Arithmetic Progression, Primitive Isotropic Vectors, and Elliptic Curves in Conway's Lorentzian Construction

Orges Leka

April 5, 2026

Abstract

We study a simple variation of Conway's Lorentzian construction of even unimodular positive definite lattices. Instead of choosing an isotropic vector whose spatial coordinates are given by consecutive integers, we allow the coordinates to run through an arbitrary arithmetic progression

$$a,\ a+d,\ a+2d,\ \ldots,\ a+(r-1)d.$$

The first observation is that the resulting Lorentzian vector is primitive exactly when $\gcd(a,d)=1$. The second observation is that the isotropy condition can be written explicitly by Faulhaber's formulas, leading to a quadratic Diophantine equation in (a,d,r,X). If a and d are fixed, then this becomes a cubic equation in (r,X), hence, in the nonsingular case, an elliptic curve over $\mathbb{Q}$. Finally, we point out that the same coprimality condition $\gcd(a,d)=1$ appears in Dirichlet's theorem on primes in arithmetic progressions. This does not by itself imply new Lorentzian constructions, but it suggests a conceptual interface between Lorentzian lattice constructions, arithmetic progressions, and the arithmetic of elliptic curves.

Contents

1. Introduction

Conway's Lorentzian construction starts from a primitive isotropic vector in an even unimodular Lorentzian lattice and produces from it a positive definite even unimodular lattice by taking an orthogonal quotient. In the classical dimension-24 case one uses the identity

$$1^2 + 2^2 + \cdots + 24^2 = 70^2,$$

which leads to the Leech lattice through an isotropic vector in a Lorentzian lattice of signature $(25, 1)$. In a recent dimension-88 construction, one uses instead identities such as

$$192^2 + 193^2 + \cdots + 279^2 = 2222^2,$$

and obtains explicit even unimodular lattices of rank 88 by the same quotient mechanism.

The present note records a simple generalization. Instead of taking a block of consecutive integers, we allow the spatial coordinates to lie in an arbitrary arithmetic progression. This leads naturally to the following questions.

(1) When is the resulting Lorentzian vector primitive?

(2) How does the isotropy condition look in closed form?

(3) What kind of Diophantine curve is obtained if one fixes the first term and the common difference of the progression?

(4) Is there a conceptual link to analytic number theory through Dirichlet's theorem on primes in arithmetic progressions?

The first answer is elementary: primitivity is equivalent to $\gcd(a, d) = 1$. The second answer is obtained by summing squares using Faulhaber's formulas. The third answer is that for fixed (a, d) the isotropy condition defines a cubic plane curve in (r, X), hence generically an elliptic curve. The fourth answer is only conceptual rather than structural: the same coprimality condition $\gcd(a, d) = 1$ that guarantees primitive arithmetic progressions also appears in Dirichlet's theorem.

This note is meant as a short conceptual paper rather than a definitive theorem paper. It also sits naturally next to the author's earlier notes on explicit lattice constructions via Lorentzian and Paley–Krieg methods.[1]

[1]For related background, see the author's notes *A Lorentzian Construction in Dimension 88 and Infinitely*

2. Conway's Lorentzian construction from primitive isotropic vectors

We begin by recalling the general framework.

Definition 2.1. Let L be an even unimodular lattice of signature $(n, 1)$. A vector $w \in L$ is called *isotropic* if

$$(w, w) = 0,$$

and *primitive* if it is not an integral multiple of another lattice vector, equivalently if the greatest common divisor of its coordinates in any integral basis is 1.

If $w \in L$ is primitive isotropic, then the quotient

$$w^{\perp}/\mathbb{Z}w$$

is an even unimodular positive definite lattice of rank $n - 1$. This is the standard Lorentzian quotient construction.

For the purposes of this note, we consider isotropic vectors whose spatial coordinates are arranged in an arithmetic progression.

Definition 2.2. Fix integers a, d, r, X with $r \geq 1$. Define the vector

$$w(a, d, r; X) := (a, a + d, a + 2d, \ldots, a + (r - 1)d; X). \tag{1}$$

We say that (1) is an *arithmetic-progression Lorentz vector*.

In the standard Lorentzian bilinear form of signature $(r, 1)$, this vector is isotropic exactly when

$$\sum_{j=0}^{r-1} (a + jd)^2 = X^2. \tag{2}$$

Thus the construction problem becomes: find primitive integer solutions to (2).

3. Arithmetic progressions and primitivity

The first point is completely elementary but conceptually important.

Lemma 3.1. *For every pair of integers a, d and every integer $r \geq 1$ one has*

$$\gcd\bigl(a, a + d, a + 2d, \ldots, a + (r - 1)d\bigr) = \gcd(a, d).$$

Proof. Let

$$g := \gcd\bigl(a, a + d, a + 2d, \ldots, a + (r - 1)d\bigr).$$

Then g divides a and also divides

$$(a + d) - a = d.$$

Hence $g \mid \gcd(a, d)$.

Conversely, if $h := \gcd(a, d)$, then h divides a and d, hence it divides every term

$$a + jd, \qquad 0 \leq j \leq r - 1.$$

Therefore $h \mid g$. Since $g \mid h$ and $h \mid g$, we conclude that $g = h$. □

Many Further Ranks, https://www.orges-leka.de/88_lorentz_paper.pdf, and *A Generalized Krieg–Paley Construction of Even Unimodular Lattices From Dimension 24 to an Infinite Family*, https://www.orges-leka.de/krieg_generalization.pdf. For general background on modular forms and theta series, see M. Koecher and A. Krieg, *Elliptische Funktionen und Modulformen*, Springer, 1998. For elliptic curves, a standard entry point is J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer.

This gives the primitive criterion immediately.

Corollary 3.2. *The arithmetic-progression vector* (1) *is primitive as soon as*

$$\gcd(a, d) = 1.$$

In particular, primitivity depends only on the first term and the common difference of the progression.

Proof. By lemma 3.1, the gcd of the spatial coordinates is exactly $\gcd(a, d)$. If this gcd is 1, then the vector is primitive. □

Remark 3.3. This criterion is formally the same coprimality condition that appears in Dirichlet's theorem on primes in arithmetic progressions. At this stage, however, one should distinguish carefully between the two roles played by the condition $\gcd(a, d) = 1$: here it guarantees primitivity of the Lorentzian vector, while in Dirichlet's theorem it guarantees that the progression

$$a,\ a + d,\ a + 2d, \ldots$$

may contain infinitely many primes.

4. Faulhaber's formula and the isotropy condition

We now rewrite the isotropy condition explicitly.

Proposition 4.1. *For integers a, d, r with $r \geq 1$,*

$$\sum_{j=0}^{r-1}(a + jd)^2 = ra^2 + ar(r - 1)d + \frac{r(r - 1)(2r - 1)}{6}d^2. \tag{3}$$

Consequently, the isotropy condition (2) *is equivalent to*

$$ra^2 + ar(r - 1)d + \frac{r(r - 1)(2r - 1)}{6}d^2 = X^2. \tag{4}$$

Proof. Expand the square:

$$(a + jd)^2 = a^2 + 2ajd + j^2d^2.$$

Summing from $j = 0$ to $j = r - 1$ gives

$$\sum_{j=0}^{r-1}(a + jd)^2 = \sum_{j=0}^{r-1} a^2 + 2ad\sum_{j=0}^{r-1} j + d^2\sum_{j=0}^{r-1} j^2.$$

Now use the standard formulas

$$\sum_{j=0}^{r-1} 1 = r, \qquad \sum_{j=0}^{r-1} j = \frac{r(r - 1)}{2}, \qquad \sum_{j=0}^{r-1} j^2 = \frac{r(r - 1)(2r - 1)}{6}.$$

Substituting them yields

$$\sum_{j=0}^{r-1}(a + jd)^2 = ra^2 + 2ad \cdot \frac{r(r - 1)}{2} + d^2 \cdot \frac{r(r - 1)(2r - 1)}{6},$$

which simplifies to (3). The equivalence with (4) is immediate. □

Remark 4.2. Equation (4) is a quadratic Diophantine equation in the four variables (a, d, r, X). If one thinks of r as fixed, then it is a quadratic form in (a, d, X). If instead one thinks of a and d as fixed, then it becomes a cubic equation in (r, X), which is the point of view relevant for elliptic curves.

5. Fixing a and d: the elliptic-curve viewpoint

We now fix integers a and d and regard (4) as an equation in the two remaining variables (r, X).

Proposition 5.1. *For fixed integers a and d, the isotropy condition (4) is equivalent to*

$$6X^2 = 2d^2r^3 + (6ad - 3d^2)r^2 + (6a^2 - 6ad + d^2)r. \tag{5}$$

Equivalently,

$$6X^2 = r\Big(2d^2r^2 + 3d(2a - d)r + (6a^2 - 6ad + d^2)\Big). \tag{6}$$

Proof. Starting from (4), expand the quadratic and cubic terms in r:

$$ra^2 + ar(r-1)d + \frac{r(r-1)(2r-1)}{6}d^2.$$

The middle term is

$$ar(r-1)d = adr^2 - adr.$$

For the last term we compute

$$r(r-1)(2r-1) = 2r^3 - 3r^2 + r.$$

Therefore

$$X^2 = ra^2 + adr^2 - adr + \frac{d^2}{6}(2r^3 - 3r^2 + r).$$

Multiplying by 6 yields

$$6X^2 = 6a^2r + 6adr^2 - 6adr + 2d^2r^3 - 3d^2r^2 + d^2r,$$

which rearranges to (5). Factoring out r gives (6). □

This puts us in the standard framework of cubic curves.

Theorem 5.2. *Fix integers a, d with $d \neq 0$. Consider the affine curve*

$$E_{a,d}: \qquad 6X^2 = 2d^2r^3 + (6ad - 3d^2)r^2 + (6a^2 - 6ad + d^2)r. \tag{7}$$

If the cubic polynomial on the right-hand side has distinct roots over $\overline{\mathbb{Q}}$, then the smooth projective model of $E_{a,d}$ is an elliptic curve over $\mathbb{Q}$.

Proof. Equation (7) defines a plane cubic curve over $\mathbb{Q}$. A smooth projective plane cubic of genus 1 together with a rational point is an elliptic curve.

The curve has the obvious rational point

$$(r, X) = (0, 0),$$

since the right-hand side of (7) is divisible by r. Thus the only issue is nonsingularity.

A plane cubic of the form

$$Y^2 = f(r), \qquad \deg f = 3,$$

is nonsingular exactly when f has no repeated root, equivalently when its discriminant is nonzero. Under this assumption, the smooth projective model has genus 1 and possesses the rational point coming from $(0, 0)$. Therefore it is an elliptic curve over $\mathbb{Q}$. □

Remark 5.3. The singular cases correspond precisely to the vanishing of the discriminant of the cubic in r. Thus the generic situation is elliptic. In particular, for fixed primitive arithmetic progression data (a, d), the search for Lorentzian isotropic vectors of the form (1) becomes a search for integer or rational points on an elliptic curve.

Example 5.4. Take $a = 1$ and $d = 1$. Then (7) becomes

$$6X^2 = 2r^3 + 3r^2 + r = r(2r + 1)(r + 1).$$

Thus the classical "sum of consecutive squares equals a square" problem appears as the arithmetic of a concrete cubic curve.

6. A conceptual connection with Dirichlet's theorem

We now explain the conceptual bridge to analytic number theory.

Dirichlet's theorem says that if

$$\gcd(a, d) = 1,$$

then the arithmetic progression

$$a,\ a + d,\ a + 2d, \ldots$$

contains infinitely many primes. The condition $\gcd(a, d) = 1$ is therefore the correct primitive hypothesis for arithmetic progressions in analytic number theory.

On the other hand, by corollary 3.2, the same condition

$$\gcd(a, d) = 1$$

is exactly what guarantees that the arithmetic-progression Lorentz vector is primitive.

This does *not* mean that Dirichlet's theorem directly produces infinitely many Conway constructions. The missing ingredient is the isotropy condition

$$\sum_{j=0}^{r-1}(a + jd)^2 = X^2,$$

which is much stronger and genuinely Diophantine. Still, the parallel is striking enough to be worth recording.

Proposition 6.1. *The search for Lorentzian vectors built from arithmetic progressions naturally splits into two parts:*

(i) *a* primitive arithmetic progression *condition,*

$$\gcd(a, d) = 1,$$

which is formally the same hypothesis as in Dirichlet's theorem;

(ii) *an* isotropy condition*,*

$$\sum_{j=0}^{r-1}(a + jd)^2 = X^2,$$

which is equivalent to a cubic Diophantine equation and, for fixed (a, d)*, to an elliptic curve.*

Thus the arithmetic-progression Lorentz problem lies conceptually at an interface between primitive progressions, analytic number theory, and the arithmetic of elliptic curves.

Proof. Part (i) is exactly corollary 3.2. Part (ii) follows from propositions 4.1 and 5.1 and theorem 5.2. The final sentence is simply a summary of these two observations. □

7. The elliptic curve attached to a fixed arithmetic progression

In this section we fix integers a, d with $d \neq 0$ and consider the Diophantine equation

$$\sum_{j=0}^{r-1}(a + jd)^2 = X^2. \tag{8}$$

As explained above, this is the isotropy condition for the Lorentzian vector

$$w = (a, a + d, \ldots, a + (r - 1)d; X).$$

We now show that, for fixed a and d, equation (8) defines a cubic curve in the variables (r, X), and in the nonsingular case an elliptic curve over $\mathbb{Q}$.

7.1. Faulhaber reduction to a cubic equation

We begin by evaluating the left-hand side of (8). Using

$$\sum_{j=0}^{r-1} j = \frac{r(r-1)}{2}, \qquad \sum_{j=0}^{r-1} j^2 = \frac{r(r-1)(2r-1)}{6},$$

we obtain

$$\begin{aligned}\sum_{j=0}^{r-1}(a+jd)^2 &= \sum_{j=0}^{r-1}(a^2 + 2ajd + j^2d^2) \\ &= ra^2 + 2ad\sum_{j=0}^{r-1} j + d^2\sum_{j=0}^{r-1} j^2 \\ &= ra^2 + ad\,r(r-1) + \frac{d^2}{6}r(r-1)(2r-1).\end{aligned}$$

Therefore (8) is equivalent to

$$X^2 = ra^2 + ad\,r(r-1) + \frac{d^2}{6}r(r-1)(2r-1). \tag{9}$$

Expanding the right-hand side gives

$$X^2 = \frac{d^2}{3}r^3 + \left(ad - \frac{d^2}{2}\right)r^2 + \left(a^2 - ad + \frac{d^2}{6}\right)r. \tag{10}$$

Multiplying by 6, we obtain the integral model

$$6X^2 = 2d^2r^3 + 3d(2a-d)r^2 + (6a^2 - 6ad + d^2)r. \tag{11}$$

Remark 7.1. Thus, for fixed a and d, the locus of solutions (r, X) is an affine cubic curve. Since $(r, X) = (0, 0)$ is always a rational point, this is naturally a candidate for an elliptic curve after passage to Weierstrass form.

7.2. A Weierstrass model

We now convert (11) to a Weierstrass equation. Set

$$x = 12d^2r, \qquad y = 72d^2X.$$

Substituting these into (11), one checks directly that the equation becomes

$$E_{a,d}: \qquad y^2 = x^3 + 18d(2a-d)x^2 + 72d^2(6a^2 - 6ad + d^2)x. \tag{12}$$

Thus the original sum-of-squares condition defines a Weierstrass curve over $\mathbb{Q}$.

For notational convenience, let

$$M := 6a^2 - 6ad + d^2, \qquad N := d^2 + 12ad - 12a^2. \tag{13}$$

Then (12) may be written more compactly as

$$E_{a,d}: \qquad y^2 = x^3 + 18d(2a-d)x^2 + 72d^2Mx. \tag{14}$$

7.3. Discriminant and j-invariant

We now compute the basic invariants of $E_{a,d}$ explicitly.

Proposition 7.2. *Let*

$$E_{a,d}: \ y^2 = x^3 + Ax^2 + Bx$$

with

$$A = 18d(2a - d), \qquad B = 72d^2(6a^2 - 6ad + d^2) = 72d^2M.$$

Then the discriminant of $E_{a,d}$ is

$$\Delta(E_{a,d}) = 12^6\, d^6\, (6a^2 - 6ad + d^2)^2\, (d^2 + 12ad - 12a^2), \tag{15}$$

and the j-invariant is

$$j(E_{a,d}) = \frac{1728\, d^6}{(6a^2 - 6ad + d^2)^2(d^2 + 12ad - 12a^2)}. \tag{16}$$

Proof. For a Weierstrass equation of the form

$$y^2 = x^3 + Ax^2 + Bx,$$

the discriminant is

$$\Delta = 16B^2(A^2 - 4B).$$

In our case,

$$A = 18d(2a - d), \qquad B = 72d^2M.$$

A direct computation gives

$$A^2 - 4B = 36d^2N,$$

with N as in (13). Therefore

$$\Delta(E_{a,d}) = 16(72d^2M)^2(36d^2N).$$

Since

$$16 \cdot 72^2 \cdot 36 = 12^6,$$

we obtain

$$\Delta(E_{a,d}) = 12^6\, d^6\, M^2\, N,$$

which is exactly (15).

For the j-invariant, we use the standard invariant

$$c_4 = 16(A^2 - 3B).$$

Again by direct computation,

$$A^2 - 3B = 108d^4,$$

hence

$$c_4 = 16 \cdot 108d^4 = 1728d^4.$$

Therefore

$$j(E_{a,d}) = \frac{c_4^3}{\Delta(E_{a,d})} = \frac{(1728d^4)^3}{12^6 d^6 M^2 N}.$$

Simplifying gives

$$j(E_{a,d}) = \frac{1728\, d^6}{M^2 N},$$

which is (16). □

Corollary 7.3. *The j-invariant depends only on the ratio $u = a/d$. Indeed, for $d \neq 0$ and $u = a/d$, one has*

$$j(E_{a,d}) = \frac{1728}{(6u^2 - 6u + 1)^2(1 + 12u - 12u^2)}. \tag{17}$$

Proof. Write

$$6a^2 - 6ad + d^2 = d^2(6u^2 - 6u + 1),$$

and

$$d^2 + 12ad - 12a^2 = d^2(1 + 12u - 12u^2).$$

Substituting into (16), the factor d^6 cancels completely. □

Remark 7.4. In particular, the j-invariant depends on (a, d) only through the slope

$$u = \frac{a}{d}.$$

It does *not* depend on the point coordinate X. This is natural, since j is an invariant of the elliptic curve itself, not of a chosen rational point on it.

7.4. Nonsingularity

We now discuss when the cubic is singular.

Theorem 7.5. *The curve $E_{a,d}$ is singular if and only if*

$$\Delta(E_{a,d}) = 0,$$

that is, if and only if one of the following holds:

$$d = 0, \qquad 6a^2 - 6ad + d^2 = 0, \qquad d^2 + 12ad - 12a^2 = 0. \tag{18}$$

In particular, if $a, d \in \mathbb{Z}$, $d \neq 0$, then $E_{a,d}$ is automatically nonsingular.

Proof. The first statement is immediate from the discriminant formula (15). It remains to show that, for integers a, d with $d \neq 0$, the last two equations in (18) have no solutions.

If

$$6a^2 - 6ad + d^2 = 0,$$

then dividing by d^2 gives

$$6\left(\frac{a}{d}\right)^2 - 6\left(\frac{a}{d}\right) + 1 = 0.$$

The roots are

$$\frac{a}{d} = \frac{3 \pm \sqrt{3}}{6},$$

which are irrational. Hence this cannot occur for integers a, d with $d \neq 0$.

Likewise, if

$$d^2 + 12ad - 12a^2 = 0,$$

then

$$1 + 12\frac{a}{d} - 12\left(\frac{a}{d}\right)^2 = 0,$$

whose roots are

$$\frac{a}{d} = \frac{3 \pm 2\sqrt{3}}{6},$$

again irrational. Therefore this case is also impossible for integers a, d with $d \neq 0$.

Thus, for nonzero integers d, the discriminant never vanishes, and the curve is nonsingular. □

Corollary 7.6. *If $a, d \in \mathbb{Z}$, $d \neq 0$, and $\gcd(a, d) = 1$, then the equation*

$$\sum_{j=0}^{r-1} (a + jd)^2 = X^2$$

defines an elliptic curve over $\mathbb{Q}$ in the variables (r, X).

Proof. By Theorem 7.5, the associated Weierstrass model is nonsingular. Hence it is an elliptic curve. □

7.5. Conductor and bad primes

We finally record the immediate information one gets about the conductor.

Proposition 7.7. *Let $E_{a,d}$ be as above. Then every prime of bad reduction divides*

$$6d(6a^2 - 6ad + d^2)(d^2 + 12ad - 12a^2). \tag{19}$$

Equivalently, if $N(E_{a,d})$ denotes the conductor, then

$$N(E_{a,d}) = \prod_{p \mid 6dMN} p^{f_p},$$

with M, N as in (13), and the local conductor exponent f_p is zero for all primes not dividing $6dMN$.

Proof. A prime of bad reduction must divide the discriminant. By (15),

$$\Delta(E_{a,d}) = 12^6 d^6 M^2 N.$$

Hence every prime dividing the conductor must divide $12dMN$, which is equivalent to (19). □

Remark 7.8. For primes $p \nmid 6d$, one has $c_4 = 1728d^4 \not\equiv 0 \pmod{p}$. Hence if $p \mid MN$ but $p \nmid 6d$, the reduction is multiplicative and the local conductor exponent is $f_p = 1$. The difficult primes are therefore those dividing $6d$, in particular 2, 3, and the prime divisors of d. Their exact exponents are determined by the Tate algorithm.

Remark 7.9. Thus the arithmetic progression Ansatz leads naturally from Lorentzian lattice constructions to an explicit family of elliptic curves over $\mathbb{Q}$, with completely explicit discriminant and j-invariant. This provides a conceptual bridge between:

1. primitive isotropic vectors in Lorentzian lattices,
2. arithmetic progressions and their sums of squares,
3. and the arithmetic of elliptic curves.

8. GCD-normalization, the associated elliptic curve, and a Szpiro-type conjecture

In this section we allow arbitrary integers a, d with $d \neq 0$, and reduce them to a primitive pair by dividing out the common divisor. This leads to a canonical elliptic curve attached to the arithmetic progression

$$a,\ a + d,\ a + 2d,\ \ldots,\ a + (r - 1)d.$$

We then compare this family with the Frey–Hellegouarch curve and formulate a natural Szpiro-type conjecture for this setting.

8.1. GCD-normalization

Let

$$g := \gcd(a, d), \qquad a = g\alpha, \qquad d = g\delta,$$

so that

$$\gcd(\alpha, \delta) = 1.$$

Consider the Diophantine equation

$$\sum_{j=0}^{r-1}(a + jd)^2 = X^2. \tag{20}$$

Since

$$a + jd = g(\alpha + j\delta),$$

we have

$$\sum_{j=0}^{r-1}(a + jd)^2 = g^2 \sum_{j=0}^{r-1}(\alpha + j\delta)^2.$$

Therefore, any integral solution of (20) satisfies

$$g^2 \sum_{j=0}^{r-1}(\alpha + j\delta)^2 = X^2.$$

Hence $g \mid X$, so we may write

$$X = gY.$$

Substituting this into (20), we obtain the primitive equation

$$\sum_{j=0}^{r-1}(\alpha + j\delta)^2 = Y^2. \tag{21}$$

Thus the arithmetic of the general pair (a, d) reduces canonically to the primitive pair (α, δ).

Proposition 8.1. *For arbitrary integers a, d with $d \neq 0$, let $g = \gcd(a, d)$ and write $a = g\alpha$, $d = g\delta$ with $\gcd(\alpha, \delta) = 1$. Then the Diophantine equation*

$$\sum_{j=0}^{r-1}(a + jd)^2 = X^2$$

has an integer solution (r, X) if and only if

$$\sum_{j=0}^{r-1}(\alpha + j\delta)^2 = Y^2$$

has an integer solution (r, Y), in which case $X = gY$.

Proof. This follows immediately from the identity

$$\sum_{j=0}^{r-1}(a + jd)^2 = g^2 \sum_{j=0}^{r-1}(\alpha + j\delta)^2.$$

If the left-hand side is a square, then g^2 divides X^2, hence $g \mid X$, and writing $X = gY$ yields the primitive equation. The converse is immediate. □

8.2. The primitive elliptic curve

For fixed (α, δ) with $\gcd(\alpha, \delta) = 1$, the primitive equation (21) leads, by the Faulhaber reduction, to the cubic

$$6Y^2 = 2\delta^2 r^3 + 3\delta(2\alpha - \delta)r^2 + (6\alpha^2 - 6\alpha\delta + \delta^2)r.$$

As in the previous section, after the change of variables

$$x = 12\delta^2 r, \qquad y = 72\delta^2 Y,$$

one obtains the Weierstrass model

$$E_{\alpha,\delta}: \qquad y^2 = x^3 + 18\delta(2\alpha - \delta)x^2 + 72\delta^2(6\alpha^2 - 6\alpha\delta + \delta^2)x. \tag{22}$$

For the nonprimitive pair $(a, d) = (g\alpha, g\delta)$, the corresponding model is

$$E_{a,d}: \qquad y^2 = x^3 + 18g^2\delta(2\alpha - \delta)x^2 + 72g^4\delta^2(6\alpha^2 - 6\alpha\delta + \delta^2)x. \tag{23}$$

Proposition 8.2. *The curves $E_{a,d}$ and $E_{\alpha,\delta}$ are isomorphic over $\mathbb{Q}$. More precisely, the change of variables*

$$x = g^2 u, \qquad y = g^3 v$$

transforms (23) *into* (22).

Proof. Substitute

$$x = g^2 u, \qquad y = g^3 v$$

into (23). Then

$$g^6 v^2 = g^6 u^3 + 18g^6\delta(2\alpha - \delta)u^2 + 72g^6\delta^2(6\alpha^2 - 6\alpha\delta + \delta^2)u.$$

Dividing by g^6 gives exactly (22). □

Remark 8.3. Thus all birational and isomorphism-invariant arithmetic of the family depends only on the primitive ratio

$$\frac{a}{d} = \frac{\alpha}{\delta}.$$

In particular, the j-invariant and the conductor are unchanged under this normalization.

8.3. Discriminant, j-invariant, and conductor support

Set

$$M_0 := 6\alpha^2 - 6\alpha\delta + \delta^2, \qquad N_0 := \delta^2 + 12\alpha\delta - 12\alpha^2.$$

Then the primitive curve takes the form

$$E_{\alpha,\delta}: \qquad y^2 = x^3 + 18\delta(2\alpha - \delta)x^2 + 72\delta^2 M_0\, x.$$

By the computation carried out in the previous section, the discriminant of this model is

$$\Delta(E_{\alpha,\delta}) = 12^6\, \delta^6\, M_0^2\, N_0, \tag{24}$$

and its j-invariant is

$$j(E_{\alpha,\delta}) = \frac{1728\, \delta^6}{M_0^2 N_0}. \tag{25}$$

For the nonprimitive model $E_{a,d}$ one has the scaling relation

$$\Delta(E_{a,d}) = g^{12}\Delta(E_{\alpha,\delta}), \tag{26}$$

while

$$j(E_{a,d}) = j(E_{\alpha,\delta}). \tag{27}$$

Proof. Equation (26) follows from the general behavior of the discriminant under

$$x = g^2 u, \qquad y = g^3 v,$$

namely a scaling factor of g^{12}. The equality (27) holds because j is invariant under isomorphism over $\mathbb{Q}$. □

Since the conductor is also invariant under $\mathbb{Q}$-isomorphism, we have

$$N(E_{a,d}) = N(E_{\alpha,\delta}). \tag{28}$$

Moreover, every prime of bad reduction must divide the discriminant, hence every prime dividing the conductor must lie in the support of

$$6\delta\, M_0\, N_0. \tag{29}$$

In particular,

$$\mathrm{Supp}\big(N(E_{\alpha,\delta})\big) \subseteq \{p :\ p \mid 6\delta M_0 N_0\}.$$

For primes $p \nmid 6\delta$, if $p \mid M_0 N_0$, then the reduction is multiplicative and the local conductor exponent is 1.

8.4. Dependence on the ratio $u = \alpha/\delta$

Putting

$$u = \frac{\alpha}{\delta},$$

the j-invariant simplifies to

$$j(u) = \frac{1728}{(6u^2 - 6u + 1)^2(1 + 12u - 12u^2)}. \tag{30}$$

Thus the j-invariant depends only on the slope $u = \alpha/\delta = a/d$.

8.5. Comparison with the Frey–Hellegouarch curve

The natural comparison object is the Frey–Hellegouarch curve attached to an abc-triple $A + B = C$,

$$E^{\mathrm{Frey}}_{A,B} : \qquad y^2 = x(x - A)(x + B).$$

Its discriminant is essentially

$$\Delta(E^{\mathrm{Frey}}_{A,B}) \asymp (ABC)^2,$$

and its conductor is supported on the radical of ABC, up to a bounded power of 2.

The family $E_{\alpha,\delta}$ above has a similar flavor:

1. it is defined from a structured Diophantine input, namely an arithmetic progression;
2. it has a visible rational 2-torsion point at $(x, y) = (0, 0)$;
3. its discriminant is given explicitly by a product of natural arithmetic factors,
$$\Delta(E_{\alpha,\delta}) = 12^6 \delta^6 M_0^2 N_0;$$
4. its conductor is supported on the radical of an explicit arithmetic quantity,
$$6\delta M_0 N_0.$$

Thus $E_{\alpha,\delta}$ may be viewed as an "arithmetic progression analogue" of a Frey-type curve: instead of encoding an additive relation $A + B = C$, it encodes the quadratic relation

$$\sum_{j=0}^{r-1} (\alpha + j\delta)^2 = Y^2.$$

8.6. A Szpiro-type conjecture for arithmetic progressions

Szpiro's conjecture predicts that for elliptic curves over $\mathbb{Q}$ with minimal discriminant $\Delta_{\min}$ and conductor N,

$$|\Delta_{\min}| \leq C_\varepsilon N^{6+\varepsilon}$$

for every $\varepsilon > 0$, with a constant C_ε depending only on ε. A modified form of Szpiro's conjecture is equivalent to the abc conjecture.

Applied to our family, this motivates the following specialization.

Conjecture 8.4 (Arithmetic-progression Szpiro principle)**.** *For every $\varepsilon > 0$ there exists a constant $C_\varepsilon > 0$ such that for all coprime integers α, δ with $\delta \neq 0$, the nonsingular curve $E_{\alpha,\delta}$ satisfies*

$$|\Delta_{\min}(E_{\alpha,\delta})| \leq C_\varepsilon \, N(E_{\alpha,\delta})^{6+\varepsilon}. \tag{31}$$

Equivalently, at the level of the explicit model, one expects the arithmetic factor

$$\delta^6 M_0^2 N_0$$

to be controlled, up to bounded model-theoretic correction, by the conductor supported on

$$6\delta M_0 N_0.$$

A more elementary radical version is the following.

Conjecture 8.5 (Radical form)**.** *For every $\varepsilon > 0$ there exists a constant $C_\varepsilon > 0$ such that for all coprime integers α, δ with $\delta \neq 0$,*

$$|\delta^6 M_0^2 N_0| \leq C_\varepsilon \, \mathrm{rad}(6\delta M_0 N_0)^{6+\varepsilon}, \tag{32}$$

where

$$M_0 = 6\alpha^2 - 6\alpha\delta + \delta^2, \qquad N_0 = \delta^2 + 12\alpha\delta - 12\alpha^2.$$

Remark 8.6. Conjecture 8.5 should be viewed as a family-level shadow of Szpiro's conjecture rather than as an independent statement. Its interest lies in the fact that it is completely explicit in the arithmetic progression parameters.

8.7. A genuinely new family-level question

The previous conjectures are specializations of known conjectural principles. A genuinely family-specific problem is the following.

Conjecture 8.7 (Arithmetic progression square-sum growth)**.** *Let $\gcd(\alpha, \delta) = 1$, $\delta \neq 0$, and suppose*

$$\sum_{j=0}^{r-1} (\alpha + j\delta)^2 = Y^2$$

for some integer $r \geq 1$. Then the associated rational point on $E_{\alpha,\delta}$ has canonical height bounded below by

$$\hat{h}(P_{r,Y}) \geq c_1 \log r - c_2$$

with constants $c_1 > 0$, $c_2 \in \mathbb{R}$ depending only on the family and not on the individual solution.

This conjecture expresses the expectation that large arithmetic progression square-sum solutions should correspond to arithmetically large points on the attached elliptic curve.

8.8. Prime parameters, a Szpiro-type prediction, and numerical verification

We now specialize the arithmetic progression family to the case

$$a = p, \qquad d = q,$$

where p and q are distinct prime numbers. Since $\gcd(p, q) = 1$, the gcd-normalization is trivial, and the primitive pair is simply $(\alpha, \delta) = (p, q)$.

Define

$$M_{p,q} := 6p^2 - 6pq + q^2, \qquad N_{p,q} := q^2 + 12pq - 12p^2. \tag{33}$$

Then the associated elliptic curve is

$$E_{p,q} : \qquad y^2 = x^3 + 18q(2p - q)x^2 + 72q^2 M_{p,q}\, x. \tag{34}$$

By the general formulas established above, its discriminant is

$$\Delta(E_{p,q}) = 12^6\, q^6\, M_{p,q}^2\, N_{p,q}, \tag{35}$$

and its j-invariant is

$$j(E_{p,q}) = \frac{1728\, q^6}{M_{p,q}^2 N_{p,q}}. \tag{36}$$

Moreover, every prime of bad reduction divides

$$6q\, M_{p,q}\, N_{p,q}, \tag{37}$$

so the conductor satisfies

$$N(E_{p,q}) = \prod_{\ell \mid 6qM_{p,q}N_{p,q}} \ell^{f_\ell}.$$

For primes $\ell \nmid 6q$ with $\ell \mid M_{p,q}N_{p,q}$, the reduction is multiplicative and hence $f_\ell = 1$.

Remark 8.8. Thus the prime-parameter family $E_{p,q}$ is an especially explicit two-parameter subfamily of the arithmetic progression curves. It may be viewed as a "prime Frey-type family", since the discriminant contains visible high powers,

$$\Delta(E_{p,q}) = 12^6 q^6 M_{p,q}^2 N_{p,q},$$

while the conductor is supported on the radical of the arithmetic quantity

$$6qM_{p,q}N_{p,q}.$$

This is directly analogous in spirit to the Frey–Hellegouarch philosophy, where the discriminant contains large powers while the conductor is governed by the radical of the input data.

Conjecture 8.9 (Prime arithmetic progression Szpiro principle)**.** *For every $\varepsilon > 0$ there exists a constant $C_\varepsilon > 0$ such that for all distinct primes p, q one has*

$$\left|\Delta_{\min}(E_{p,q})\right| \le C_\varepsilon\, N(E_{p,q})^{6+\varepsilon}. \tag{38}$$

Equivalently, at the level of the explicit model (34), one expects

$$|q^6 M_{p,q}^2 N_{p,q}| \ll_\varepsilon \operatorname{rad}(6qM_{p,q}N_{p,q})^{6+\varepsilon}. \tag{39}$$

Remark 8.10. This conjecture is not intended as a new principle independent of Szpiro or abc. Rather, it is a concrete family-level specialization of the Szpiro/abc philosophy to the explicit arithmetic progression curves (34). What is new is the appearance of the two specific quadratic forms

$$M_{p,q} = 6p^2 - 6pq + q^2, \qquad N_{p,q} = q^2 + 12pq - 12p^2,$$

which arise naturally from the Conway–Lorentz arithmetic progression Ansatz.

Numerical verification for all prime pairs $p, q \le 100$

We verified with `SymPy` that for all ordered pairs of distinct primes

$$(p, q), \qquad p \neq q, \qquad p, q \le 100,$$

the following hold:

1. the explicit discriminant formula (35) agrees with the discriminant computed directly from the cubic polynomial
$$x^3 + 18q(2p - q)x^2 + 72q^2 M_{p,q} x;$$
2. the explicit formula (36) agrees with the invariant expression
$$j = \frac{c_4^3}{\Delta};$$
3. no singular case occurs in this range;
4. the radical ratio
$$R_6(p, q) := \frac{|\Delta(E_{p,q})|}{\mathrm{rad}(6qM_{p,q}N_{p,q})^6}$$
remains bounded throughout the sample.

In fact, among all 600 ordered prime pairs with $p \neq q$ and $p, q \le 100$, the maximal value observed was

$$R_6(3, 2) = \frac{524288}{14641} \approx 35.81.$$

This does not prove the conjecture, of course, but it is consistent with the expected Szpiro-type behavior of the family.

9. Arithmetic progressions with coprime moduli

In this section we fix a block length $r \ge 1$ and study a single arithmetic progression

$$a,\ a + d,\ a + 2d,\ a + 3d,\ \ldots$$

with

$$\gcd(a, d) = 1.$$

We divide this progression into consecutive blocks of length r:

$$B_m(a, d; r) := (a + rmd,\ a + (rm + 1)d,\ \ldots,\ a + (rm + r - 1)d), \qquad m \ge 0.$$

The natural Lorentzian vector attached to the m-th block is

$$w_m = (0,\ a + rmd,\ a + (rm + 1)d, \ldots, a + (rm + r - 1)d;\ X_m).$$

We say that the block $B_m(a, d; r)$ is *isotropic* if there exists an integer X_m such that

$$\sum_{j=0}^{r-1} \big(a + (rm + j)d\big)^2 = X_m^2. \tag{40}$$

Because we have inserted an initial 0, the corresponding Conway–Lorentz vector has $r + 1$ spatial coordinates and one time coordinate. The extra zero does not change the isotropy equation, but it does ensure that the resulting Conway quotient has rank r.

The goal of this section is to answer the following structural question.

Question. For fixed r, fixed a, and fixed d with $\gcd(a, d) = 1$, are there only finitely many isotropic blocks?

The answer depends entirely on whether r is a square.

Step 1: every block is primitive

We begin with the easy but important observation that all blocks remain primitive as long as the initial progression is primitive.

Lemma 9.1. *Let $r \geq 1$, let $m \geq 0$, and set*

$$A_m := a + rmd.$$

Then

$$\gcd(A_m, d) = \gcd(a, d).$$

In particular, if $\gcd(a, d) = 1$, then every block

$$B_m(a, d; r) = (A_m, A_m + d, \ldots, A_m + (r-1)d)$$

is primitive in the sense that

$$\gcd(A_m, A_m + d, \ldots, A_m + (r-1)d) = 1.$$

Proof. Since $A_m = a + rmd$, we have

$$A_m - a = rmd.$$

Therefore any common divisor of a and d also divides A_m and d, so

$$\gcd(a, d) \mid \gcd(A_m, d).$$

Conversely, any common divisor of A_m and d divides

$$A_m - rmd = a,$$

so it divides both a and d. Hence

$$\gcd(A_m, d) \mid \gcd(a, d).$$

The two divisibilities imply

$$\gcd(A_m, d) = \gcd(a, d).$$

Finally, for any arithmetic progression one has

$$\gcd(A_m, A_m + d, \ldots, A_m + (r-1)d) = \gcd(A_m, d),$$

because the difference of consecutive terms is d, and conversely every common divisor of A_m and d divides all terms. Thus if $\gcd(a, d) = 1$, then the whole block has greatest common divisor 1. □

So the primitive condition is completely stable under passage from one block to the next.

Step 2: rewrite isotropy in a uniform way

The next step is to rewrite the isotropy equation in a form better suited for arithmetic analysis.

Proposition 9.2. *Let*

$$A_m := a + rmd.$$

Then the block $B_m(a, d; r)$ is isotropic if and only if

$$X_m^2 = rA_m^2 + r(r-1)dA_m + \frac{r(r-1)(2r-1)}{6}d^2. \tag{41}$$

Proof. We begin with

$$\sum_{j=0}^{r-1}(A_m + jd)^2.$$

Expanding the square gives

$$(A_m + jd)^2 = A_m^2 + 2A_m jd + j^2 d^2.$$

Summing from $j = 0$ to $j = r - 1$ yields

$$\sum_{j=0}^{r-1}(A_m + jd)^2 = \sum_{j=0}^{r-1} A_m^2 + 2A_m d \sum_{j=0}^{r-1} j + d^2 \sum_{j=0}^{r-1} j^2.$$

We now use the standard formulas

$$\sum_{j=0}^{r-1} 1 = r, \qquad \sum_{j=0}^{r-1} j = \frac{r(r-1)}{2}, \qquad \sum_{j=0}^{r-1} j^2 = \frac{r(r-1)(2r-1)}{6}.$$

Substituting these into the previous expression gives

$$\sum_{j=0}^{r-1}(A_m + jd)^2 = rA_m^2 + 2A_m d \cdot \frac{r(r-1)}{2} + d^2 \cdot \frac{r(r-1)(2r-1)}{6}.$$

The middle term simplifies to $r(r-1)dA_m$, so we obtain exactly

$$\sum_{j=0}^{r-1}(A_m + jd)^2 = rA_m^2 + r(r-1)dA_m + \frac{r(r-1)(2r-1)}{6}d^2.$$

Thus equation (40) is equivalent to (41). □

This is already enough to see that, for fixed r, a, d, isotropic blocks are governed by a quadratic equation in the block index m, since $A_m = a + rmd$ is affine in m. However, the most useful form is obtained after completing the square.

Theorem 9.3. *Fix integers $r \geq 1$, a, and $d \neq 0$, and let*

$$A_m = a + rmd.$$

Define

$$U := 2X_m, \qquad Y := 2A_m + (r-1)d. \tag{42}$$

Then the isotropy equation for the m-th block is equivalent to the Pell-type equation

$$U^2 - rY^2 = \frac{r(r^2-1)}{3}d^2. \tag{43}$$

Moreover, Y is constrained by the congruence

$$Y \equiv 2a + (r-1)d \pmod{2rd}. \tag{44}$$

Conversely, any integer solution (U, Y) of (43) satisfying (44) arises from a unique integer block index

$$m = \frac{Y - (2a + (r-1)d)}{2rd}, \tag{45}$$

and then yields an isotropic block.

Proof. Start from Proposition 9.2:

$$X_m^2 = rA_m^2 + r(r-1)dA_m + \frac{r(r-1)(2r-1)}{6}d^2.$$

Multiply by 4:

$$4X_m^2 = 4rA_m^2 + 4r(r-1)dA_m + \frac{2r(r-1)(2r-1)}{3}d^2.$$

By the definition $U = 2X_m$, the left-hand side is U^2. We now want to recognize the first two terms on the right as part of rY^2.

By definition,

$$Y = 2A_m + (r-1)d.$$

Therefore

$$Y^2 = (2A_m + (r-1)d)^2 = 4A_m^2 + 4(r-1)dA_m + (r-1)^2d^2.$$

Multiplying by r gives

$$rY^2 = 4rA_m^2 + 4r(r-1)dA_m + r(r-1)^2d^2.$$

Subtracting this from the expression for U^2 gives

$$U^2 - rY^2 = \frac{2r(r-1)(2r-1)}{3}d^2 - r(r-1)^2d^2.$$

Factor out $r(r-1)d^2$:

$$U^2 - rY^2 = r(r-1)d^2\left(\frac{2(2r-1)}{3} - (r-1)\right).$$

Now simplify the bracket:

$$\frac{2(2r-1)}{3} - (r-1) = \frac{4r-2}{3} - \frac{3r-3}{3} = \frac{r+1}{3}.$$

Hence

$$U^2 - rY^2 = r(r-1)d^2 \cdot \frac{r+1}{3} = \frac{r(r^2-1)}{3}d^2,$$

which proves (43).

Next, because $A_m = a + rmd$, we have

$$Y = 2A_m + (r-1)d = 2a + 2rmd + (r-1)d.$$

This shows immediately that

$$Y - (2a + (r-1)d) = 2rmd,$$

so

$$Y \equiv 2a + (r-1)d \pmod{2rd}.$$

This is (44).

Conversely, suppose (U, Y) is an integer solution of (43) and that (44) holds. Then the congruence implies that

$$Y - (2a + (r-1)d)$$

is divisible by $2rd$, so the formula (45) defines an integer m. By construction,

$$Y = 2(a + rmd) + (r-1)d = 2A_m + (r-1)d.$$

Substituting this identity into (43) and reversing the previous algebra shows that

$$U^2 = 4\left(rA_m^2 + r(r-1)dA_m + \frac{r(r-1)(2r-1)}{6}d^2\right).$$

Since U is even whenever the right-hand side is divisible by 4 (and in our construction $U = 2X_m$), we recover an integer $X_m = U/2$ satisfying the isotropy equation. Uniqueness of m follows from the explicit formula (45). □

This theorem is the key structural statement. It says that, once r, a, d are fixed, the isotropic blocks are exactly the integer points of a Pell-type conic together with one fixed congruence condition.

Step 3: finiteness when r is a square

We can now answer the finiteness question in the square case.

Theorem 9.4. *Assume that $r = s^2$ is a perfect square. Fix integers a, d with $d \neq 0$ and $\gcd(a, d) = 1$. Then there are only finitely many isotropic blocks of length r in the progression*

$$a,\ a+d,\ a+2d, \ldots.$$

Proof. By Theorem 9.3, isotropic blocks correspond to integer solutions of

$$U^2 - rY^2 = \frac{r(r^2-1)}{3}d^2.$$

If $r = s^2$, then this becomes

$$U^2 - s^2Y^2 = \frac{s^2(s^4-1)}{3}d^2.$$

Factor the left-hand side:

$$(U - sY)(U + sY) = \frac{s^2(s^4-1)}{3}d^2.$$

The right-hand side is a fixed nonzero integer depending only on r and d. An integer has only finitely many factorizations into a product of two integers. Therefore there are only finitely many pairs

$$(U - sY,\ U + sY)$$

and hence only finitely many pairs (U, Y) solving the equation.

Finally, each such pair (U, Y) gives at most one block index m through the formula

$$m = \frac{Y - (2a + (r-1)d)}{2rd}.$$

Therefore there are only finitely many integers m for which the block $B_m(a, d; r)$ is isotropic. □

Remark 9.5. This is exactly the mechanism we observed earlier for $r = 16$. Since $16 = 4^2$ is a square, the Pell-type equation degenerates to a factorization problem, and only finitely many blocks can occur.

Step 4: the non-square case

When r is not a square, the behavior is completely different.

Theorem 9.6. *Assume that $r \geq 2$ is not a perfect square. Fix integers a, d with $d \neq 0$ and $\gcd(a, d) = 1$. Then the set of isotropic blocks of length r is either empty or infinite.*

Proof. Again, by Theorem 9.3, isotropic blocks correspond to integer solutions of

$$U^2 - rY^2 = C, \qquad C := \frac{r(r^2-1)}{3}d^2, \tag{46}$$

subject to the congruence condition

$$Y \equiv 2a + (r-1)d \pmod{2rd}.$$

Suppose first that there are no solutions to (46) satisfying the congruence. Then there are no isotropic blocks, and we are done.

Now suppose that there exists at least one isotropic block. Then there exists at least one integer solution (U_0, Y_0) of (46) satisfying the congruence.

Because r is not a square, the real quadratic field $\mathbb{Q}(\sqrt{r})$ has infinitely many units of norm 1. Concretely, there exists a fundamental unit

$$\varepsilon = u_1 + v_1\sqrt{r} > 1$$

with

$$u_1^2 - rv_1^2 = 1.$$

For each $n \geq 0$, define

$$U_n + Y_n\sqrt{r} := (U_0 + Y_0\sqrt{r})\,\varepsilon^n.$$

Taking norms from $\mathbb{Q}(\sqrt{r})$ to $\mathbb{Q}$ gives

$$U_n^2 - rY_n^2 = (U_0^2 - rY_0^2)(u_1^2 - rv_1^2)^n = C \cdot 1^n = C.$$

Thus each (U_n, Y_n) is again an integer solution of (46). Since $\varepsilon > 1$, these solutions are distinct and unbounded.

So far we have produced infinitely many solutions of the Pell-type equation, but we still need to preserve the congruence condition on Y. For this, reduce the sequence modulo $2rd$. Because there are only finitely many residue classes modulo $2rd$, the sequence

$$(Y_n \bmod 2rd)$$

is eventually periodic; in fact the whole pair (U_n, Y_n) modulo $2rd$ is periodic because multiplication by ε acts through a finite group of units modulo $2rd$.

Hence there exists a positive integer N such that multiplication by ε^N acts trivially on the residue class of (U_0, Y_0) modulo $2rd$. It follows that the subsequence

$$(U_{kN}, Y_{kN}), \qquad k = 0, 1, 2, \ldots,$$

satisfies

$$Y_{kN} \equiv Y_0 \pmod{2rd}$$

for all k. Since Y_0 already satisfies

$$Y_0 \equiv 2a + (r-1)d \pmod{2rd},$$

the same is true for every Y_{kN}. Therefore every (U_{kN}, Y_{kN}) corresponds to an isotropic block.

Finally, the block index attached to (U_{kN}, Y_{kN}) is

$$m_k = \frac{Y_{kN} - (2a + (r-1)d)}{2rd}.$$

As the values Y_{kN} are unbounded and distinct, the integers m_k are also unbounded and distinct. Hence there are infinitely many isotropic blocks. □

Corollary 9.7. *Fix $r \geq 1$, $d \neq 0$, and $\gcd(a, d) = 1$. Then:*

(i) *if r is a square, there are only finitely many isotropic blocks of length r;*

(ii) *if r is not a square, there are either no isotropic blocks or infinitely many.*

Proof. If $r = 1$, every block has length one, and

$$a + md$$

isotropic simply means

$$(a + md)^2 = X^2,$$

which is always true with $X = \pm(a + md)$. So there are infinitely many isotropic blocks in that trivial case.

For $r \geq 2$, part (i) is exactly Theorem 9.4, and part (ii) is exactly Theorem 9.6. □

Step 5: conceptual interpretation

It is useful to summarize the logic in words.

Remark 9.8. Fixing r and looking at consecutive blocks of length r is very different from fixing (a, d) and letting the block length vary. When the block length is fixed, the starting point of the block becomes the variable, and the isotropy problem collapses to a conic. After a simple completion of the square, this conic becomes the Pell-type equation

$$U^2 - rY^2 = \frac{r(r^2 - 1)}{3} d^2.$$

The arithmetic dichotomy is therefore exactly the classical dichotomy for Pell-type equations:

- if r is a square, the conic factors and gives only finitely many integral points;
- if r is not a square, the conic is genuinely Pellian and, once it has one integral point in the correct residue class, it has infinitely many.

In particular, the statement "there are always only finitely many isotropic blocks" is false in general. It is true precisely in the square case.

Step 6: two standard examples

We conclude with the two examples that motivated the discussion.

Example 9.9 (The square case $r = 16$)**.** For $r = 16$ we obtain

$$U^2 - 16Y^2 = 1360d^2.$$

This factors as

$$(U - 4Y)(U + 4Y) = 1360d^2,$$

so for fixed d there are only finitely many possibilities. Therefore every primitive progression (a, d) has only finitely many isotropic blocks of length 16.

Example 9.10 (The nonsquare case $r = 24$)**.** For $r = 24$ we obtain

$$U^2 - 24Y^2 = 4600d^2.$$

This is a genuine Pell-type equation. For $(a, d) = (1, 1)$ one obtains the classical identity

$$1^2 + 2^2 + \cdots + 24^2 = 70^2,$$

so at least one isotropic block exists. Since 24 is not a square, Theorem 9.6 shows that there are in fact infinitely many isotropic blocks of length 24 for this progression.

10. Action on the Blocks of the Arithmetic Progression

In this section we formulate carefully in what sense a group can act on the isotropic blocks coming from one fixed arithmetic progression. The main point is that the automorphism group of the Euclidean Conway quotient does *not* act directly on the isotropic vector itself, because that vector becomes zero in the quotient. Nevertheless, there is a natural and very useful group-theoretic structure in the ambient Lorentzian lattice, and this structure gives a genuine permutation action on the set of isotropic blocks that produce the same Euclidean lattice.

We write everything in a form valid for general fixed rank r. At the end one may specialize to the Leech case $r = 24$. In that case the Euclidean quotient is the Leech lattice Λ whenever it is rootless.

The ambient Lorentzian lattice and the block vectors

Let

$$L \cong II_{r+1,1}$$

be an even unimodular Lorentzian lattice of signature $(r+1, 1)$. We fix integers a, d with

$$\gcd(a, d) = 1,$$

and we fix the block length $r \geq 1$. For each integer $m \geq 0$ we define

$$A_m := a + rmd.$$

The m-th block of the arithmetic progression

$$a,\ a+d,\ a+2d, \ldots$$

of length r is

$$(A_m,\ A_m + d,\ A_m + 2d, \ldots, A_m + (r-1)d).$$

As in Conway's Lorentzian construction, we prepend a zero-coordinate and append a time coordinate. Thus the associated Lorentzian vector is

$$w_m := (0,\ A_m,\ A_m + d,\ A_m + 2d, \ldots, A_m + (r-1)d; X_m) \in L.$$

We call w_m an *isotropic block vector* if

$$\langle w_m, w_m \rangle = 0.$$

Equivalently,

$$\sum_{j=0}^{r-1} (A_m + jd)^2 = X_m^2.$$

Since $\gcd(A_m, d) = \gcd(a, d) = 1$, every such isotropic block vector is primitive.

Whenever w_m is primitive isotropic, the Conway quotient is

$$L_{w_m} := w_m^{\perp} / \mathbb{Z} w_m,$$

which is an even unimodular positive definite lattice of rank r.

Definition 10.1 (Blocks of a fixed arithmetic progression)**.** For fixed (a, d, r) define

$$\mathcal{B}(a, d, r) := \{w_m : m \geq 0,\ \langle w_m, w_m \rangle = 0\}.$$

Thus $\mathcal{B}(a, d, r)$ is the set of isotropic block vectors cut out from one fixed arithmetic progression and one fixed block length.

The Leech-type subfamily

The discussion below applies to any isometry class of Conway quotient. Since your main interest is the Leech lattice, we isolate that case.

Definition 10.2 (The Leech subfamily)**.** Assume now that $r = 24$. Define

$$\mathcal{B}_\Lambda(a, d, 24) := \{w_m \in \mathcal{B}(a, d, 24) : L_{w_m} \cong \Lambda\}.$$

Thus $\mathcal{B}_\Lambda(a, d, 24)$ consists exactly of those isotropic blocks on the fixed arithmetic progression whose Conway quotient is the Leech lattice.

More generally, for arbitrary fixed r, one may replace Λ by any fixed positive definite even unimodular lattice M of rank r and define

$$\mathcal{B}_M(a, d, r) := \{w_m \in \mathcal{B}(a, d, r) : L_{w_m} \cong M\}.$$

Everything below remains valid with M in place of Λ.

Why $\mathrm{Aut}(\Lambda)$ does not act directly on block vectors

Suppose $w \in \mathcal{B}_\Lambda(a, d, 24)$ and

$$L_w = w^\perp/\mathbb{Z}w \cong \Lambda.$$

An automorphism of Λ is an isometry

$$\varphi \in \mathrm{Aut}(\Lambda).$$

However, the isotropic vector w itself does not live in the quotient lattice L_w. Indeed, by definition of the quotient one has

$$w \equiv 0 \pmod{\mathbb{Z}w}.$$

So the class of w in L_w is simply the zero vector. Therefore it makes no sense to apply φ directly to w.

This is the first conceptual point:

> The automorphism group of the Euclidean Conway quotient does not act directly on the isotropic vector that produced the quotient.

The correct place where the symmetry acts is the ambient Lorentzian lattice. The relevant group is the stabilizer of the isotropic line generated by w.

The stabilizer of an isotropic block and its quotient action

Let $w \in \mathcal{B}(a, d, r)$ be primitive isotropic. Define its stabilizer in the orthogonal group of the ambient Lorentzian lattice by

$$\mathrm{Stab}_{O(L)}(w) := \{g \in O(L) : g(w) = w\}.$$

Every element of this stabilizer preserves $w^\perp$ and also preserves the sublattice $\mathbb{Z}w$. Hence it induces an isometry of the quotient lattice

$$w^\perp/\mathbb{Z}w = L_w.$$

Thus there is a natural homomorphism

$$\rho_w : \mathrm{Stab}_{O(L)}(w) \longrightarrow \mathrm{Aut}(L_w).$$

Proposition 10.3 (The natural quotient action)**.** *Let $w \in \mathcal{B}(a,d,r)$ be primitive isotropic. Then every $g \in \mathrm{Stab}_{O(L)}(w)$ induces a well-defined automorphism of $L_w = w^\perp/\mathbb{Z}w$. Consequently there is a natural group homomorphism*

$$\rho_w : \mathrm{Stab}_{O(L)}(w) \to \mathrm{Aut}(L_w).$$

Proof. Take $g \in \mathrm{Stab}_{O(L)}(w)$. Since $g(w) = w$ and g preserves the bilinear form, we have

$$\langle g(x), w\rangle = \langle x, g^{-1}(w)\rangle = \langle x, w\rangle$$

for all $x \in L$. Therefore if $x \in w^\perp$, then $g(x) \in w^\perp$ as well. So g restricts to an isometry of $w^\perp$.

Moreover, because $g(w) = w$, the rank-one sublattice $\mathbb{Z}w$ is preserved. Hence g passes to the quotient and defines a map

$$\bar{g} : w^\perp/\mathbb{Z}w \to w^\perp/\mathbb{Z}w.$$

Since g is an isometry on $w^\perp$, the induced map $\bar{g}$ preserves the quotient form. Thus $\bar{g} \in \mathrm{Aut}(L_w)$.

Finally, if $g, h \in \mathrm{Stab}_{O(L)}(w)$, then the induced map of gh on the quotient is the composition of the induced maps of g and h. Hence

$$\rho_w(gh) = \rho_w(g)\rho_w(h),$$

so ρ_w is a group homomorphism. □

Remark 10.4. In the Leech case $L_w \cong \Lambda$, so ρ_w is a homomorphism

$$\rho_w : \mathrm{Stab}_{O(L)}(w) \to \mathrm{Aut}(\Lambda).$$

Thus the Leech automorphism group appears naturally as a quotient of the stabilizer of the isotropic line generated by w.

A permutation action on the set of block vectors

The next step is to identify a group that really does act on the set of isotropic block vectors. The most natural choice is the subgroup of the ambient orthogonal group that preserves the set of blocks under consideration.

Definition 10.5 (Block-preserving group)**.** For fixed (a,d,r) and a fixed Euclidean lattice type M of rank r, define

$$\Gamma_{\mathrm{block}}(M; a,d,r) := \{g \in O(L) : g(\mathcal{B}_M(a,d,r)) = \mathcal{B}_M(a,d,r)\}.$$

In particular, in the Leech case $r = 24$ we define

$$\Gamma_{\mathrm{block}}(a,d) := \{g \in O(II_{25,1}) : g(\mathcal{B}_\Lambda(a,d,24)) = \mathcal{B}_\Lambda(a,d,24)\}.$$

By construction, $\Gamma_{\mathrm{block}}(M; a,d,r)$ acts on $\mathcal{B}_M(a,d,r)$ by permutation. This is the precise version of the informal sentence "a sensible group acts on the isotropic blocks and permutes them."

Proposition 10.6 (Permutation action on isotropic blocks)**.** *For fixed (a,d,r) and fixed Euclidean quotient type M, the group*

$$\Gamma_{\mathrm{block}}(M; a,d,r)$$

acts on the set $\mathcal{B}_M(a,d,r)$ by permutations.

Proof. By definition, every $g \in \Gamma_{\text{block}}(M; a, d, r)$ maps the set $\mathcal{B}_M(a, d, r)$ to itself. Therefore the assignment

$$(g, w) \longmapsto g(w)$$

defines a map

$$\Gamma_{\text{block}}(M; a, d, r) \times \mathcal{B}_M(a, d, r) \longrightarrow \mathcal{B}_M(a, d, r).$$

This is a group action because the identity element of $O(L)$ fixes every vector and because for $g, h \in \Gamma_{\text{block}}(M; a, d, r)$ one has

$$(gh)(w) = g(h(w))$$

for every block vector w. Hence the action is a genuine permutation action. □

Orbit language

The block-preserving group partitions the set of isotropic blocks into orbits. This gives a clean way to organize all isotropic blocks that produce the same Euclidean Conway quotient.

Definition 10.7 (Orbit equivalence of block vectors)**.** Let $w_1, w_2 \in \mathcal{B}_M(a, d, r)$. We say that w_1 and w_2 are *block-equivalent* if they lie in the same $\Gamma_{\text{block}}(M; a, d, r)$-orbit. Equivalently, there exists

$$g \in \Gamma_{\text{block}}(M; a, d, r)$$

with

$$g(w_1) = w_2.$$

This is stronger than merely asking that $L_{w_1} \cong L_{w_2} \cong M$. Indeed, by definition every block in $\mathcal{B}_M(a, d, r)$ already has quotient lattice isometric to M. The orbit relation asks in addition that there exist an ambient Lorentzian isometry respecting the chosen arithmetic-progression family.

The relation with the full orthogonal group

The full orthogonal group $O(L)$ acts on the set of primitive isotropic vectors of L. If $g \in O(L)$ and w is primitive isotropic, then $g(w)$ is again primitive isotropic. Moreover,

$$L_{g(w)} = g(w)^{\perp}/\mathbb{Z}g(w) \cong w^{\perp}/\mathbb{Z}w = L_w.$$

So the Conway quotient is constant along $O(L)$-orbits of primitive isotropic vectors.

However, the subset $\mathcal{B}_M(a, d, r)$ is much smaller than the full $O(L)$-orbit. Indeed, in $\mathcal{B}_M(a, d, r)$ we insist that the vector have the special block form

$$(0, A, A + d, \ldots, A + (r - 1)d; X)$$

with fixed step size d and with first coordinate constrained by the fixed arithmetic progression. Thus the subgroup $\Gamma_{\text{block}}(M; a, d, r)$ is the appropriate one when the arithmetic shape must be preserved.

Theorem 10.8 (Orbit criterion inside the block family)**.** *Let $w_1, w_2 \in \mathcal{B}_M(a, d, r)$. Then the following are equivalent:*

(i) *w_1 and w_2 lie in the same $\Gamma_{\text{block}}(M; a, d, r)$-orbit.*

(ii) *There exists an isometry $g \in O(L)$ such that*

$$g(w_1) = w_2$$

and such that g maps the whole block family $\mathcal{B}_M(a, d, r)$ to itself.

Proof. This is simply the definition of the block-preserving subgroup. Condition (i) says that there exists some

$$g \in \Gamma_{\text{block}}(M; a, d, r)$$

with $g(w_1) = w_2$. But by definition of $\Gamma_{\text{block}}(M; a, d, r)$ such a g is an element of $O(L)$ that maps $\mathcal{B}_M(a, d, r)$ to itself. Hence (ii) holds.

Conversely, if (ii) holds, then the assumed g belongs to $\Gamma_{\text{block}}(M; a, d, r)$, and therefore w_1 and w_2 lie in the same orbit under this group. Hence (i) holds. □

The role of the stabilizer and the role of the orbit group

There are therefore two different but compatible groups in the picture.

(1) The stabilizer $\text{Stab}_{O(L)}(w)$ of a single block vector w. This group fixes the block vector and acts on the Conway quotient

$$L_w = w^{\perp}/\mathbb{Z}w.$$

In the Leech case this gives access to $\text{Aut}(\Lambda)$.

(2) The block-preserving group $\Gamma_{\text{block}}(M; a, d, r)$. This group acts on the whole set of isotropic block vectors of the chosen arithmetic family and permutes them.

The first group controls the internal symmetry of the Euclidean quotient attached to one block. The second group controls the motion between different blocks of the same arithmetic family.

This explains precisely in what sense one may hope to "permute isotropic blocks by the Leech lattice or by the corresponding Lorentzian lattice." The direct action is not by $\text{Aut}(\Lambda)$ itself on the block vectors, but by a subgroup of the ambient Lorentzian orthogonal group whose stabilizers induce $\text{Aut}(\Lambda)$ on each quotient.

A practical interpretation

Suppose $r = 24$ and you have found a family of isotropic blocks

$$w_{m_1}, w_{m_2}, w_{m_3}, \cdots \in \mathcal{B}_\Lambda(a, d, 24)$$

all coming from the same arithmetic progression. Then the useful questions are:

- What is the subgroup
$$\Gamma_{\text{block}}(a, d) \subset O(II_{25,1})$$
that preserves this family?
- How many orbits does this group have on
$$\mathcal{B}_\Lambda(a, d, 24)?$$
- For a fixed block w, how does the stabilizer $\text{Stab}_{O(L)}(w)$ map onto $\text{Aut}(\Lambda)$?
- Can one describe the orbit structure in terms of explicit arithmetic invariants of the blocks, such as their Pell parameters or congruence data?

These are natural and concrete questions, and they do not suffer from the conceptual problem that an automorphism of the quotient lattice cannot be applied directly to the isotropic vector.

Summary

We summarize the discussion in one sentence.

> The meaningful group action on isotropic blocks is not a direct action of $\mathrm{Aut}(\Lambda)$ on the block vectors themselves, but rather the action of a block-preserving subgroup of the ambient Lorentzian orthogonal group, whose stabilizers induce the Leech automorphism group on the associated Conway quotients.

Thus one obtains a clean orbit decomposition of the isotropic blocks that generate the Leech lattice, while keeping the arithmetic-progression structure visible throughout.

11. Action on the blocks of the arithmetic progression in the Leech-lattice case

In this section we specialize the general discussion to the classical Conway case

$$r = 24, \qquad (a, d) = (1, 1).$$

Then the underlying arithmetic progression is simply

$$1, 2, 3, 4, 5, \ldots,$$

and the m-th block of length 24 is

$$B_m = (24m + 1, 24m + 2, \ldots, 24m + 24).$$

Whenever the corresponding sum of squares is a square,

$$(24m + 1)^2 + (24m + 2)^2 + \cdots + (24m + 24)^2 = X_m^2,$$

we obtain the primitive isotropic Lorentz vector

$$w_m := (0, 24m + 1, 24m + 2, \ldots, 24m + 24; X_m) \in II_{25,1}.$$

By Conway's quotient construction, the lattice

$$L_{w_m} := w_m^{\perp}/\mathbb{Z}w_m$$

is an even unimodular positive definite lattice of rank 24. In the present discussion we focus on those blocks for which this quotient is the Leech lattice.

Definition 11.1. Let

$$\mathcal{B}_\Lambda(1, 1, 24) := \{\, w_m : w_m \text{ is isotropic and } L_{w_m} \cong \Lambda \,\}.$$

We call this the *Leech block set* attached to the natural numbers in blocks of length 24.

The point of the definition is that we do not let $\mathrm{Aut}(\Lambda)$ act directly on the vector w_m itself. The vector w_m lives in the Lorentz lattice $II_{25,1}$, whereas $\mathrm{Aut}(\Lambda)$ acts on the quotient lattice L_{w_m}. The correct mechanism is therefore to use the ambient orthogonal group and its action on primitive isotropic vectors.

1. The Pell parametrization of isotropic 24-blocks

For a general fixed pair (a, d) and fixed length r, we already saw that the block condition is equivalent to an inhomogeneous Pell-type equation. In the present case $r = 24$ and $(a, d) = (1, 1)$, so the starting term of the m-th block is

$$A_m = 24m + 1.$$

The isotropy condition becomes

$$A_m^2 + (A_m + 1)^2 + \cdots + (A_m + 23)^2 = X_m^2.$$

Completing the square in the standard way, set

$$U_m := 2X_m, \qquad Y_m := 2A_m + 23 = 48m + 25.$$

Then the isotropy condition is equivalent to

$$U_m^2 - 24Y_m^2 = 4600.$$

Thus the isotropic blocks are exactly the integer solutions of

$$U^2 - 24Y^2 = 4600$$

with the additional congruence condition

$$Y \equiv 25 \pmod{48}.$$

This description is useful because it separates the problem into

- the Pell-type norm equation, and
- the congruence condition selecting exactly those solutions that come from blocks on the original arithmetic progression.

Remark 11.2. The condition $Y \equiv 25 \pmod{48}$ is not incidental. It is exactly the statement that

$$A = \frac{Y - 23}{2}$$

should satisfy $A \equiv 1 \pmod{24}$, i.e. that the block really starts at a number of the form $24m + 1$.

2. The correct group acting on the block set

Let $L := II_{25,1}$, and let

$$\mathrm{O}(L) = \mathrm{O}(II_{25,1})$$

be its full integral orthogonal group. The group $\mathrm{O}(L)$ acts on primitive isotropic vectors by

$$g \cdot w := g(w).$$

Of course, for a general $g \in \mathrm{O}(L)$ and a general isotropic block $w_m \in \mathcal{B}_\Lambda(1, 1, 24)$, the image $g(w_m)$ need not again be a block on the same arithmetic progression. It will merely be another primitive isotropic vector in L.

This leads to the following natural definition.

Definition 11.3. Define

$$\Gamma_{\mathcal{B}} := \{\, g \in \mathrm{O}(II_{25,1}) : g(\mathcal{B}_\Lambda(1, 1, 24)) = \mathcal{B}_\Lambda(1, 1, 24) \,\}.$$

In words, $\Gamma_{\mathcal{B}}$ is the subgroup of the Lorentz orthogonal group that preserves the Leech block set.

By construction, $\Gamma_{\mathcal{B}}$ acts on $\mathcal{B}_\Lambda(1,1,24)$ by permutation. Thus the block set decomposes into $\Gamma_{\mathcal{B}}$-orbits.

Remark 11.4. This is the precise version of the informal idea that "the Leech lattice should permute the isotropic blocks." The acting group is not $\mathrm{Aut}(\Lambda)$ by itself, but the subgroup of the Lorentz orthogonal group whose action preserves the distinguished family of arithmetic-progression blocks that produce the Leech lattice.

3. The stabilizer of a reference block and the appearance of $\mathrm{Aut}(\Lambda)$

Fix one reference block, say

$$w_0 = (0, 1, 2, \ldots, 24; 70),$$

which is isotropic because

$$1^2 + 2^2 + \cdots + 24^2 = 70^2.$$

Its quotient lattice is the Leech lattice:

$$L_{w_0} = w_0^\perp / \mathbb{Z}w_0 \cong \Lambda.$$

Now consider the stabilizer

$$\mathrm{Stab}_{\mathrm{O}(L)}(w_0) := \{g \in \mathrm{O}(L) : g(w_0) = w_0\}.$$

Every element of this stabilizer preserves $w_0^\perp$ and $\mathbb{Z}w_0$, hence induces an automorphism of the quotient lattice

$$\rho : \mathrm{Stab}_{\mathrm{O}(L)}(w_0) \longrightarrow \mathrm{Aut}(L_{w_0}) \cong \mathrm{Aut}(\Lambda).$$

So the automorphism group of the Leech lattice appears naturally as the quotient action of the Lorentz stabilizer of the reference isotropic vector.

The key point is the following.

Proposition 11.5. *The map*

$$\rho : \mathrm{Stab}_{\mathrm{O}(L)}(w_0) \to \mathrm{Aut}(\Lambda)$$

is a well-defined group homomorphism. In particular, every lift of an automorphism of the Leech lattice fixes the reference vector w_0 and therefore preserves the reference block.

Proof. If $g \in \mathrm{Stab}_{\mathrm{O}(L)}(w_0)$, then $g(w_0) = w_0$. Since g is an isometry, it preserves orthogonality, hence

$$g(w_0^\perp) = w_0^\perp.$$

Because g fixes w_0, it also preserves the line $\mathbb{Z}w_0$. Therefore g descends to a well-defined map on the quotient

$$\overline{g} : w_0^\perp / \mathbb{Z}w_0 \to w_0^\perp / \mathbb{Z}w_0.$$

As g preserves the bilinear form on L, the induced map preserves the positive definite form on the quotient. Hence $\overline{g} \in \mathrm{Aut}(L_{w_0}) \cong \mathrm{Aut}(\Lambda)$. The assignment $g \mapsto \overline{g}$ is clearly compatible with composition, so it is a group homomorphism. □

Remark 11.6. This proposition also shows what *does not* happen: an automorphism of the Leech lattice does not move the reference block to a different block on the arithmetic progression. Any lift of such an automorphism lies in the stabilizer of w_0, so it fixes w_0.

4. How to obtain nontrivial permutations of the isotropic blocks

To move one isotropic block to another, one must leave the stabilizer of a single block and work in the full group $\Gamma_{\mathcal{B}}$. The correct orbit statement is the following.

Theorem 11.7. *Let $w_1, w_2 \in \mathcal{B}_\Lambda(1,1,24)$. Then the following are equivalent:*

1. *There exists an isometry $g \in \mathrm{O}(II_{25,1})$ such that $g(w_1) = w_2$.*
2. *The induced Conway quotients are isometric:*
$$w_1^\perp/\mathbb{Z}w_1 \cong w_2^\perp/\mathbb{Z}w_2.$$
3. *Both w_1 and w_2 lie in the same $\mathrm{O}(II_{25,1})$-orbit of primitive isotropic vectors.*

In particular, if $w_1, w_2 \in \mathcal{B}_\Lambda(1,1,24)$, then any Lorentz isometry carrying w_1 to w_2 automatically carries one Leech quotient to another Leech quotient.

Proof. The implication (1)⇒(2) is immediate: if $g(w_1) = w_2$, then g carries $w_1^\perp$ onto $w_2^\perp$ and induces an isometry of the quotients.

The equivalence of (1) and (3) is simply the definition of belonging to the same orbit under the action of $\mathrm{O}(II_{25,1})$.

Finally, in the present setup the quotient lattices are both isometric to the Leech lattice by definition of the block set. Hence (2) holds automatically once $w_1, w_2 \in \mathcal{B}_\Lambda(1,1,24)$. The point is that the ambient orthogonal group is the correct group controlling the permutation of primitive isotropic vectors that produce isometric Conway quotients. □

5. Arithmetic invariants inherited along block orbits

We now address the central arithmetic question: if a Lorentz isometry sends one Leech block to another,
$$g(w_1) = w_2, \qquad w_1, w_2 \in \mathcal{B}_\Lambda(1,1,24),$$
what arithmetic data of w_1 are preserved in w_2?

The answer has two levels.

Level 1: invariants preserved because we stay inside the same arithmetic-progression block set.

If $w_i = w_{m_i}$ with
$$w_{m_i} = (0, 24m_i + 1, 24m_i + 2, \ldots, 24m_i + 24; X_{m_i}),$$
then both vectors automatically share the following arithmetic features:

1. the block length is the same: $r = 24$;
2. the common difference is the same: $d = 1$;
3. the first entry after the initial zero lies in the same congruence class:
$$A_{m_i} = 24m_i + 1 \equiv 1 \pmod{24};$$
4. the corresponding Pell parameter satisfies
$$Y_{m_i} = 2A_{m_i} + 23 = 48m_i + 25 \equiv 25 \pmod{48};$$
5. the Pell norm is fixed:
$$U_{m_i}^2 - 24Y_{m_i}^2 = 4600, \qquad U_{m_i} = 2X_{m_i};$$

6. primitivity is preserved:
$$\gcd(A_{m_i}, 1) = 1.$$

These are not subtle; they are simply the defining arithmetic constraints for belonging to the same block family.

Level 2: invariants preserved because the ambient Lorentz isometry preserves the quadratic form.

Since $g \in \mathrm{O}(II_{25,1})$, we have
$$\langle g(x), g(y)\rangle = \langle x, y\rangle \qquad \text{for all } x, y \in II_{25,1}.$$

Applied to w_1 and $w_2 = g(w_1)$, this gives:

1. isotropy is preserved:
$$\langle w_2, w_2\rangle = \langle w_1, w_1\rangle = 0;$$
2. primitivity is preserved, because a lattice isometry is invertible over $\mathbb{Z}$;
3. the quotient lattice is preserved up to isometry:
$$L_{w_1} \cong L_{w_2} \cong \Lambda;$$
4. all quotient-lattice invariants are inherited, for example:
   - absence of roots,
   - the theta series,
   - the minimum norm,
   - the kissing number,
   - the full automorphism-group type of the quotient.

In this sense, every block in the same orbit carries the same Conway output.

Remark 11.8. What is *not* obviously preserved by a general Lorentz isometry is the literal coordinate pattern of the block in the standard basis. The conditions
$$(0, 24m+1, 24m+2, \ldots, 24m+24; X)$$
are arithmetic conditions tied to a chosen coordinate model. The group element g preserves the Lorentz form, not the coordinate shape. Thus the preservation of "being a block on the natural numbers" is a condition defining the subgroup $\Gamma_{\mathcal{B}}$, not a formal consequence of orthogonality alone.

6. A useful orbit criterion inside the Leech block set

The previous discussion suggests the following criterion.

Proposition 11.9. *Let $w_1, w_2 \in \mathcal{B}_\Lambda(1,1,24)$. If there exists $g \in \Gamma_{\mathcal{B}}$ with $g(w_1) = w_2$, then the following arithmetic data are inherited from w_1 to w_2:*
$$r = 24, \qquad d = 1, \qquad A \equiv 1 \pmod{24}, \qquad Y \equiv 25 \pmod{48}, \qquad U^2 - 24Y^2 = 4600,$$
and the Conway quotient remains isometric to the Leech lattice.

Proof. Because $g \in \Gamma_{\mathcal{B}}$, the image of a Leech block is again a Leech block on the same arithmetic progression. Therefore the block description of w_2 has exactly the same defining arithmetic shape as that of w_1, namely length 24, common difference 1, and starting point congruent to 1 modulo 24. Equivalently, the corresponding Pell parameter remains congruent to 25 modulo 48 and satisfies the same norm equation. Since g is a Lorentz isometry, it also preserves isotropy and the isometry class of the quotient lattice. Hence the quotient remains the Leech lattice. □

7. Interpretation

The conceptual picture is therefore the following.

1. The isotropic 24-blocks on the natural numbers are parametrized by a Pell-type equation plus a congruence condition.
2. Among them, the subset that gives the Leech lattice forms the set $\mathcal{B}_\Lambda(1,1,24)$.
3. The ambient Lorentz orthogonal group contains a subgroup $\Gamma_{\mathcal{B}}$ that preserves this set.
4. The stabilizer of a single reference block maps to $\mathrm{Aut}(\Lambda)$, so the Leech automorphism group appears naturally inside the Lorentz picture.
5. The nontrivial permutation of different Leech blocks is controlled not by $\mathrm{Aut}(\Lambda)$ alone, but by the larger ambient group $\Gamma_{\mathcal{B}}$.

Thus the correct mechanism is not that the Leech lattice directly acts on the blocks, but rather that the Lorentz symmetries compatible with the block condition permute the Leech-producing blocks, while the Leech automorphism group appears as the quotient action of the stabilizer of any fixed block.

12. The Leech lattice corresponds to the natural numbers

We now explain that, in the arithmetic-progression formulation of the isotropy equation, the Leech lattice is uniquely attached to the natural numbers.

The natural numbers as an arithmetic progression

Among all arithmetic progressions

$$a,\ a+d,\ a+2d,\ \dots,$$

the progression of natural numbers is characterized exactly by

$$(a,d) = (1,1).$$

Indeed, this choice gives

$$1,2,3,4,\dots,$$

and conversely any arithmetic progression equal to the natural numbers must have first term 1 and common difference 1.

For a general arithmetic progression, the isotropy equation is

$$\sum_{j=0}^{r-1}(a+jd)^2 = X^2.$$

Therefore, for

$$(a,d) = (1,1),$$

it becomes

$$1^2 + 2^2 + \cdots + r^2 = X^2.$$

Using Faulhaber's formula, this is equivalent to

$$\frac{r(r+1)(2r+1)}{6} = X^2.$$

Uniqueness of the positive integral solution

The Diophantine equation

$$1^2 + 2^2 + \cdots + r^2 = X^2$$

is the classical *cannonball problem*. Its unique positive integral solution is

$$(r, X) = (24, 70).$$

Equivalently,

$$\frac{24 \cdot 25 \cdot 49}{6} = 70^2.$$

From the elliptic-curve viewpoint developed earlier in this paper, the specialization $(a, d) = (1, 1)$ of the general cubic equation is

$$6X^2 = 2r^3 + 3r^2 + r = r(r + 1)(2r + 1).$$

Thus the natural-number progression determines the affine cubic

$$6X^2 = r(r + 1)(2r + 1),$$

or equivalently

$$X^2 = \frac{r(r + 1)(2r + 1)}{6}.$$

This is an elliptic curve over $\mathbf{Q}$. By the theorem of Mordell–Weil, its rational points form a finitely generated abelian group, and by Siegel's theorem it has only finitely many integral points. In the present case, the integral-point computation yields exactly one positive solution, namely

$$(r, X) = (24, 70).$$

Hence, if one starts from the arithmetic progression of natural numbers, that is from

$$(a, d) = (1, 1),$$

and searches for integers r and X such that the isotropy equation holds, one arrives uniquely at

$$(r, X) = (24, 70).$$

Conway's construction and the Leech lattice

For this unique solution, the corresponding isotropic vector is

$$w = (1, 2, \ldots, 24; 70).$$

Since

$$\gcd(1, 1) = 1,$$

the vector w is primitive. Therefore Conway's Lorentzian construction applies, and one obtains the positive definite even unimodular lattice

$$w^{\perp}/\mathbf{Z}w.$$

But the identity

$$1^2 + 2^2 + \cdots + 24^2 = 70^2$$

is precisely the classical identity underlying Conway's Lorentzian construction of the Leech lattice. Therefore the quotient

$$(1, 2, \ldots, 24; 70)^{\perp}/\mathbf{Z}(1, 2, \ldots, 24; 70)$$

is the Leech lattice.

Conclusion

We may summarize the discussion as follows.

Proposition 12.1. *The natural numbers correspond exactly to the arithmetic progression*

$$(a, d) = (1, 1).$$

For this progression, the isotropy equation is

$$1^2 + 2^2 + \cdots + r^2 = X^2.$$

Its unique positive integral solution is

$$(r, X) = (24, 70).$$

The associated primitive isotropic vector is

$$(1, 2, \ldots, 24; 70),$$

and Conway's Lorentzian quotient attached to this vector is the Leech lattice. Thus, in the arithmetic-progression formulation, the Leech lattice is uniquely attached to the natural numbers.

In this precise sense, the Leech lattice corresponds to the natural numbers: the natural-number progression is exactly the progression $(a, d) = (1, 1)$, its isotropy equation has exactly one positive integral solution, and that unique solution is the classical Conway vector producing the Leech lattice.

13. Outlook

This note suggests several directions for further study.

(1) **Explicit families.** For fixed rank r, classify or parametrize solutions of

$$\sum_{j=0}^{r-1} (a + jd)^2 = X^2$$

with $\gcd(a, d) = 1$.

(2) **Lorentzian constructions in new ranks.** Every primitive isotropic solution gives a candidate vector for a Conway-style Lorentzian quotient construction. It would be interesting to see whether this viewpoint yields systematic families of explicit lattices.

(3) **Interaction with modular forms.** If the resulting positive definite lattices have interesting theta series, then one may compare the Lorentzian construction with other explicit constructions, for example the generalized Paley–Krieg construction.

(4) **Analytic number theory.** Although Dirichlet's theorem does not directly solve the Lorentzian problem, the shared coprimality condition suggests that arithmetic progressions are the correct language for placing the construction in a wider number-theoretic framework.

14. Conclusion

The main observations of this note are simple but, we believe, conceptually neat.

- Arithmetic progressions provide a natural class of candidate coordinate systems for primitive isotropic vectors in Conway's Lorentzian construction.
- The primitivity condition is exactly $\gcd(a, d) = 1$.
- The isotropy condition is an explicit quadratic Diophantine equation obtained by Faulhaber's formula.
- For fixed (a, d), this equation becomes a cubic in (r, X) and hence, generically, an elliptic curve.
- The same coprimality condition also governs Dirichlet's theorem on primes in arithmetic progressions, suggesting a conceptual bridge to analytic number theory.

Taken together, these facts suggest that Conway's Lorentzian construction may be viewed not only as a lattice-theoretic quotient construction, but also as a meeting point of arithmetic progressions, Diophantine equations, and elliptic curves.

References

[1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer.

[2] M. Koecher and A. Krieg, *Elliptische Funktionen und Modulformen*, Springer, 1998.

[3] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer.

[4] O. Leka, *A Lorentzian Construction in Dimension 88 and Infinitely Many Further Ranks*, https://www.orges-leka.de/88_lorentz_paper.pdf.

[5] O. Leka, *A Generalized Krieg–Paley Construction of Even Unimodular Lattices From Dimension 24 to an Infinite Family*, https://www.orges-leka.de/krieg_generalization.pdf.