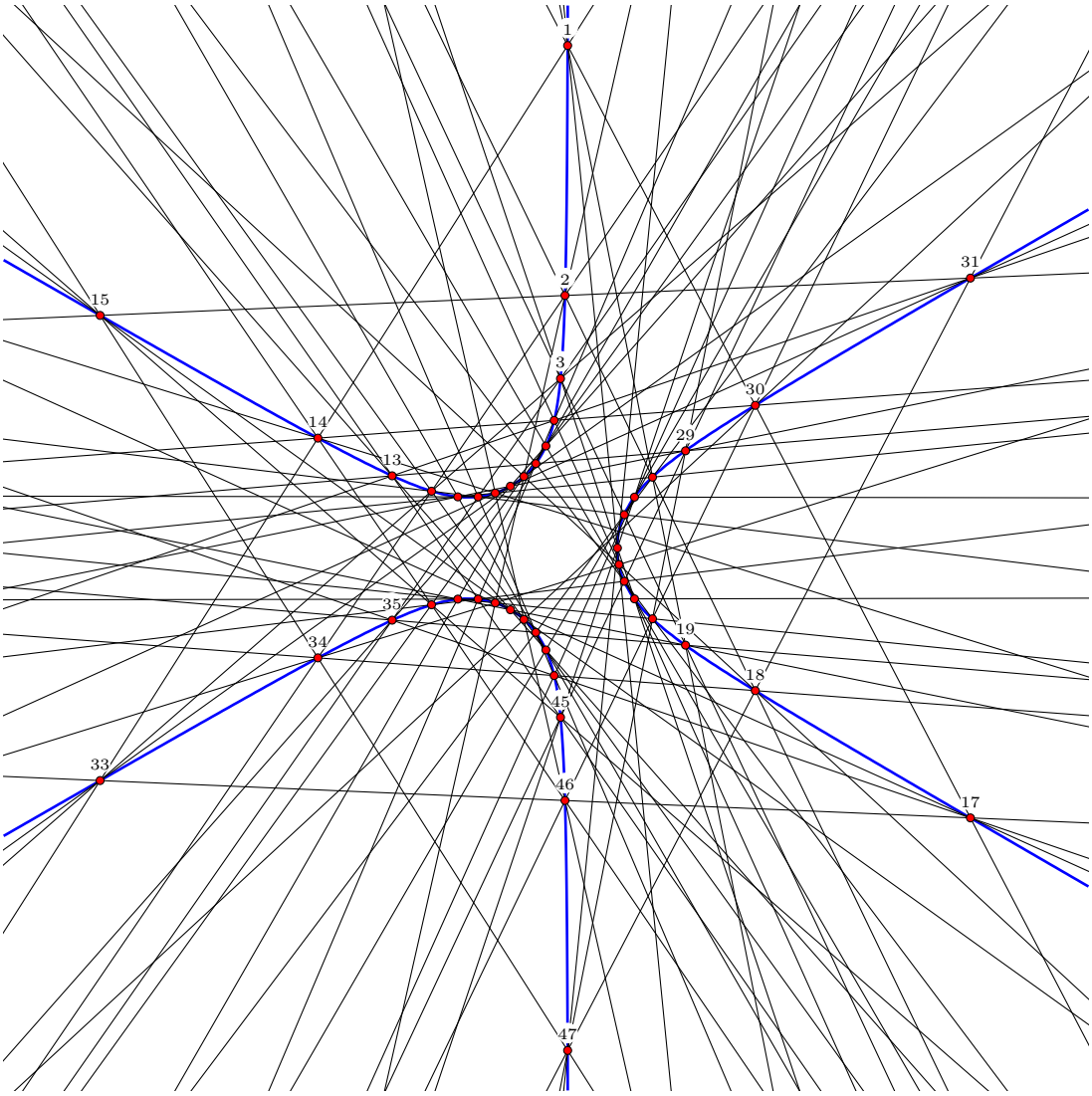


Figure 3: An elliptic D_3-symmetric $(45_4, 60_3)$ configuration. For this figure we have chosen the generator 1 in $\mathbb{Z}_{48}$.

3.3 D_3-symmetric $(9k_4, 12k_3)$ configurations for k even

Let $k \geq 2$ be an even integer and let $n_k := 3k + 1$. Notice that n_k is odd.

As above, Let $S_0^* := S_0 \cup \{0\}$ and define the following sequence of triples $\langle (a_i, b_i, c_i) : i \in \mathbb{Z} \rangle$ in $S_0^* \times S_0^* \times S_0^*$: Let $(a_0, b_0, c_0) := (0, 0, 0)$ and for all $i \in \mathbb{Z}$ let

$$(a_{i+1}, b_{i+1}, c_{i+1}) := (a_i - 2, b_i + 1, c_i + 1)\,.$$

Then, the sequence has the following properties:

(a) For all $i \in \mathbb{Z}$, $a_i + b_i + c_i \equiv 0 \pmod{n_k}$, and $b_i = c_i$.

(b) For $t := \frac{3k}{2}$ we have $(a_t, b_t, c_t) = (1, t, t)$.

(c) For all $i \in \mathbb{Z}$, $(a_{i+n_k}, b_{i+n_k}, c_{i+n_k}) = (a_i, b_i, c_i)$, and for all all $0 < s < n_k$, $\{a_{i+s}, b_{i+s}, c_{i+s}\} \neq \{a_i, b_i, c_i\}$.

(d) In $\mathbb{Z}/n_k\mathbb{Z}$, for $t := \frac{3k}{2}$ and for all $s \in \mathbb{Z}$ we have

$$-(a_{t+s}, b_s, c_s) = (a_{t-s+1}, b_{t-s+1}, c_{t-s+1}).$$

Property (a) shows that every triple in the sequence is a proto-line in S_0^*. Property (c) shows that the sequence contains exactly n_k pairwise different proto-lines, including the proto-line $(0, 0, 0)$. Now, we remove the proto-line $(0, 0, 0)$ and let L_0 be the set of the remaining $3k$ proto-lines. Property (d) shows that a proto-line (u, v, w) is in L_0 if and only if the proto-line $-(u, v, w)$ is in L_0. Furthermore, notice that every number $0 < \ell < n_k$ appears in exactly 3 proto-lines in L_0.

For the construction of the remaining k proto-lines in S_0, we will again visualize the argument. As above, we write just the proto-line with the greater number of $\bullet$'s — having in mind that each proto-line (u, v, w) represents also the proto-line $-(u, v, w)$. This way, we just have to find $\frac{k}{2}$ proto-lines. In order to clearly show the structure of the construction in the general proof, we omit the least point of a proto-line and write the number of the least point as an index to the the other two points of the proto-line. For example, for $k = 4$ (*i.e.*, $n_k = 13$) and the proto-line $(1, 3, 9)$ we will write:

12	11	10	9	8	7
1	2	3	4	5	6
		$\bullet_1$	$\circ_1$		

instead of

12	11	10	9	8	7
1	2	3	4	5	6
$\bullet$		$\bullet$	$\circ$		

This way, we can write different proto-lines in the same row without ambiguity. Later, we will omit the columns with points that appear as indices, which makes the tables less wide. For example, for $k = 8$ (*i.e.*, $n_k = 25$) the following diagram represents the three proto-lines $(1, 7, 17)$, $(2, 9, 14)$, and $(4, 6, 15)$:

24	23	22	21	20	19	18	17	16	15	14	13
1	2	3	4	5	6	7	8	9	10	11	12
					$\bullet_4$	$\bullet_1$	$\circ_1$	$\bullet_2$	$\circ_4$	$\circ_2$	

We first consider the cases when $k = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20$, and then we consider the cases when $k \geq 22$, where we will consider the four cases $k \equiv 0, 2, 4, 6 \pmod 8$ separately.

The following diagrams show the $\frac{k}{2}$ proto-lines for $k = 2, 4, \ldots, 18, 20$ (where we do not write the points which appear as indices):

5	4
2	3
$\bullet_1$	$\circ_1$

$k = 2$

10	9	8	7
3	4	5	6
$\bullet_1$	$\circ_1$	$\bullet_2$	$\bullet_2$

$k = 4$

15	14	13	12	11	10
4	5	6	7	8	9
$\bullet_1$	$\circ_1$	$\bullet_2$	$\bullet_3$	$\circ_2$	$\bullet_3$

$k = 6$

20	19	18	17	16	15	14	13
5	6	7	8	9	10	11	12
$\bullet_4$	$\bullet_2$		$\circ_2$	$\circ_4$			
		$\bullet_3$			$\circ_3$	$\bullet_1$	$\circ_1$

$k = 8$

25	24	23	22	21	20	19	18	17	16
6	7	8	9	10	11	12	13	14	15
$\bullet_4$				$\circ_4$	$\bullet_2$		$\circ_2$		
	$\bullet_1$	$\circ_1$	$\bullet_5$			$\bullet_3$		$\circ_5$	$\circ_3$

$k = 10$

30	29	28	27	26	25	24	23	22	21	20	19
7	8	9	10	11	12	13	14	15	16	17	18
				$\bullet_6$	$\bullet_4$	$\bullet_2$		$\circ_2$	$\circ_4$	$\circ_6$	
$\bullet_3$	$\bullet_1$	$\circ_1$	$\circ_3$				$\bullet_5$				$\bullet_5$

$k = 12$

35	34	33	32	31	30	29	28	27	26	25	24	23	22
8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\bullet_6$	$\bullet_4$	$\bullet_2$		$\circ_2$	$\circ_4$	$\circ_6$							
			$\bullet_7$				$\bullet_5$	$\bullet_1$	$\circ_1$	$\circ_7$	$\bullet_3$	$\circ_5$	$\bullet_3$

$k = 14$

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
$\bullet_8$	$\bullet_6$	$\bullet_4$	$\bullet_2$		$\circ_2$	$\circ_4$	$\circ_6$	$\circ_8$							
				$\bullet_7$					$\bullet_3$	$\bullet_5$	$\circ_7$	$\circ_3$	$\bullet_1$	$\circ_1$	$\circ_5$

$k = 16$

45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
$\bullet_8$	$\bullet_6$	$\bullet_4$	$\bullet_2$		$\circ_2$	$\circ_4$	$\circ_6$	$\circ_8$									
				$\bullet_9$					$\bullet_3$	$\bullet_7$	$\bullet_5$	$\circ_3$	$\circ_9$	$\bullet_1$	$\circ_1$	$\circ_5$	$\circ_7$

$k = 18$

50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\bullet_{10}$	$\bullet_8$	$\bullet_6$	$\bullet_4$	$\bullet_2$		$\circ_2$	$\circ_4$	$\circ_6$	$\circ_8$	$\circ_{10}$									
					$\bullet_9$						$\bullet_5$	$\bullet_3$	$\bullet_7$	$\circ_9$	$\circ_3$	$\circ_5$	$\bullet_1$	$\circ_1$	$\bullet_7$

$k = 20$

Notice that in the diagrams above, in the case when $k \equiv 4, 6 \pmod 8$, there is always a single proto-line which contains just points from the second row. In fact, this will always be the case. Another feature of the diagrams above is that all the numbers $1, \ldots, \frac{k}{2}$ appear as indices — also this will always be the case.

As mentioned above, for $k \geq 20$ we will consider the four cases $k \equiv 0, 2, 4, 6 \pmod 8$ separately. However, the structure of the proto-lines consisting only of even numbers is always the same. This structure is illustrated by the following diagram. In the diagram, u denotes the largest *even* number which is less than or equal to $\frac{k}{2}$ (*i.e.*, u is either $\frac{k}{2}$ or $\frac{k}{2} - 1$), $M := \frac{k+u+2}{2}$, and $N := \frac{k}{2} + 1$:

$\ldots$	N	$N+1$	$\ldots$	$M-2$	$M-1$	M	$M+1$	$M+2$	$\ldots$	$N+u-1$	$N+u$	$\ldots$
					$\bullet_2$		$\circ_2$					
				$\bullet_4$				$\circ_4$				
			$\ldots$						$\ldots$			
		$\bullet_{u-2}$								$\circ_{u-2}$		
	$\bullet_u$										$\circ_u$	

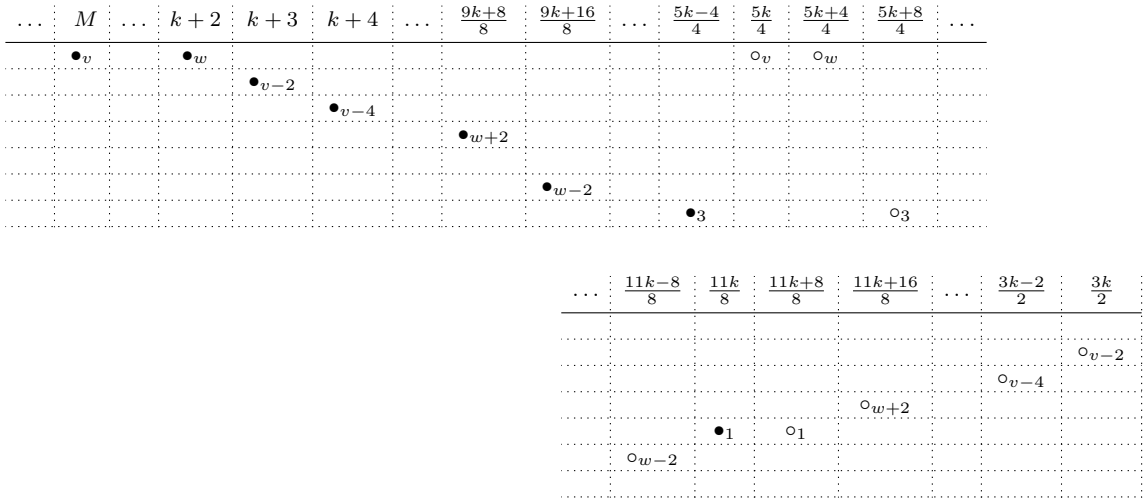
We will call these $\frac{u}{2}$ proto-lines the *even block*. Notice that the structure of the even block already appears for $k = 14, 16, 18$.

In order to complete the proof of Theorem 4, we have to construct the remaining $\frac{k}{2} - \frac{u}{2}$ proto-lines which consist only of *odd* numbers, the so-called *odd block*. The following four diagrams show the structure of these odd blocks for $k \geq 22$.

The structure of the odd block for $k \geq 24$ and $k \equiv 0 \pmod 8$

Let now $k \equiv 0 \pmod 8$ with $k \geq 24$. Then $u = \frac{k}{2}$, $M = \frac{3k}{4} + 1$, $N = \frac{k}{2} + 1$, and $N + u = k + 1$. Furthermore, let $v := \frac{k}{2} - 1$ and $w := \frac{k}{4} - 1$; then $M + v = \frac{5k}{4}$. Notice

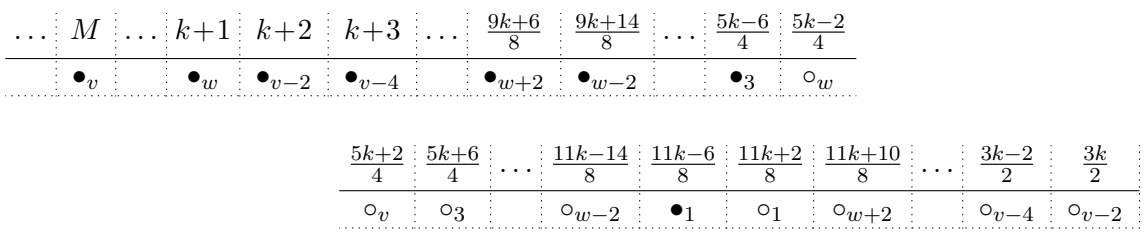
that v and w are both odd. The following diagram illustrates the construction of the odd block:



Notice that the odd block fits well with the even block: For example, the number M, which was missing in the even block, appears in the proto-line $(v, M, -(M+v)$ (recall that $M+v=\frac{5k}{4}$). Furthermore, the number $N+u+1=k+2$, which is the least number which is bigger than the maximum of the numbers in the even block, appears in the proto-line $(w, k+2, -(\frac{5k}{4}+1))$. The other numbers of the odd block are covered by the proto-lines with least number $v-2, v-4, \ldots, w+2, w-2, \ldots, 3, 1$, where the proto-line $(1, \frac{11k}{8}, -\frac{11k+8}{8})$ covers the gap between the proto-lines $(w+2, \frac{9k+8}{8}, -\frac{11k+16}{8})$ and $(w-2, \frac{9k+16}{8}, -\frac{11k-8}{8})$.

The structure of the odd block for $k \geq 26$ and $k \equiv 2 \pmod 8$

For $k \equiv 2 \pmod 8$ with $k \geq 26$ let $u=\frac{k}{2}-1$, $M=\frac{3k+2}{4}$, $N=\frac{k}{2}+1$, and $N+u=k$. Furthermore, let $v:=\frac{k}{2}$ and $w:=\frac{k-6}{4}$; then $M+v=\frac{5k+2}{4}$. The following diagram illustrates the construction of the odd block:



The structure of the odd block for $k \geq 20$ and $k \equiv 4 \pmod 8$

For $k \equiv 4 \pmod 8$ with $k \geq 20$ let $u=\frac{k}{2}$, $M=\frac{3k+4}{4}$, $N=\frac{k}{2}+1$, and $N+u=k+1$. Furthermore, let $v:=\frac{k}{2}-1$ and $w:=\frac{k+8}{4}$; then $M+v=\frac{5k}{4}$. The following diagram

illustrates the construction of the odd block:

$\dots$	M	$\dots$	$k+2$	$k+3$	$\dots$	$\frac{9k-12}{8}$	$\frac{9k-4}{8}$	$\dots$	$\frac{5k-8}{4}$	$\frac{5k-4}{4}$
	$\bullet_v$		$\bullet_{v-2}$	$\bullet_{v-4}$		$\bullet_{w+2}$	$\bullet_{w-2}$		$\bullet_3$	$\bullet_w$

$\frac{5k}{4}$	$\frac{5k+4}{4}$	$\dots$	$\frac{11k-4}{8}$	$\frac{11k+4}{8}$	$\frac{11k+12}{8}$	$\frac{11k+20}{8}$	$\dots$	$\frac{3k-4}{2}$	$\frac{3k-2}{2}$	$\frac{3k}{2}$
$\circ_v$	$\circ_3$		$\circ_{w-2}$	$\bullet_1$	$\circ_1$	$\circ_{w+2}$		$\circ_{v-4}$	$\circ_{v-2}$	$\bullet_w$

The structure of the odd block for $k \geq 22$ and $k \equiv 6 \pmod 8$

For $k \equiv 6 \pmod 8$ with $k \geq 22$ let $u = \frac{k}{2} - 1$, $M = \frac{3k+2}{4}$, $N = \frac{k}{2} + 1$, and $N + u = k$. Furthermore, let $v := \frac{k}{2}$ and $w := \frac{k-6}{4}$; then $M + v = \frac{5k+2}{4}$. The following diagram illustrates the construction of the odd block:

$\dots$	M	$\dots$	$k+1$	$k+2$	$\dots$	$\frac{9k-6}{8}$	$\frac{9k+2}{8}$	$\frac{9k+10}{8}$	$\frac{9k+18}{8}$	$\dots$	$\frac{5k-2}{4}$	$\frac{5k+2}{4}$
	$\bullet_v$		$\bullet_{v-2}$	$\bullet_{v-4}$		$\bullet_{w+2}$	$\bullet_1$	$\circ_1$	$\bullet_{w-2}$		$\bullet_3$	$\circ_v$

$\frac{5k+6}{4}$	$\frac{5k+10}{4}$	$\dots$	$\frac{11k-2}{8}$	$\frac{11k+6}{8}$	$\dots$	$\frac{3k-4}{2}$	$\frac{3k-2}{2}$	$\frac{3k}{2}$
$\bullet_w$	$\circ_3$		$\circ_{w-2}$	$\circ_{w+2}$		$\circ_{v-4}$	$\circ_{v-2}$	$\bullet_w$

Let us now consider the case $k = 2$ which yields an elliptic D_3-symmetric $(18_4, 24_3)$ configuration. Figure 4 shows one realization of the resulting configurations.

4 On elliptic $(3r_4, 4r_3)$ configurations

In order to obtain an elliptic D_3-symmetric $(9k_4, 12k_3)$ configuration, it was sufficient to construct $4k$ proto-lines in the $3k$-element set S_0. Thus, if all the proto-lines we constructed were proper lines, then we would have an elliptic $(3k_4, 4k_3)$ configuration — but this is in general not the case.

However, there is a simple algorithm which gives us elliptic $(3r_4, 4r_3)$ configurations for infinitely many values of r. The algorithm is given in the proof of the following

Proposition 5. *For every prime $p > 7$, there is an elliptic $((p-1)_3)$ configuration and for every prime $p > 7$ with $3r = p - 1$ (for some r), there is an elliptic $(3r_4, 4r_3)$ configuration.*

Proof. Let $p > 7$ be a prime, let Γ_0 be an elliptic curve, and let P be a point on Γ_0 of order $p - 1$. Furthermore, let $\mathbb{F}_p$ be the Galois field of order p. Similar as above, we will construct the elliptic configurations in $\mathbb{F}_p \setminus \{0\}$.

First recall that for any prime p, the multiplicative group $\mathbb{F}_p$ is cyclic, *i.e.*, there exists a generator $g \in \mathbb{F}_p$ such that $\operatorname{ord}(g) = p - 1$. Before we start the construction, let us prove the following claim.

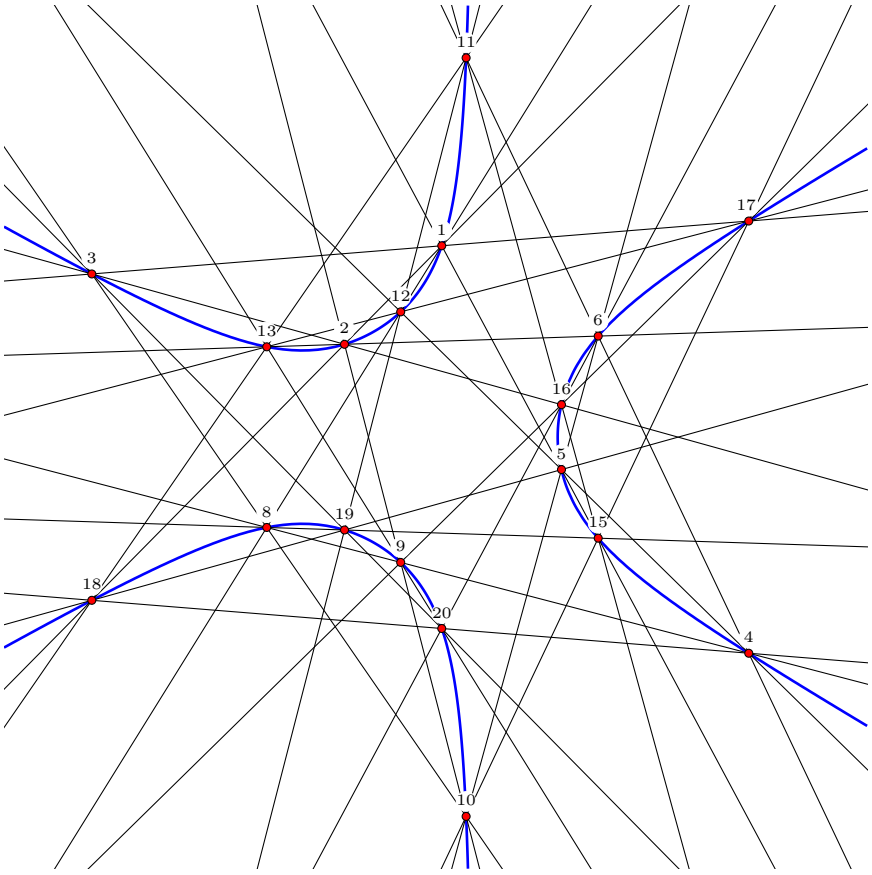


Figure 4: An elliptic D_3-symmetric $(18_4, 24_3)$ configuration.

Claim. If $p > 7$ is a prime, then the multiplicative group of $\mathbb{F}_p$ has a generator g such that $g \not\equiv -2, \frac{p-1}{2} \pmod{p}$.

Proof of Claim. If $\mathbb{F}_p$ has a generator g such that $g \not\equiv -2, \frac{p-1}{2} \pmod{p}$, then we are done. Now, assume that $g = \frac{p-1}{2}$ is a generator. Then, for any n with $1 < n < p-1$ and $(n, p-1) = 1$, g^n is also a generator. So, if we find two distinct n, m with $1 < n, m < p-1$ and $(n, p-1) = 1 = (m, p-1)$, then g, g^n, and g^m are pairwise distinct generators and we have found a generator which satisfies the conditions in the Claim. It remains to show that for every prime $p > 7$ there are distinct n, m with $1 < n, m < p-1$ such that $(n, p-1) = 1 = (m, p-1)$, which is is obviously the case.

Let now $p > 7$ be a prime and let g be a generator of the multiplicative group of $\mathbb{F}_p$ with $g \not\equiv -2, \frac{p-1}{2} \pmod{p}$ and let

$$L_0 := \left\{ \left(g^n, g^{n+1}, -(g^n + g^{n+1})\right) : 0 \leq n < p-1 \right\}.$$

Then L_0 is a set of $p-1$ lines in $\mathbb{F}_p \setminus \{0\}$. To see this, notice that by the properties of g, for all n we have $g^n \neq g^{n+1}$ and that $-(g^n + g^{n+1}) \in \{g^n, g^{n+1}\}$ would imply that $g \equiv \frac{p-1}{2} \pmod{p}$ or $g \equiv -2 \pmod{p}$.

Now, with the $p-1$ lines in $\mathbb{F}_p \setminus \{0\}$ and the point P on Γ_0 of order $p-1$, we can easily construct a $((p-1)_3)$ configuration with all its points on Γ_0.

Let us now assume that in addition to $p > 7$ we have that $p-1 = 3r$ for some $r \geq 4$, and let again g be a generator of the multiplicative group of $\mathbb{F}_p$ with $g \not\equiv -2, \frac{p-1}{2} \pmod{p}$. Let $x := g^r$ and let $y := 1+x+x^2$. Then, since $x^3 = 1$, we have $xy = y$, which implies that $x \equiv 0 \pmod{p}$ or $1+x+x^2 \equiv 0 \pmod{p}$. Since the former is impossible (recall that g is a generator of the multiplicative group of $\mathbb{F}_p$), we have that $1+x+x^2 \equiv 0 \pmod{p}$, and since $1, x, x^2$ are pairwise distinct, this implies that $(1, x, x^2)$ is a line in $\mathbb{F}_p$. Consequently,

$$L_1 := \big\{a \cdot \big(1, x, x^2\big) : a \in \mathbb{F}_p \setminus \{0\}\big\}$$

is an r-element set of lines in $\mathbb{F}_p$ which is disjoint from L_0. To see this, notice that no element of L_0 is of the form $a \cdot (1, x, x^2))$ for some $a \in \mathbb{F}_p \setminus \{0\}$ and for all $a, b \in \mathbb{F}_p \setminus \{0\}$, if $\{a, ax, ax^2\} \cap \{b, bx, bx^2\} \neq \emptyset$ then $\{a, ax, ax^2\} = \{b, bx, bx^2\}$. Thus, $L_0 \cup L_1$ is a $4r$-element set of lines in $\mathbb{F}_p \setminus \{0\}$ and together with the point P on Γ_0 of order $p-1$, we can easily construct a $(3r_4, 4r_3)$ configuration with all its points on Γ_0. *q.e.d.*

Example 4. We illustrate the construction of the previous proof for the cases $r = 6$, *i.e.*, we deal with the prime $p = 3r+1 = 19$, where we have chosen the generator $g = 3$ in the multiplicative group of $\mathbb{F}_{19}$. The set L_0 contains the lines

$$(1,3,15),(3,9,7),(9,8,2),(8,5,6),(5,15,18),(15,7,16),$$
$$(7,2,10),(2,6,11),(6,18,14),(18,16,4),(16,10,12),(10,11,17),$$
$$(11,14,13),(14,4,1),(4,12,3),(12,17,9),(17,13,8),(13,1,5).$$

The set L_1 adds the lines

$$(1,7,11),(2,3,14),(4,6,9),(5,16,17),(8,12,18),(10,13,15).$$

The resulting elliptic D_1-symmetric $(18_4, 24_3)$ configuration is shown in Figure 5 (compare to Figure 4).

We also add the case $r = 10$, *i.e.*, for the prime $p = 3r+1 = 31$. Observe that since $30 = 3r$ is not a multiple of 9, the $(30_4, 40_3)$ configuration cannot be realized by the methods from Section 3. We omit the list of points and refer directly to Figure 6.

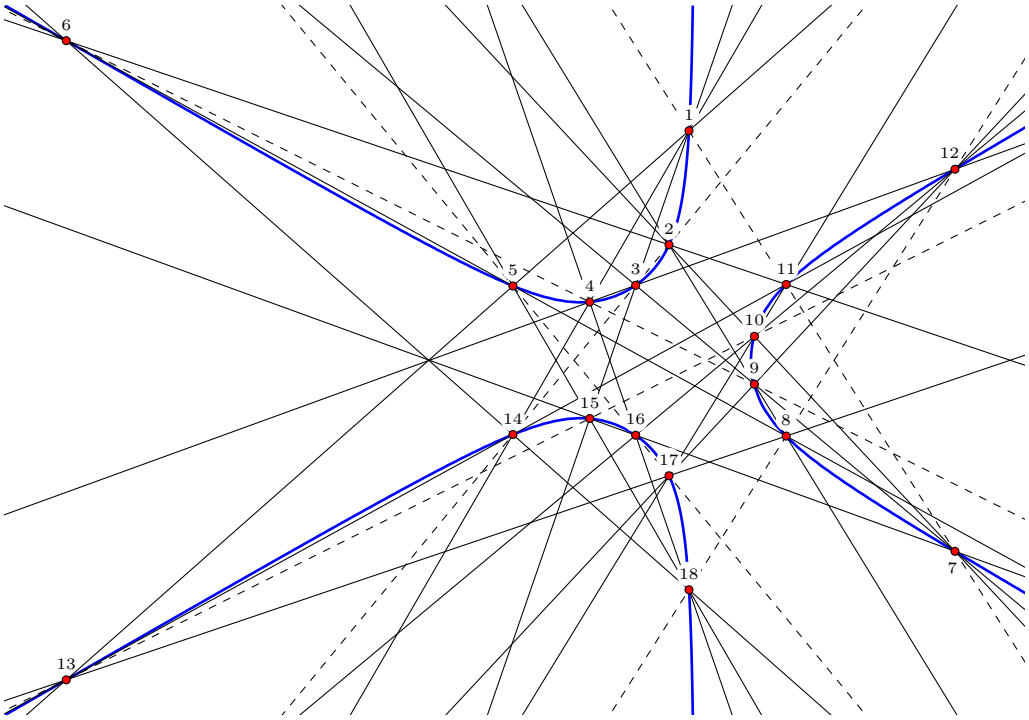


Figure 5: The solid and the dashed lines form an elliptic D_1-symmetric $(18_4, 24_3)$ configuration derived from $\mathbb{Z}/19\mathbb{Z}$. The solid lines in the set L_0 alone are an elliptic D_1-symmetric (18_3) configuration.

5 Elliptic configurations resulting from groups of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$

We conclude this paper by presenting some $(3r_4, 4r_3)$ configurations which are derived from groups of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ by similar methods. Here, the points are again constructed by using the Weierstrass $\wp$-function (see, *e.g.*, [16, p 440]). In Figure 7 we realize the group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ on an elliptic curve consisting of two components. There are 15 real points and the point $\mathscr{O}$ at infinity $(0, 1, 0)$. Using all real points the result is an elliptic D_1-symmetric $(15_4, 20_3)$ configuration. Notice that such a configuration cannot be constructed by the methods presented in Section 3 and Section 4.

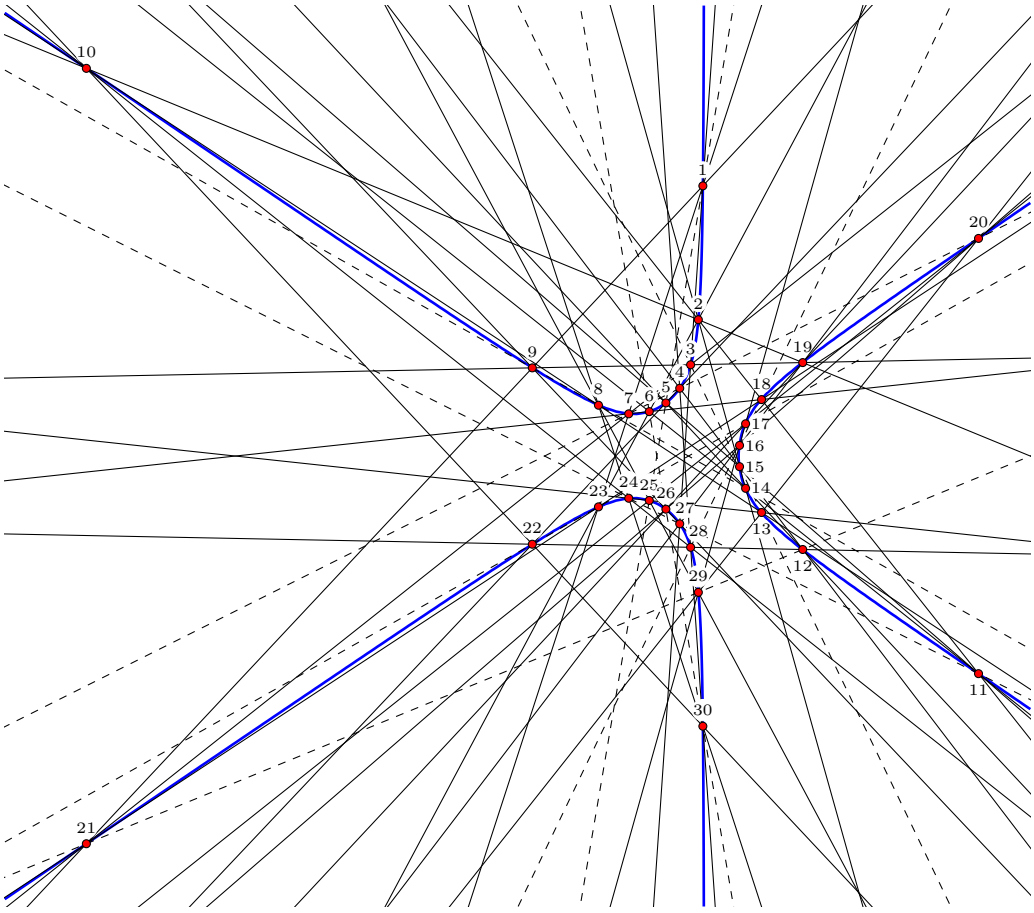


Figure 6: The solid and the dashed lines form an elliptic D_1-symmetric $(30_4, 40_3)$ configuration derived from $\mathbb{Z}/31\mathbb{Z}$, the solid lines alone are an elliptic D_1-symmetric (30_3) configuration.

Figure 8 shows an elliptic D_3-symmetric $(18_4, 24_3)$ configuration derived from the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. The group on the elliptic curve has 21 real points and 3 points at infinity. Using only 18 of the real points it is possible to realize a $(18_4, 24_3)$ configuration sitting on two components of the elliptic curve. Recall that we had a $(18_4, 24_3)$ configuration on a one component curve in Figure 4 and another one in Figure 5. It is clear that the three $(18_4, 24_3)$ configurations in Figure 8, Figure 4 and Figure 5 are not projectively isomorphic, since the respective cubic curves are not projectively isomorphic. However, the configurations could still be combinatorially isomorphic. But the Menger graphs (see [15, p. 28]) of the three configurations turn out to be non-isomorphic: The ranks of the corresponding adjacency matrices are different. In general the question may be more delicate to settle as one might have to look at the Levi graph (see [22, p. 5]) of the configurations since the Menger graphs of non-isomorphic configurations may be isomorphic (see [16], [19, Section 1.4] and the open questions in Section 6)

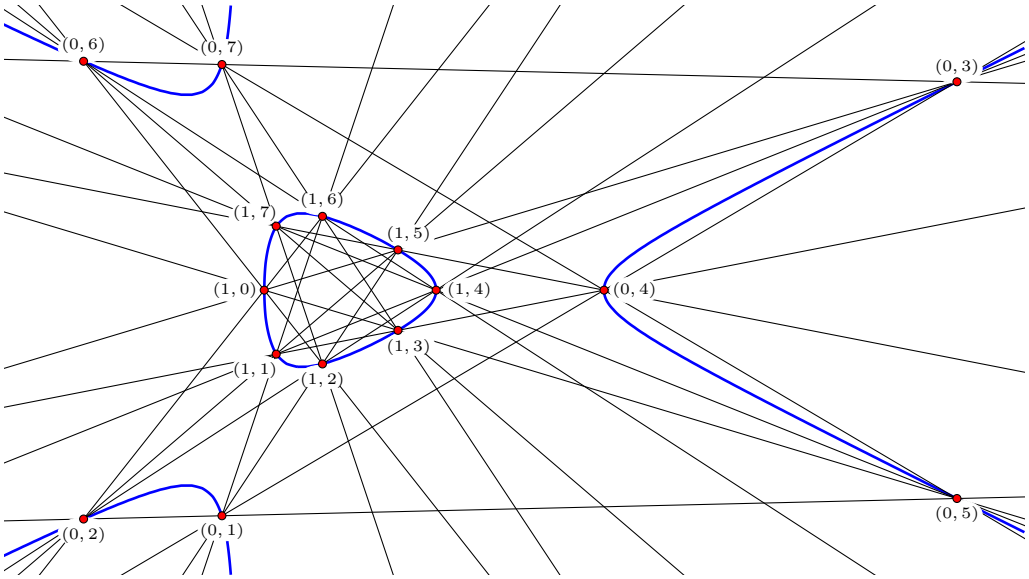


Figure 7: Elliptic D_1-symmetric $(15_4, 20_3)$ configuration derived from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

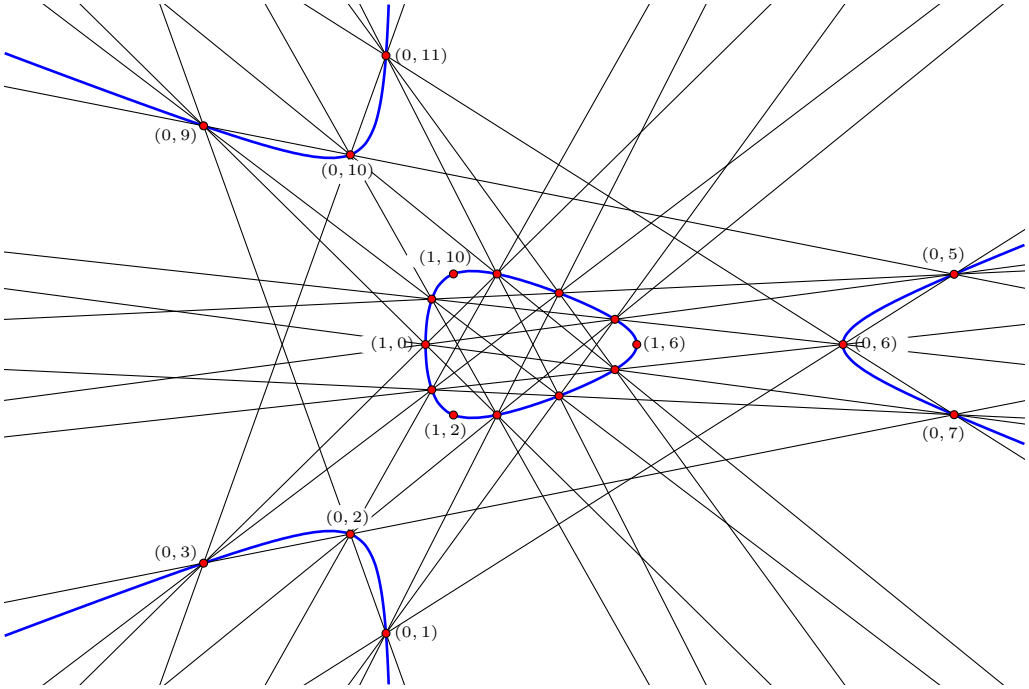


Figure 8: Elliptic D_3-symmetric $(18_4, 24_3)$ configuration derived from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

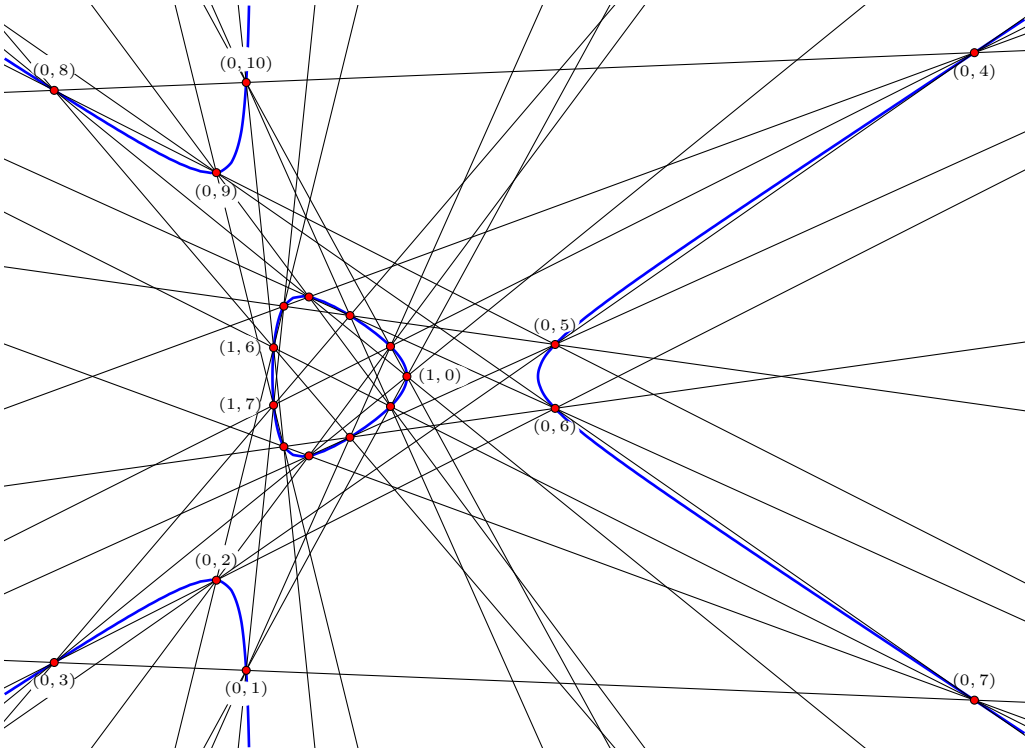


Figure 9: Elliptic D_1-symmetric $(21_4, 28_3)$ configuration derived from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$

For Figure 9 we started with the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ with 21 real points and one point at inifinity. Here, an elliptic D_1-symmetric $(21_4, 28_3)$ configuration results. Such a configuration cannot be constructed by the methods presented in Section 3 and Section 4.

Our last example starts with the group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/13\mathbb{Z}$ with 25 real points on the curve and one point at infinity. Omitting the real point corresponding to the group element $(1, 0)$ of order 2, we have 24 real points which carry an elliptic D_1-symmetric $(24_4, 32_3)$ configuration, as shown in Figure 10. Such a configuration cannot be constructed by the methods presented in Section 3 and Section 4.

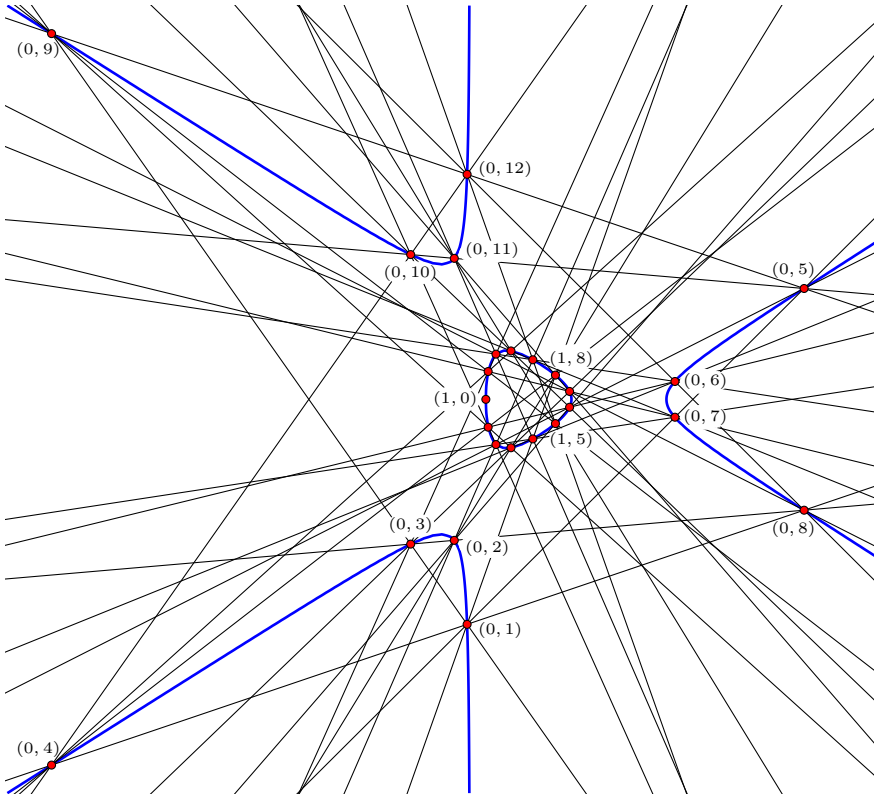


Figure 10: Elliptic D_1-symmetric $(24_4, 32_3)$ configuration derived from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$

6 Open problems

As always, with every solved problem, new questions arise. For example:

1. For certain values of r, several of the presented methods can be used to produce a $(3r_4, 4r_3)$ configuration. Even within the methods there is some freedom (*e.g.*, the choice of the generator of the respective group, or in the construction of the proto-lines). Question: Which of these configurations are combinatorially or projectively isomorphic?
2. Is it possible to generalize the methods we used for the construction of configurations starting from groups of the form $\mathbb{Z}/k\mathbb{Z}$ to groups of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ to find other $(3r_4, 4r_3)$ configurations?
3. Can the configurations that we constructed also be geometrically realized without the points lying on cubic curves? Are there realizations with other symmetry types?

Acknowledgement: We would like to thank the two referees for their careful reading and their numerous comments that helped to improve this article.

References

[1] Leah Wrenn Berman. Even astral configurations. *Electron. J. Combin.*, 11(1):Research Paper 37, 23, 2004.

[2] Leah Wrenn Berman. Some results on odd astral configurations. *Electron. J. Combin.*, 13(1):Research Paper 27, 31, 2006.

[3] Leah Wrenn Berman. Geometric constructions for 3-configurations with non-trivial geometric symmetry. *Electron. J. Combin.*, 20(3):Paper 9, 29, 2013.

[4] Leah Wrenn Berman. Geometric constructions for symmetric 6-configurations. In *Rigidity and symmetry*, volume 70 of *Fields Inst. Commun.*, pages 61–85. Springer, New York, 2014.

[5] Leah Wrenn Berman. Using conics to construct geometric 3-configurations, part I: symmetrically generalizing the Pappus configuration. *J. Geom.*, 108(2):591–609, 2017.

[6] Leah Wrenn Berman. Using conics to construct geometric 3-configurations, part II: the generalized Steiner construction. *J. Geom.*, 108(3):1055–1072, 2017.

[7] Leah Wrenn Berman and Jürgen Bokowski. Linear astral (n_5) configurations with dihedral symmetry. *European J. Combin.*, 29(8):1831–1842, 2008.

[8] Leah Wrenn Berman, Jürgen Bokowski, Branko Grünbaum, and Tomaž Pisanski. Geometric "floral" configurations. *Canad. Math. Bull.*, 52(3):327–341, 2009.

[9] Leah Wrenn Berman and Nadine Alise Burtt. A new construction for symmetric $(4, 6)$-configurations. *Ars Math. Contemp.*, 3(2):165–175, 2010.

[10] Leah Wrenn Berman, Philip DeOrsey, Jill R. Faudree, Tomaž Pisanski, and Arjana Žitnik. Chiral astral realizations of cyclic 3-configurations. *Discrete Comput. Geom.*, 64(2):542–565, 2020.

[11] Leah Wrenn Berman and Jill R. Faudree. Highly incident configurations with chiral symmetry. *Discrete Comput. Geom.*, 49(3):671–694, 2013.

[12] Leah Wrenn Berman and Branko Grünbaum. Deletion constructions of symmetric 4-configurations. Part I. *Contrib. Discrete Math.*, 5(1):18–33, 2010.

[13] Leah Wrenn Berman and William H. Mitchell. Sparse line deletion constructions for symmetric 4-configurations. *Ars Math. Contemp.*, 9(2):165–186, 2015.

[14] Leah Wrenn Berman and Laura Ng. Constructing 5-configurations with chiral symmetry. *Electron. J. Combin.*, 17(1):Research Paper 2, 14, 2010.

[15] H. S. M. Coxeter. Configurations and maps. *Rep. Math. Colloquium (2)*, 8:18–38, 1949.

[16] H. S. M. Coxeter. Self-dual configurations and regular graphs. *Bull. Amer. Math. Soc.*, 56:413–455, 1950.

[17] J. M. Feld. Configurations inscriptible in a plane cubic curve. *Amer. Math. Monthly*, 43:549–555,1936.

[18] Harald Gropp. The construction of all configurations $(12_4, 16_3)$. In *Fourth Czechoslovakian Symposium on Combinatorics, Graphs and Complexity (Prachatice, 1990)*, volume 51 of *Ann. Discrete Math.*, pages 85–91. North-Holland, Amsterdam, 1992.

[19] Branko Grünbaum. *Configurations of points and lines*, volume 103 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009.

[20] Lorenz Halbeisen and Norbert Hungerbühler. An elementary approach to Hessian curves with torsion group $\mathbb{Z}/6\mathbb{Z}$. *Int. Electron. J. Pure Appl. Math.*, 13:1–30, 2019.

[21] Lorenz Halbeisen and Norbert Hungerbühler. Constructing cubic curves with involutions. *Beitr. Algebra Geom.* (to appear). arxiv.org/abs/2106.08154

[22] Friedrich Wilhelm Levi. *Finite Geometrical Systems.* University of Calcutta, Calcutta, 1942.

[23] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186, 1977.

[24] Barry Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44:129–162, 1978.

[25] Václav Metelka. Über ebene Konfigurationen $(12_4, 16_3)$, die mit einer irreduziblen Kurve dritter Ordnung inzidieren. *Časopis Pěst. Mat.*, 091(3):261–307, 1966.

[26] Václav Metelka. On two special configurations $(12_4, 16_3)$. *Časopis Pěst. Mat.*, 110(4):351–355, 1985.

[27] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2009.