ANNALS OF MATHEMATICS

Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups

By Leonid Vaserstein

SECOND SERIES, VOL. 171, NO. 2

March, 2010

ANMAAH

Annals of Mathematics, **171** (2010), 979–1009

Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups

By LEONID VASERSTEIN

Abstract

A polynomial parametrization for the group of integer two-by-two matrices with determinant one is given, solving an old open problem of Skolem and Beurkers. It follows that, for many Diophantine equations, the integer solutions and the primitive solutions admit polynomial parametrizations.

Introduction

This paper was motivated by an open problem from [8, p. 390]:

> CNTA 5.15 (Frits Beukers). Prove or disprove the following statement: There exist four polynomials A, B, C, D with integer coefficients (in any number of variables) such that $AD - BC = 1$ and all integer solutions of $ad - bc = 1$ can be obtained from A, B, C, D by specialization of the variables to integer values.

Actually, the problem goes back to Skolem [14, p. 23]. Zannier [22] showed that three variables are not sufficient to parametrize the group $\mathrm{SL}_2\,\mathbb{Z}$, the set of all integer solutions to the equation $x_1x_2 - x_3x_4 = 1$.

Apparently Beukers posed the question because $\mathrm{SL}_2\,\mathbb{Z}$ (more precisely, a congruence subgroup of $\mathrm{SL}_2\,\mathbb{Z}$) is related with the solution set X of the equation $x_1^2 + x_2^2 = x_3^2 + 3$, and he (like Skolem) expected the negative answer to CNTA 5.15, as indicated by his remark [8, p. 389] on the set X:

> I have begun to believe that it is not possible to cover all solutions by a finite number of polynomials simply because I have never

The paper was conceived in July of 2004 while the author enjoyed the hospitality of Tata Institute for Fundamental Research, India.

> seen a polynomial parametrisation of all two-by-two determinant one matrices with integer entries.

In this paper (Theorem 1 below) we obtain the affirmative answer to CNTA 5.15. As a consequence we prove, for many polynomial equations, that either the set X of integer solutions is a polynomial family or (more generally) X is a finite union of polynomial families. It is also possible to cover all solutions of $x_1^2 + x_2^2 = x_3^2 + 3$ by two polynomial triples; see Example 15 below.

Skolem [14, Bemerkung 1, p. 23] conjectured that $\mathrm{SL}_n\,\mathbb{Z}$ does not admit a polynomial parametrization for any n. However the main result of Carter and Keller [4] refutes this for $n \geq 3$, and our Theorem 1 refutes this for $n = 2$ and also implies a similar result for $n \geq 3$; see Corollary 17(a).

A few words about our terminology. Let

$$(P_1(y_1, \ldots, y_N), \ldots, P_k(y_1, \ldots, y_N))$$

be a k-tuple of polynomials in N variables with integer coefficients. Plugging in all N-tuples of integers, we obtain a family X of integer k-tuples, which we call a *polynomial family* (defined over the integers $\mathbb{Z}$) with N parameters. We also say that the set X admits a *polynomial parametrization* with N parameters. In other words, a polynomial family X is the image (range) $P(\mathbb{Z}^N)$ of a polynomial map $P : \mathbb{Z}^N \to \mathbb{Z}^k$. We call this map P a *polynomial parametrization* of X.

Given a Diophantine equation or a system of Diophantine equations, we can ask whether the solution set (over $\mathbb{Z}$) is a polynomial family. In other words, we can search for a general solution (i.e., a polynomial parametrization for the set). In the case of a polynomial equation, the polynomials in any polynomial parametrization form a polynomial solution.

If no polynomial parametrization is known or exists, we can ask whether the solution set is a finite union of polynomial families. Loosely speaking, are the solutions covered by a finite number of polynomials?

Also we can ask about polynomial parametrization of all primitive solutions. Recall that a k-tuple of integers is called *primitive* (or unimodular) if its GCD is 1. For any homogeneous equation, a polynomial parametrization of all primitive solutions leads to a polynomial parametrization of all solutions with one additional parameter.

The open problem CNTA 5.15 quoted above is the question whether the group $\mathrm{SL}_2\,\mathbb{Z}$ is a polynomial family, i.e., admits a polynomial parametrization. Our answer is "yes":

THEOREM 1. $\mathrm{SL}_2\,\mathbb{Z}$ *is a polynomial family with* 46 *parameters.*

We will prove this theorem in Section 1. The proof refines computations in [10], [2], [13], [18] and [4], especially, the last two papers.

Now we consider some applications of the theorem and some examples. First we deal with an arbitrary system of linear equations. Then we consider quadratic equations. Finally, we consider Diophantine equations of higher degree. On the way, we make a few general remarks on the polynomial families.

It is easy to see that the solution set for any system of linear equations (with integer coefficients) either is empty or admits a polynomial parametrization of degree ≤ 1 with the number of parameters N less than or equal to the number of variables k. In Section 2, using our Theorem 1, we obtain this:

COROLLARY 2. *The set of all primitive solutions for any linear system of equations with integer coefficients either consists of* ≤ 2 *solutions or is a polynomial family.*

For example, the set $\mathrm{Um}_n\,\mathbb{Z}$ of all primitive (unimodular) n-tuples of integers turns out to be a polynomial family provided that $n \ge 2$. The case $n \ge 3$ is much easier, and this result can be easily extended to more general rings; see Section 2 below. When $n = 1$, the set $\mathrm{Um}_1\,\mathbb{Z} = \{\pm 1\}$ consists of two elements. This set is not a polynomial family but can be covered by two (constant) polynomials.

In general, a finite set with cardinality $\neq 1$ is not a polynomial family but can be covered by a finite number of (constant) polynomials (the number is zero in the case of an empty set).

The set $\mathrm{Um}_n\,\mathbb{Z}$ is a projection of the set X of all integer solutions to the quadratic equation $x_1x_2 + \cdots + x_{2n-1}x_{2n} = 1$. So if X is a polynomial family, then obviously $\mathrm{Um}_n\,\mathbb{Z}$ is a polynomial family. Using Theorem 1, we will show X is a polynomial family if $n \ge 2$. (When $n = 1$ the solution set $\mathrm{Um}_1\,\mathbb{Z} = \mathrm{GL}_1\,\mathbb{Z} = \{\pm 1\}$ to the equation $x_1x_2 = 1$ is not a polynomial family.)

COROLLARY 3. *When* $n \ge 2$, *the set of all integer solutions of*

$$x_1x_2 + \cdots + x_{2n-1}x_{2n} = 1$$

is a polynomial family.

In fact, Theorem 1 implies that for many other quadratic equations, the set of all integer or all primitive solutions is a polynomial family or a finite union of polynomial families. A useful concept here is that of a Q-unimodular vector x, where $Q(x)$ is a quadratic form, i.e., a homogeneous, degree two polynomial with integer coefficient. An integer vector x is called Q-unimodular if there is a vector x' such that $Q(x + x') - Q(x) - Q(x') = 1$. Our Corollary 3 is a particular case of the following result, which we will prove in Section 3:

COROLLARY 4. *Consider the set* X *of all* Q*-unimodular solutions to* $Q(x) = Q_0$, *where* $Q(x)$ *is a quadratic form in* k *variables and* Q_0 *is a given number. Assume that* $k \ge 4$ *and that* $Q(x) = x_1x_2 + x_3x_4 + Q'(x_5, \ldots, x_k)$. *Then* X *is a polynomial family with* $3k + 80$ *parameters.*

Under the additional condition that $k \geq 6$ and $Q'(x_5, \dots, x_k) = x_5x_6 + Q''(x_7, \dots, x_k)$, it is easy to get a better bound (with $3k-6$ instead of $3k+80$) without using Theorem 1 (see Proposition 3.4 below).

Note that for nonsingular quadratic forms Q (when the corresponding symmetric bilinear form $(x, x')_Q = Q(x+x')-Q(x)-Q(x')$ has an invertible matrix), "Q-unimodular" means "primitive." In general, the orthogonal group acts on the integer solutions Z and on the Q-unimodular solutions X, a fact we use to prove Corollary 4.

Now we make several remarks about the integer solutions x to $Q(x) = Q_0$ that are not Q-unimodular. We observe that both GCD(x) and the GCD of all $(x, x')_Q$ are invariants under the action. In the case when Q is nonsingular, Corollary 4 describes the set Z of all integer solutions z as follows: if $Q_0 = 0$ (homogeneous case), then $z = xy_0$ with primitive x, so Z is a polynomial family with an additional parameter; if $Q_0 \neq 0$, then Z is a finite union of polynomial families indexed by the square divisors of Q_0. We will show elsewhere that the set Z for Q in Corollary 4 or, more generally, for any isotropic quadratic form Q, is a finite union of polynomial families.

Example 5. The solution set for the Diophantine equation $x_1x_2 = x_3^2$ admits a polynomial parametrization with three parameters:

$$(x_1, x_2, x_3) = y_1(y_2^2, y_3^2, y_2y_3).$$

Among these solutions, the primitive solutions are those with $y_1 = \pm 1$ and $(y_2, y_3) \in \mathrm{Um}_2\,\mathbb{Z}$. So by Theorem 1 (or Corollary 3 with $n = 2$), the set of all primitive solutions is the union of two polynomial families. The set of primitive solutions is not a polynomial family.

This follows easily from the fact that the polynomial ring $\mathbb{Z}[y_1, \dots, y_N]$ is a unique factorization domain from any N, so within any polynomial family either all $x_1 \geq 0$ or all $x_1 \leq 0$.

The number 2 here is related to the fact that the group $\mathrm{SL}_2\,\mathbb{Z}$ acts on the two-by-two symmetric matrices with two orbits on the determinant 0 primitive matrices. The action is

$$\begin{pmatrix} x_1 & x_3 \\ x_3 & x_4 \end{pmatrix} \mapsto \alpha^T \begin{pmatrix} x_1 & x_3 \\ x_3 & x_4 \end{pmatrix} \alpha \quad \text{for } \alpha \in \mathrm{SL}_2\,\mathbb{Z},$$

where α^T is the transpose of α.

An alternative description of the action of $\mathrm{SL}_2\,\mathbb{Z}$ is

$$\begin{pmatrix} x_3 & -x_1 \\ x_2 & -x_3 \end{pmatrix} \mapsto \alpha^{-1} \begin{pmatrix} x_3 & -x_1 \\ x_2 & -x_3 \end{pmatrix} \alpha \quad \text{for } \alpha \in \mathrm{SL}_2\,\mathbb{Z}.$$

The trace 0 and the determinant $x_1x_2 - x_3^2$ are preserved under this action.

Example 6. The solution set for $x_1x_2 + x_3x_4 = 0$ admits the following polynomial parametrization with five parameters:

$$(x_1, x_2, x_3, x_4) = y_5(y_1y_2, y_3y_4, y_1y_3, y_2y_4).$$

Such a solution is primitive if and only if $y_5 = \pm 1$ and $(y_1, y_4), (y_2, y_3) \in \mathrm{Um}_2\,\mathbb{Z}$. So by Theorem 1, the set of all primitive solutions is a polynomial family with 92 parameters. By Theorem 2.2 below, the number of parameters can be reduced to 90.

Example 7. Consider the equation $x_1x_2 = x_3^2 + D$ with a given $D \in \mathbb{Z}$. The case $D = 0$ was considered in Example 5, so assume now that $D \neq 0$. We can identify solutions with integer symmetric two-by-two matrices of determinant D. The group $\mathrm{SL}_2\,\mathbb{Z}$ acts on the set X of all solutions as in Example 5. It is easy to see and well known that every orbit contains either a matrix $\left(\begin{smallmatrix} a & b \\ b & d \end{smallmatrix}\right)$ with $a \neq 0$ and $(1-|a|)/2 \le b \le |a|/2 \le |d|/2$ or a matrix $\left(\begin{smallmatrix} 0 & b \\ b & 0 \end{smallmatrix}\right)$ with $b^2 = -D$. In the first case, $|D| = |ad - b^2| \ge a^2 - a^2/4 = 3a^2/4 \ge 3b^2/16$, and d is determined by a and b; hence the number of orbits is at most $8|D|/3$. Therefore the total number of orbit is bounded by $8|D|/3 + 2$. (Better bounds and connections with the class number of the field $\mathbb{Q}[\sqrt{D}]$ are known.)

By Theorem 1, every orbit is a polynomial family with 46 parameters, so the set X can be covered by a finite set of polynomials, and the subset of primitive solutions can be covered by a finite set of polynomials with 46 parameters each. When $D = \pm 1$ or ± 2, the number of orbits and hence the number of polynomial families is two. When $D = \pm 3$, the number of orbits is four.

When D is square-free, every integer solution is primitive.

Example 8. Consider the equation $x_1x_2 + x_3x_4 = D$ with a given integer D (i.e., the equation in Corollary 4 with $k = 4$ and $Q_0 = D$). The case $D = 0$ was considered in Example 6, so assume now that $D \neq 0$. The group $\mathrm{SL}_2\,\mathbb{Z} \times \mathrm{SL}_2\,\mathbb{Z}$ acts on the solutions $\left(\begin{smallmatrix} x_1 & x_3 \\ -x_4 & x_2 \end{smallmatrix}\right)$ by

$$\begin{pmatrix} x_1 & x_3 \\ -x_4 & x_2 \end{pmatrix} \mapsto \alpha^{-1} \begin{pmatrix} x_1 & x_3 \\ -x_4 & x_2 \end{pmatrix} \beta, \quad \text{where } \alpha, \beta \in \mathrm{SL}_2\,\mathbb{Z}.$$

It is well known that every orbit contains the matrix $\mathrm{diag}(d, D/d)$, where $d = \mathrm{GCD}(x_1, x_2, x_3, x_4)$. So the number of orbits is the number of squares d^2 dividing D. By Theorem 1, the set X of integers solutions is a finite union of polynomial families, and the subset X' of primitive solutions is a polynomial family with 92 parameters. When D is square-free, $X' = X$. When $D = \pm 1$, Theorem 1 gives a better number of parameters, namely 46 instead of 92.

Example 9. Let $D \ge 2$ be a square-free integer. It is convenient to write solutions $(x_1, x_2) = (a, b)$ of Pell's equation $x_1^2 - Dx_2^2 = 1$ as $a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$.

Then they form a group under multiplication. All solutions are primitive, and they are parametrized by two integers, m and n, as

$$a + b\sqrt{D} = (a_0 + b_0\sqrt{D})^m (a_1 + b_1\sqrt{D})^n,$$

where $a_0 + b_0\sqrt{D}$ is a solution of infinite order and $a_1 + b_1\sqrt{D}$ is a solution of finite order (this is not a polynomial parametrization!).

We claim that every polynomial solution to the equation is constant. Since D is not a square, this is obvious. Here is a more sophisticated argument which works for many "sparse" sequences:

It is clear that $\sum |a|^{-\varepsilon} < \infty$ for any $\varepsilon > 0$, where the sum is taken over all solutions $a + b\sqrt{D}$. On the other hand, if we have a nonconstant polynomial solution, we have a nonconstant univariate solution $f(y) + g(y)\sqrt{D}$. If $g(x)$ is not constant, then $f(y)$ is not constant. Let $d \geq 1$ be the degree of $f(x)$. Then $\sum_{z\in\mathbb{Z}} |f(z)|^{-\varepsilon} = \infty$ provided that $0 < \varepsilon \leq 1/d$. Since $f(z)$ takes every value at most d times, we obtain a contradiction that proves $d = 0$.

Since the set X of all integer solutions is infinite, it cannot be covered by a finite number of polynomials.

Remarks. (1) Let $a_1, a_2, \ldots$ be a sequence of integers satisfying a linear recurrence equation $a_n = c_1 a_{n-1} + \cdots + c_k a_{n-k}$ with some $k \geq 1$ and $c_i \in \mathbb{Z}$ for all $n \geq k+1$. Then the argument in Example 9 shows that the set X of all integers a_i either is finite or is not a finite union of polynomial families. Note that X is finite if and only if any of the following conditions holds:

- the sequence is bounded,
- the sequence is periodic,
- the sequence satisfies a linear recurrence equation with all zeros of the characteristic polynomial being roots of 1,
- the sequence satisfies a linear recurrence equation with all zeros of the characteristic polynomial on the unit circle.

(2) The partition function $p(n)$ provides another set of integers that is not a finite union of polynomial families (use the well-known asymptotic for $p(n)$ and the argument in Example 9).

(3) By author's request, S. Frisch [6] proved that every subset of $\mathbb{Z}^k$ with a finite complement is a polynomial family.

(4) The set of all positive composite numbers is parametrized by the polynomial

$$(y_1^2 + y_2^2 + y_3^2 + y_4^2 + 2)(y_5^2 + y_6^2 + y_7^2 + y_8^2 + 2).$$

(5) It is known [9] that the union of the set of (positive) primes and a set of negative integers is a polynomial family. In the terms of [9], the set of primes is

both Diophantine and listable. On the other hand, it is an easy fact that the set of primes is not a polynomial family; see Corollary 5.15 below and the remark after its proof.

Corollaries 2–4 and Examples 5–9 above are about quadratic equations. The next three examples are about higher degree polynomial equations.

Example 10. The Fermat equation $y_1^n + y_2^n = y_3^n$ with any given $n \geq 3$ has three "trivial" polynomial families of solutions with one parameter each when n is odd, and it has four polynomial families of solutions when n is even. Fermat's Last Theorem says that these polynomial families cover all integer solutions.

Example 11. It is unknown whether the solution set of

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 = 0$$

can be covered by a finite set of polynomials. A negative answer was conjectured in [7].

Example 12. It is unknown whether the solution set of

$$x_1^3 + x_2^3 + x_3^3 = 1$$

can be covered by a finite number of polynomials. It is known (see [11, Th. 2]) that the set cannot by covered by a finite number of univariant polynomials.

To deal with equations $x_1^2 + x_2^2 = x_3^2$ and $x_1^2 + x_2^2 = x_3^2 + 3$ (which are equivalent over the rational numbers $\mathbb{Q}$ to the equations in Examples 5 and 7 with $D = 3$, respectively) we need a polynomial parametrization of a congruence subgroup of $\mathrm{SL}_2\,\mathbb{Z}$.

Recall that for any nonzero integer q, the *principal congruence subgroup* $\mathrm{SL}_2(q\mathbb{Z})$ consists of $\alpha \in \mathrm{SL}_2\,\mathbb{Z}$ such that $\alpha \equiv 1_2 = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ modulo q. A *congruence subgroup* of $\mathrm{SL}_2\,\mathbb{Z}$ is a subgroup containing a principal congruence subgroup.

THEOREM 13. *Every principal congruence subgroup of* $\mathrm{SL}_2\,\mathbb{Z}$ *admits a polynomial parametrization with* 94 *parameters.*

We will prove this theorem in Section 5 below. Theorem 13 implies that every congruence subgroup is a finite union of polynomial families. There are congruence subgroups that are not polynomial families; see Proposition 5.13 and Corollary 5.14 below.

Example 14. Consider the equation $x_1^2 + x_2^2 = x_3^2$. Its integer solutions are known as *Pythagorean triples*; sometimes the name is reserved for solutions that are primitive and/or positive. Let X be the set of all integer solutions

The equation can be written as $x_1^2 = (x_2 + x_3)(x_3 - x_2)$ so every element of X gives a solution to the equation in Example 5.

The set X is not a polynomial family but can be covered by two polynomial families:

$$(x_1, x_2, x_3) = y_3(2y_1y_2, y_1^2 - y_2^2, y_1^2 + y_2^2) \text{ or } y_3(y_1^2 - y_2^2, 2y_1y_2, y_1^2 + y_2^2).$$

The subset X' of all primitive solutions is the disjoint union of four families described by the same polynomials but with $y_3 = \pm 1$ and $(y_1, y_2) \in \mathrm{Um}_2\,\mathbb{Z}$ with odd $y_1 + y_2$.

To get a polynomial parametrization of these pairs (y_1, y_2) and hence to cover X' by four polynomials, we use Theorem 13. Let H be the subgroup of $\mathrm{SL}_2\,\mathbb{Z}$ generated by $\mathrm{SL}_2(2\mathbb{Z})$ and the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The first rows of matrices in H are exactly the $(a, b) \in \mathrm{Um}_2\,\mathbb{Z}$ such that $a + b$ is odd. It follows from Theorem 13 (see Example 5.12 below) that H is a polynomial family with 95 parameters. Thus, the set X' of primitive solutions is the union of four polynomial families with 95 parameters each.

Example 15. Now we consider the equation $x_1^2 + x_2^2 = x_3^2 + 3$. Finding its integer solutions was a famous open problem stated as a limerick a long time ago; it is [8, CNTA 5.14]. Using the obvious connection with the equation in our Example 7, Beukers [8] splits the set of solutions X into two families, each of them parametrized by the group H above (Example 14).

So Theorem 13 implies that X is the union of two polynomial families, contrary to the belief of Beukers [8].

Example 16. A few results of the last millennium, [5] and [3], together with our results, show that for arbitrary integers a, b, c and any integers $\alpha, \beta, \gamma \geq 1$, the set of primitive solutions to the equation $ax_1^\alpha + bx_2^\beta = cx_3^\gamma$ can be covered by a finite (possibly, empty) set of polynomial families. Details will appear elsewhere. The minimal cardinality of the set is not always known; in the case of $\alpha = \beta = \gamma \geq 3$, the cardinality is 8 for even α and 6 for odd α (Fermat's Last Theorem).

In a future paper, using a generalization of Theorem 1 to rings of algebraic numbers, we will prove that many arithmetic groups are polynomial families. In Section 5 of this paper, we will consider only Chevalley-Demazure groups of classical type, namely $\mathrm{SL}_n\,\mathbb{Z}$, the symplectic groups $\mathrm{Sp}_{2n}\,\mathbb{Z}$, the orthogonal groups $\mathrm{SO}_n\,\mathbb{Z}$, and the corresponding spinor groups $\mathrm{Spin}_n\,\mathbb{Z}$.

Recall that

- $\mathrm{Sp}_{2n}\,\mathbb{Z}$ is a subgroup of $\mathrm{SL}_{2n}\,\mathbb{Z}$ preserving the bilinear form

$$x_1y_2 - y_1x_2 + \cdots + x_{2n-1}y_{2n} - y_{2n-1}x_{2n},$$

- $\mathrm{SO}_{2n}\,\mathbb{Z}$ is a subgroup of $\mathrm{SL}_{2n}\,\mathbb{Z}$ preserving the quadratic form

$$x_1x_2 + \cdots + x_{2n-1}x_{2n},$$

- $\mathrm{SO}_{2n+1}\,\mathbb{Z}$ is a subgroup of $\mathrm{SL}_{2n+1}\,\mathbb{Z}$ preserving the quadratic form

$$x_1x_2 + \cdots + x_{2n-1}x_{2n} + x_{2n+1}^2,$$

- there is a homomorphism (isogeny) $\mathrm{Spin}_n\,\mathbb{Z} \to \mathrm{SO}_n\,\mathbb{Z}$ whose kernel and cokernel are both of order 2 (see [17]),
- $\mathrm{Spin}_3\,\mathbb{Z} = \mathrm{SL}_2\,\mathbb{Z} = \mathrm{Sp}_2\,\mathbb{Z}$ (see Example 5),
- $\mathrm{Spin}_4\,\mathbb{Z} = \mathrm{SL}_2\,\mathbb{Z} \times \mathrm{SL}_2\,\mathbb{Z}$ (see Example 8),
- $\mathrm{Spin}_5\,\mathbb{Z} = \mathrm{Sp}_4\,\mathbb{Z}$ and $\mathrm{Spin}_6\,\mathbb{Z} = \mathrm{SL}_4\,\mathbb{Z}$ (see [21]).

From Theorem 1, we easily obtain (see Section 4)

COROLLARY 17. *For any $n \geq 2$,*

(a) *the group $\mathrm{SL}_n\,\mathbb{Z}$ is a polynomial family with $39 + n(3n+1)/2$ parameters,*

(b) *the group $\mathrm{Spin}_{2n+1}\,\mathbb{Z}$ is a polynomial family with $4n^2 + 41$ parameters,*

(c) *the group $\mathrm{Sp}_{2n}\,\mathbb{Z}$ is a polynomial family with $3n^2 + 2n + 41$ parameters,*

(d) *the group $\mathrm{Spin}_{2n+2}\,\mathbb{Z}$ is a polynomial family with $4(n+1)^2 - (n+1) + 36$ parameters.*

So $\mathrm{SO}_{n+1}\,\mathbb{Z}$ is the union of two polynomial families.

The polynomial parametrization of $\mathrm{SL}_n\,\mathbb{Z}$ implies obviously that the group $\mathrm{GL}_n\,\mathbb{Z}$ is a union of two polynomial families for all $n \geq 1$. (It is also obvious that $\mathrm{GL}_n\,\mathbb{Z}$ is not a polynomial family.) Less obvious is the following consequence of Corollary 17(a):

COROLLARY 18. *For any integer $n \geq 1$, the set M_n of all integer $n \times n$ matrices with nonzero determinant is a polynomial family in $\mathbb{Z}^{n^2}$ that has $2n^2 + 6n + 39$ parameters.*

Proof. When $n = 1$, M_1 is the set of nonzero integers. It is parametrized by the polynomial

$$f(y_1, y_2, y_3, y_4, y_5) = (y_1^2 + y_2^2 + y_3^2 + y_4^2 + 1)(2y_5 + 1)$$

with five parameters. (We used Lagrange's theorem asserting that the polynomial $y_1^2 + y_2^2 + y_3^2 + y_4^2$ parametrizes all integers ≥ 0, but we did not use Corollary 17.)

Assume now that $n \geq 2$. Every matrix $\alpha \in M_n$ has the form $\alpha = \beta\mu$, where $\beta \in \mathrm{SL}_n\,\mathbb{Z}$ and μ is an upper triangular matrix with nonzero diagonal entries. Using $39 + 3n(n+1)/2$ parameters for α (see Corollary 17(a)), five parameters for each diagonal entry in μ (see the case $n = 1$ above), and one parameter for each off-diagonal entry in μ, we obtain a polynomial parametrization for M_n whose number of parameters is

$$39 + 3n(n+1)/2 + 5n + n(n-1)/2 = 2n^2 + 6n + 39. \qquad \square$$

Remark 1. Similarly, every system of polynomial inequalities (with the inequality signs $\neq$, $\geq$, $\leq$, $>$, $<$ instead of the equality sign in polynomial equations) can be converted to a system of polynomial equations by introducing additional variables. For example, the set M_n in Corollary 18 is a projection of the set of all integer solutions to the (n^2+5)-variable polynomial equation

$$\det(x_{i,j}) = (x_{n^2+1}^2 + x_{n^2+2}^2 + x_{n^2+3}^2 + x_{n^2+4}^2 + 1)(2x_{n^2+5} + 1).$$

The polynomial parametrization of $\mathrm{SL}_n\,\mathbb{Z}$ with $n \geq 3$ is related to a bounded generation of this group. In [4], it is proved that every matrix in $\mathrm{SL}_n\,\mathbb{Z}$ with $n \geq 3$ is a product of $36 + n(3n-1)/2$ elementary matrices (for $n = 2$, the number of elementary matrices is unbounded). Since there are $n^2 - n$ types of elementary matrices $z^{i,j}$ with $i \neq j$, this gives a polynomial parametrization of $\mathrm{SL}_n\,\mathbb{Z}$ for $n \geq 3$, with

$$(n^2 - n)(36 + n(3n-1)/2)$$

parameters. Conversely, any polynomial matrix

$$\alpha(y_1, \ldots, y_N) \in \mathrm{SL}_n(\mathbb{Z}[y_1, \ldots, x_N])$$

is a product of elementary polynomial matrices [15] if $n \geq 3$. When $\alpha(\mathbb{Z}^N) = \mathrm{SL}_n\,\mathbb{Z}$, this gives a representation of every matrix in $\mathrm{SL}_n\,\mathbb{Z}$ as a product of a bounded number of elementary matrices.

We conclude the introduction with remarks on possible generalization of Theorem 1 to commutative rings A with 1. If A is semi-local (which includes all fields and local rings) or, more generally, A satisfies the first Bass stable range condition $\mathrm{sr}(A) = 1$ (which includes, e.g., the ring of all algebraic integers; see [19]), then every matrix in $\mathrm{SL}_2\,A$ has the form

$$\begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & u_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u_4 & 1 \end{pmatrix},$$

which gives a polynomial matrix

$$P(y_1, y_2, y_3, y_4) \in \mathrm{SL}_2(\mathbb{Z}[y_1, y_2, y_3, y_4])$$

such that $P(A^4) = \mathrm{SL}_2\,A$. For any commutative A with 1, any N, and any polynomial matrix

$$P(y_1, \ldots, y_N) \in \mathrm{SL}_2(\mathbb{Z}[y_1, \ldots, y_N]),$$

all matrices $\alpha \in P(A^n)$ have the same Whitehead determinant $\mathrm{wh}(\alpha) \in \mathrm{SK}_1\,A$; see [1]. There are rings A, e.g., $A = \mathbb{Z}[\sqrt{-D}]$ for some D [2], such that $\mathrm{wh}(\mathrm{SL}_2\,A) = \mathrm{SK}_1\,A \neq 0$. For such rings A, there in no N and P such that $P(A^N) = \mathrm{SL}_2\,A$.

Allowing coefficients in A does not help much. For any matrix

$$P(y_1, \ldots, y_N) \in \mathrm{SL}_2(A[y_1, \ldots, y_N]),$$

all matrices in $P(A^N)$ have the same image in $\mathrm{SK}_1 A/\mathrm{Nill}_1 A$, where $\mathrm{Nill}_1 A$ is the subgroup of $\mathrm{SK}_1 A$ consisting of $\mathrm{wh}(\alpha)$ with unipotent matrices α. There are rings A such that $\mathrm{wh}(\mathrm{SL}_2 A) = \mathrm{SK}_1 A \neq \mathrm{Nill}_1 A$; see [2]. For such a ring A, there in no N and P such that $P(A^N) = \mathrm{SL}_2 A$.

1. **Proof of Theorem** 1

We denote elementary matrices by

$$b^{1,2} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad c^{2,1} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}.$$

It is clear that each of the subgroups $\mathbb{Z}^{1,2}$ and $\mathbb{Z}^{2,1}$ of $\mathrm{SL}_2 \mathbb{Z}$ is a polynomial family with one parameter.

Note that the conjugates of all elementary matrices are covered by a polynomial matrix

$$\Phi_3(y_1, y_2, y_3) := \begin{pmatrix} 1 + y_1 y_3 y_2 & y_1^2 y_3 \\ -y_2^2 y_3 & 1 - y_1 y_3 y_2 \end{pmatrix}$$

in three variables. Namely, for $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2 \mathbb{Z}$,

$$\alpha e^{1,2} \alpha^{-1} = \begin{pmatrix} 1 - aec & a^2 e \\ -c^2 e & 1 + aec \end{pmatrix} \quad \text{and} \quad \alpha e^{2,1} \alpha^{-1} = \begin{pmatrix} 1 + bed & -b^2 e \\ d^2 e & 1 - bed \end{pmatrix}.$$

Remark 2. Conversely, every value of Φ_3 is a conjugate of $b^{1,2}$ in $\mathrm{SL}_2 \mathbb{Z}$ for some $b \in \mathbb{Z}$.

Next we denote by X_4 the set of matrices of the form

$$\alpha\alpha^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \left[\alpha, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right] = \alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \alpha^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

where $\alpha \in \mathrm{SL}_2 \mathbb{Z}$. Since

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

we have

$$\begin{aligned} \alpha\alpha^T &= \begin{pmatrix} 1 - bd & b^2 \\ -d^2 & 1 + bd \end{pmatrix} \begin{pmatrix} 1 - ac & a^2 \\ -c^2 & 1 + ac \end{pmatrix} \begin{pmatrix} 1 - bd & b^2 \\ -d^2 & 1 + bd \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &=: \Phi_4(a, b, c, d). \end{aligned}$$

Hence the set X_4 is covered by a polynomial matrix $\Phi_4(y_1, y_2, y_3, y_4)$ in four variables: $X_4 \subset \Phi_4(\mathbb{Z}^4)$.

Remark 3. $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \Phi_4(0, 0, 0, 0) \in \Phi_4(\mathbb{Z}^4)$, while reduction modulo 2 shows that X_4 does not contain $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

Note that $\Phi_4(\pm 1, 0, 0, \pm 1) = \operatorname{diag}(1, 1)$. Therefore we can define the polynomial matrix

$$\Phi_5(y_1, y_2, y_3, y_4, y_5) = \begin{pmatrix} y_5 & 0 \\ 0 & 1 \end{pmatrix} \Phi_4(1+y_1y_5, y_2y_5, y_3y_5, 1+y_4y_5) \begin{pmatrix} y_5 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \in \mathrm{SL}_2(\mathbb{Z}[y_1, y_2, y_3, y_4, y_5]).$$

By definition,

$$\begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+ae & be \\ ce & 1+de \end{pmatrix} \begin{pmatrix} 1+ae & ce \\ be & 1+de \end{pmatrix} \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1+ae & be^2 \\ c & 1+de \end{pmatrix} \begin{pmatrix} 1+ae & ce^2 \\ b & 1+de \end{pmatrix} \in \Phi_5(\mathbb{Z}^5)$$

if $a, b, c, d, e \in \mathbb{Z}$, $e \neq 0$, and the second matrix on the left side is in $\mathrm{SL}_2\,\mathbb{Z}$.

For $a, b, c, d, e \in \mathbb{Z}$, we denote by $X_5 \subset \Phi_5(\mathbb{Z}^5)$ the set of matrices of the form

$$\begin{pmatrix} 1+ae & be^2 \\ c & 1+de \end{pmatrix} \begin{pmatrix} 1+ae & ce^2 \\ b & 1+de \end{pmatrix} \quad \text{with} \quad \begin{pmatrix} 1+ae & be^2 \\ c & 1+de \end{pmatrix} \in \mathrm{SL}_2\,\mathbb{Z}.$$

The case $e = 0$ is included because $\Phi_5(0, b, c, 0, 0) = \left(\begin{smallmatrix} 1 & 0 \\ b+c & 1 \end{smallmatrix}\right)$.

Note that $X_5^{-1} = X_5$. Set $Y_5 := X_5^T$ (the transpose of the set X_5).

Our next goal is to prove that every matrix in $\mathrm{SL}_2\,\mathbb{Z}$ is a product of a small number of elementary matrices and matrices from X_5 and Y_5.

LEMMA 1.1. *Let $a, c, e \in \mathbb{Z}$, and let $\alpha = \left(\begin{smallmatrix} 1+ae & ce \\ * & * \end{smallmatrix}\right) \in \mathrm{SL}_2\,\mathbb{Z}$. Then there are $u, v \in \mathbb{Z}$, $\varepsilon \in \{1, -1\}$, and $\varphi \in X_5$ such that the matrix*

$$\alpha(eu)^{1,2} v^{2,1} (-c_1 e)^{1,2} \varphi (-\varepsilon e v)^{1,2} (-\varepsilon u)^{2,1}$$

has the form $\begin{pmatrix} * & * \\ \varepsilon c & 1+ae \end{pmatrix}$, *where $c_1 := c + u(1+ae)$.*

Proof. The case $1 + ae = 0$ is trivial (we can take $u = v = 0$ and $\varepsilon = -e$), so we assume that $1 + ae \neq 0$. By Dirichlet's theorem on primes in arithmetic progressions, we find $u \in \mathbb{Z}$ such that either $c_1 := c + u(1 + ae) \equiv 1 \bmod 4$ and $-c_1$ is a prime or $c_1 := c + u(1 + ae) \equiv 3 \bmod 4$ and c_1 is a prime. Then $\mathrm{GL}_1(\mathbb{Z}/c_1\mathbb{Z})$ is a cyclic group, and the image of -1 in this group is not a square. So $a = \pm a_1^2 \bmod c_1$ for some $a_1 \in \mathbb{Z}$. We write $a + vc_1 = \varepsilon a_1^2$ with $v \in \mathbb{Z}$ and $\varepsilon \in \mathrm{GL}_1\,\mathbb{Z}$. Then, for some $b_1, d_1 \in \mathbb{Z}$,

$$\alpha(ue)^{1,2} v^{2,1} (-c_1 e)^{1,2} = \begin{pmatrix} 1+\varepsilon a_1^2 e & c_1 e \\ * & * \end{pmatrix} (-c_1 e)^{1,2} = \begin{pmatrix} 1+\varepsilon a_1^2 e & -\varepsilon c_1 e^2 a_1^2 \\ b_1 & d_1 \end{pmatrix}.$$

Let β be the rightmost matrix above, and note that

$$\beta^{-1} = \begin{pmatrix} d_1 & \varepsilon c_1 a_1^2 e^2 \\ -b_1 & 1+\varepsilon a_1^2 e \end{pmatrix}.$$

Since $\det(\beta) = 1$, we conclude that $d_1 - 1 \in e\mathbb{Z}$.

We set

$$\gamma := \begin{pmatrix} d_1 & -b_1 a_1^2 e^2 \\ \varepsilon c_1 & 1+\varepsilon a_1^2 e \end{pmatrix} = \begin{pmatrix} * & * \\ \varepsilon c_1 & 1+(a+vc_1)e \end{pmatrix}.$$

Then $\varphi := \beta^{-1}\gamma \in X_5$ and $\gamma = \beta\varphi$.

Now

$$\begin{aligned}\gamma(-\varepsilon ev)^{1,2}(-\varepsilon u)^{2,1} &= \begin{pmatrix} * & * \\ \varepsilon c_1 & 1+ae \end{pmatrix}(-\varepsilon u)^{2,1} \\ &= \begin{pmatrix} * & * \\ \varepsilon(c+u(1+ae)) & 1+ae \end{pmatrix}(-\varepsilon u)^{2,1} = \begin{pmatrix} * & * \\ \varepsilon c & 1+ae \end{pmatrix}. \quad \square\end{aligned}$$

LEMMA 1.2. *Let* $\alpha = \left(\begin{smallmatrix} a & b \\ * & * \end{smallmatrix}\right) \in \mathrm{SL}_2\,\mathbb{Z}$, *with* $m \geq 1$ *an integer. Then there are* $z_i \in \mathbb{Z}$, $\varphi \in X_5$, *and* $\psi \in Y_5$ *such that*

$$\alpha^m z_1^{1,2} z_2^{2,1} z_3^{1,2} \varphi z_4^{1,2} z_5^{2,1} z_6^{1,2} z_7^{2,1} \psi z_8^{2,1} z_9^{1,2} z_{10}^{2,1} = \begin{pmatrix} a^m & b \\ * & * \end{pmatrix}.$$

Proof. By the Cayley-Hamilton theorem and mathematical induction on m, we have

$$\alpha^m = f 1_2 + g\alpha = \begin{pmatrix} f+ga & gb \\ * & * \end{pmatrix} \quad \text{with } f, g \in \mathbb{Z},$$

where 1_2 is the identity matrix. Since $1 = \det(\alpha^m) \equiv f^2 \bmod g$, we can write $g = g_1 g_2$ with $f \equiv 1 \bmod g_1$ and $f \equiv -1 \bmod g_2$.

By Lemma 1.1, there are $z_1, z_2, z_3, z_4, k_1 \in \mathbb{Z}$ and $\varphi_1 \in X_5$ such that

$$\alpha^m z_1^{1,2} z_2^{2,1} z_3^{1,2} \varphi_1 z_4^{1,2} k_1^{2,1} =: \beta = \beta = \begin{pmatrix} * & * \\ \pm g_2 b & f+ga \end{pmatrix}.$$

Now we apply Lemma 1.1 to the matrix

$$\theta = -\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \beta \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} -f-ga & \pm g_2 b \\ * & * \end{pmatrix}$$

instead of α. So there are $k_2, -z_6, -z_7, -z_8, -z_9 \in \mathbb{Z}$ and $\varphi' \in X_5$ such that

$$\theta k_2^{1,2}(-z_6)^{2,1}(-z_7)^{1,2}\varphi'(-z_8)^{1,2}(-z_9)^{2,1} = \begin{pmatrix} * & * \\ \pm b & -f-ga \end{pmatrix}.$$

Negating this and conjugating by $\big(0 \quad -1\genfrac{}{}{0pt}{}{1}{0}\big)^{-1}$ we obtain that

$$\beta(-k_2)^{2,1} z_6^{1,2} z_7^{2,1} \psi z_8^{2,1} z_9^{1,2} = \mu = \begin{pmatrix} f+ga & \pm b \\ * & * \end{pmatrix},$$

where $\psi := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)^{-1} \varphi' \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in Y_5$.

The matrix α is lower triangular modulo b, so $f + ga \equiv a^m \bmod b$. We find $z_{10} \in \mathbb{Z}$ such that $f + ga \pm z_{10} b = a^m$ and set $z_5 = k_1 - k_2$ to obtain our conclusion. □

COROLLARY 1.3. *Let* $\alpha = \left(\begin{smallmatrix} a & b \\ * & * \end{smallmatrix}\right) \in \mathrm{SL}_2\,\mathbb{Z}$, *with* $m \geq 1$ *an integer, and* $\varepsilon \in \{\pm 1\}$. *Assume that* $a^m \equiv \varepsilon \bmod b$. *Then there are* $z_i \in \mathbb{Z}$ *and* $\varphi_i \in X_5$ *such that*

$$\alpha^m z_1^{1,2} z_2^{2,1} z_3^{1,2} \varphi_1 z_4^{1,2} z_5^{2,1} z_6^{1,2} z_7^{2,1} \varphi_2 z_8^{2,1} z_9^{1,2} z_{10}^{2,1} z_{11}^{1,2} z_{12}^{2,1} = \varepsilon 1_2.$$

Proof. By Lemma 1.2, we find $t_1, z_i \in \mathbb{Z}$ with $1 \leq i \leq 9$, $\varphi \in X_5$, and $\psi \in Y_5$ such that the matrix

$$\beta := \alpha^m z_1^{1,2} z_2^{2,1} z_3^{1,2} \varphi z_4^{1,2} z_5^{2,1} z_6^{1,2} z_7^{2,1} \psi z_8^{2,1} z_9^{1,2} t_1^{2,1} = \begin{pmatrix} a^m & b \\ * & * \end{pmatrix}.$$

Now we can find $t_2, z_{11}, z_{12} \in \mathbb{Z}$ such that $\beta t_2^{2,1} z_{11}^{1,2} z_{12}^{2,1} = \varepsilon 1_2$. The conclusion follows from setting $z_{10} = t_1 + t_2$. □

For any integer $s \geq 1$, we denote by the Δ_s the following polynomial matrix in s parameters:

$$\Delta_s(y_1, \ldots, y_s) = y_1^{1,2} y_2^{2,1} \cdots,$$

where the last factor is the elementary matrix $y_s^{1,2}$ (resp., $y_s^{2,1}$) when s is odd (resp., even). We set

$$\Gamma_s(y_1, \ldots, y_s) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Delta_s(y_1, \ldots, y_s) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}.$$

Note that

$$\Gamma_s(y_1, \ldots, y_s) = \Delta_s(y_1, \ldots, y_s)^{-1} = \Gamma_s(y_1, \ldots, y_s)^T \quad \text{for even } s,$$
$$\Delta_s(y_1, \ldots, y_s) = \Delta_s(y_1, \ldots, y_s)^{-1} = \Gamma_s(y_1, \ldots, y_s)^T \quad \text{for odd } s,$$

where "T" denotes transpose, and that $\Delta_s(y_1, \ldots, y_s) = \Gamma_{s+1}(0, y_1, \ldots, y_s)$ for any s.

COROLLARY 1.4. *Let* $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2\,\mathbb{Z}$ *and* $\varepsilon \in \{\pm 1\}$. *Assume that for some coprime integers* $m, n \geq 1$, *we have* $a^m \equiv \pm 1 \bmod b$ *and* $a^n \equiv \pm 1 \bmod c$. *Then there are* $\varepsilon \in \{\pm 1\}$, $\delta_i \in \Delta_i(\mathbb{Z}^i)$, $\gamma_i \in \Gamma_i(\mathbb{Z}^i)$, $\varphi_i \in X_5$, *and* $\psi_i \in Y_5$ *such that*

$$\alpha = \varepsilon \gamma_5 \varphi_1 \gamma_4 \psi_2 \delta_7 \psi_1 \delta_4 \varphi_2 \gamma_3.$$

Proof. Replacing m and n by their positive multiples, we can assume that $n = m - 1$. By Corollary 1.3,

$$\alpha^m = \pm\gamma_5\varphi_1\gamma_4\varphi_2\delta_3$$

with $\varphi_1, \varphi_2 \in X_5,\ \delta_3 \in \Delta_3(\mathbb{Z}^3),\ \gamma_4 \in \Gamma_4(\mathbb{Z}^4)$, and $\gamma_5 \in \Gamma_5(\mathbb{Z}^5)$.

Applying Corollary 1.3 to α^T instead of α, we get

$$(\alpha^T)^n = \pm\gamma_5'\varphi_1'\gamma_4'\varphi_2'\delta_3'$$

with $\varphi_i' \in X_5,\ \delta_3' \in \Delta_3(\mathbb{Z}^3)$, and $\gamma_i' \in \Gamma_i(\mathbb{Z}^i)$.

Conjugating by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, we obtain that

$$\alpha^{-n} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} (\alpha^T)^n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \pm\delta_5\psi_1\delta_4\psi_2\gamma_3$$

with $\psi_i \in Y_5,\ \gamma_3 \in \Gamma_3$, and $\delta_i \in \Delta_4(\mathbb{Z}^i)$.

Therefore

$$\alpha = \alpha^m\alpha^{-n} = \pm\gamma_5\varphi_1\gamma_4\varphi_2\delta_7\psi_1\delta_4\psi_2\gamma_3, \quad \text{where } \delta_7 := \delta_3\delta_5 \in \Delta_7(\mathbb{Z}^7). \qquad \square$$

PROPOSITION 1.5. *Every matrix $\alpha \in \mathrm{SL}_2\,\mathbb{Z}$ can be represented as*

$$\alpha = \gamma_5\varphi_1\gamma_4\varphi_2\delta_7\psi_1\delta_4\psi_2\gamma_6$$

with $\delta_i \in \Delta_i(\mathbb{Z}^i),\ \gamma_i \in \Gamma_i(\mathbb{Z}^i),\ \varphi_i \in X_5$, and $\psi_i \in Y_5$.

Proof. Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. The case $a = 0$ is trivial, so let $a \neq 0$. As in the proof of Lemma 1.1, can find an integer u such that $|b + au|$ is a positive prime $\equiv 3$ modulo 4. Then we find an integer v such that $c + av$ is a positive prime such that

$$\mathrm{GCD}(c + av - 1, |b + au| - 1) = 1 \text{ or } 2.$$

Let now $m = (|b + au| - 1)/2$ and $n = c + av - 1$. Then $\mathrm{GCD}(m, n) = 1$, i.e., m, n are coprime, i.e., $(m, n) \in \mathrm{Um}_2\,\mathbb{Z}$. Moreover $a^m \equiv \pm 1 \bmod (b + au)$ and $a^m \equiv 1 \bmod (c + av)$.

By Corollary 1.4, we have

$$v^{2,1}\alpha u^{1,2} = \pm\gamma_5'\varphi_1\gamma_4\varphi_2\delta_7\psi_1\delta_4\psi_2\gamma_3$$

with $\delta_i \in \Delta_i(\mathbb{Z}^i),\ \gamma_i, \gamma_i' \in \Gamma_i(\mathbb{Z}^i),\ \varphi_i \in X_5$, and $\psi_i \in Y_5$.

Set $\gamma_5 = (-v)^{2,1}\gamma_5' \in \Gamma_5(\mathbb{Z}^5)$ and $\gamma_4' = \gamma_3(-u)^{1,2} \in \Gamma_4(\mathbb{Z}^4)$. It remains to observe that $\pm 1_2 \in \Delta_4(\mathbb{Z}^4) \cap \Gamma_4(\mathbb{Z}^4)$; hence $\pm\Gamma_i(\mathbb{Z}^i) \subset \Gamma_{i+2}(\mathbb{Z}^{i+2})$ for all $i \geq 1$. In particular, both γ_4' and $-\gamma_4'$ belong to $\Gamma_6(\mathbb{Z}^6)$. $\square$

Note that Theorem 1 follows from Proposition 1.5. The polynomial parametrization of $\mathrm{SL}_2\,\mathbb{Z}$ in Proposition 1.5 is explicit enough to see that the number of parameters is 46 and the total degree is at most 78. This is because the degrees of Δ_s and Γ_s are both s and the degree of Φ_5 is 13.

2. **Primitive vectors and systems of linear equations**

First, Proposition 1.5 yields a lemma:

LEMMA 2.1. *For any* $(a,b) \in \mathrm{Um}_2 \mathbb{Z}$ *there are* $\delta_i, \delta_i' \in \Delta_i(\mathbb{Z}^i)$, $\varphi_i \in X_5$, $\gamma_4, \gamma_6 \in \Gamma_i(\mathbb{Z}^4)$, *and* $\psi_i \in Y_5$ *such that*

$$(a,b) = (1,0)\delta_4'\varphi_1\gamma_4\psi_2\delta_7\psi_1\delta_4\varphi_2\gamma_6.$$

Proof. Let α be a matrix in $\mathrm{SL}_2 \mathbb{Z}$ with the first row (a,b). We write α as in Proposition 1.5. Multiplying by the row $(1,0)$ on the left, we obtain

$$(a,b) = (1,0)\alpha = (1,0)\gamma_5\varphi_1\gamma_4\psi_2\delta_7\psi_1\delta_4\varphi_2\gamma_6.$$

Since

$$(1,0)\Gamma_s(y_1,\dots,y_s) = (1,0)\Delta_{s-1}(y_2,\dots,y_s),$$

we can replace γ_5 by $\delta_4' \in \Delta_4(\mathbb{Z}^4)$. □

The lemma implies the following result:

THEOREM 2.2. *The set* $\mathrm{Um}_2 \mathbb{Z}$ *of coprime pairs of integers admits a polynomial parametrization with* 45 *parameters.*

For $n \geq 3$, it is easy to show that $\mathrm{Um}_n \mathbb{Z}$ admits a polynomial parametrization with $2n$ parameters. This is because the ring $\mathbb{Z}$ satisfies the second Bass stable range condition. Now we introduce this condition.

A row $(a_1,\dots,a_n) \in A^n$ over an associative ring A with 1 is said to be *unimodular* if $a_1A + \cdots + a_nA = A$, i.e., there are $b_i \in A$ such that $\sum a_ib_i = 1$. Let $\mathrm{Um}_n A$ denote the set of all unimodular rows in A^n.

We write $\mathrm{sr}(A) \leq n$ if for any $(a_1,\dots,a_{n+1}) \in \mathrm{Um}_{n+1} A$ there are $c_i \in A$ such that $(a_1 + a_{n+1}c_1,\dots,a_n + a_{n+1}c_n) \in \mathrm{Um}_n A$.

For example, it is easy to see that $\mathrm{sr}(A) \leq 1$ for any semi-local ring A and that $\mathrm{sr}(\mathbb{Z}) \leq 2$.

It is shown in [16] that for any m the condition $\mathrm{sr}(A) \leq m$ implies that $\mathrm{sr}(A) \leq n$ for every $n \geq m$. Moreover, if $\mathrm{sr}(A) \leq m$ and $n \geq m+1$, then for any $a = (a_1,\dots,a_n) \in \mathrm{Um}_n A$ there are $c_1,\dots,c_m \in A$ such that $a' = (a_i') \in \mathrm{Um}_{n-1} A$, where $a_i' = a_i + a_nc_i$ for $i = 1,\dots,m$ and $a_i' = a_i$ for $i = m+1,\dots,n-1$.

Using now $b_i \in A$ such that $\sum a_i'b_i = 1$, we obtain that

$$a\prod_{i=1}^{m} c_i^{n,i} \prod_{i=1}^{n-1}(b_i(1-a_n))^{i,n} \prod_{i=1}^{n-1}(-a_i')^{n,i} = (0,\dots,0,1).$$

Here $x^{i,j}$ denotes an elementary matrix with x at position (i,j). We denote by E_nA the subgroup of $\mathrm{GL}_n A$ generated by these elementary matrices.

Thus, there is a polynomial matrix $\alpha \in E_n(\mathbb{Z}\langle y_1, \dots, y_{2n+m-2}\rangle)$ (with non-commuting y_i) that is a product of $2n+m-2$ elementary matrices, such that $\mathrm{Um}_n\, A$ is the set of last rows of all matrices in $\alpha(\mathbb{Z}^{2n+m-2})$.

In particular, taking $A = \mathbb{Z}$ and $m = 2$, we obtain this:

PROPOSITION 2.3. *For any $n \geq 3$, the set $\mathrm{Um}_n\, \mathbb{Z}$ is a polynomial family with $2n$ parameters.*

Now we are ready to prove Corollary 2. Consider now an arbitrary system $x\gamma = b$ of l linear equations for k variables x with integer coefficients. We write x and solutions as rows. Reducing the coefficient matrix γ to a diagonal form $\alpha\gamma\beta$ (where $\alpha \in \mathrm{SL}_k\, \mathbb{Z}$, $\beta \in \mathrm{SL}_l\, \mathbb{Z}$, and the diagonal entries are the Smith invariants) by row and column addition operations with integer coefficient, we write our answer, describing all integer solutions, in one of these three forms:

(1) $0 = 1$ (there are no solutions);

(2) $x = c\alpha$, where $c \in \mathbb{Z}^k$ (so $c\alpha$ is only solution);

(3) $x = y\alpha$, where y is the row of k parameters (i.e., x is arbitrary);

(4) $x = (a, y)\alpha$ with a row y of N parameters ($1 \leq N \leq k-1$) and $a \in \mathbb{Z}^{k-N}$.

Thus, the set X of all solutions, when it is not empty, is a polynomial family with N parameters ($0 \leq N \leq k$) and the degree of parametrization is at most 1.

Now we are interested in the set Y primitive solutions. In case (1), Y is empty. In case (2), Y either is empty or consists of a single solution.

In case (3), $N = k$ and $Y = \mathrm{Um}_N\, \mathbb{Z}$, which is a polynomial family by Theorem 2.2 and Proposition 2.3 provided that $N \geq 2$. When $N = 1$, we have $\alpha = \pm 1$, and the set $Y = \mathrm{Um}_1\, \mathbb{Z} = \{\pm 1\}$ is not a polynomial family, but consists of two constant polynomial families.

In case (4) with $a = 0$ (the homogeneous case), we have $N < k$ and the set Y is also parametrized by $\mathrm{Um}_N\, \mathbb{Z}$.

Now we have to deal with case (4) with $a \neq 0$. Let $d = \mathrm{GCD}(a)$. Then Y is parametrized by the set $\{Z = \{b \in \mathbb{Z}^N : \mathrm{GCD}(d, \mathrm{GCD}(b)) = 1\}$. We find a polynomial $f(t) \in \mathbb{Z}[t]$ whose range reduced modulo d is $\mathrm{GL}_1(\mathbb{Z}/d\mathbb{Z})$. (Find $f(t)$ modulo every prime p dividing d and then use the Chinese Remainder Theorem; the degree of $f(t)$ is at most the largest $p-1$.)

Then the range of the polynomial $f_2(t_1, t_2) := f(t_1) + dt_2$ consists of all integers z such that $\mathrm{GCD}(d, z) = 1$. Therefore the set Z consists of $f_2(z_1, z_2)u$ with $z_1, z_2 \in \mathbb{Z}$ and $u \in \mathrm{Um}_N\, \mathbb{Z}$. Thus, any polynomial parametrization of $\mathrm{Um}_N\, \mathbb{Z}$ yields a polynomial parametrization of Z (and hence Y) with two additional parameters. By Theorem 2.2 and Proposition 2.3, the number of parameters is at most $41 + 2k$ (at most $2k$ when $N \geq 3$).

3. **Quadratic equations**

In this section we prove Corollary 4, which includes Corollary 3 as a particular case with $Q_0 = 1$, $k = 2n$, and

$$Q'(x_5, \dots, x_k) = x_5x_6 + \cdots + x_{2n-1}x_{2n}$$

($Q' = 0$ when $n = 2$). We write the k-tuples in $\mathbb{Z}^k$ as rows. Let $e_1, \dots, e_k$ be the standard basis in $\mathbb{Z}^k$.

We denote by $\mathrm{SO}(Q, \mathbb{Z})$ the subgroup of $\mathrm{SL}_n \mathbb{Z}$ consisting of matrices $a \in \mathrm{SL}_n \mathbb{Z}$ such that $Q(x\alpha) = Q(x)$. In the end of this section, we prove that, under the conditions of Corollary 4, the group $\mathrm{SO}(Q, \mathbb{Z})$ consists of two disjoint polynomial families.

We define a bilinear form $(\cdot, \cdot)_Q$ on $\mathbb{Z}^k$ by $(a, b)_Q = Q(a+b)-Q(a)-Q(b)$.

Following [20], we introduce elementary transformations

$$\tau(e, u) \in \mathrm{SO}(Q, \mathbb{Z}),$$

where $e = e_1$ or e_2 and $(e, u)_Q = 0$, by setting

$$v\tau(e, u) = v + (e, v)_Q u - (u, v)_Q e - Q(u)(e, v)_Q e$$

(this works because $Q(e) = 0$).

LEMMA 3.1. *Let Q be as in Corollary* 4. *Then for any Q-unimodular row $v \in \mathbb{Z}^k$, there are $u, u' \in U = \sum_{i=5}^{k} \mathbb{Z}e_i \subset \mathbb{Z}^k$ such that the first four entries of the row $v\tau(e_1, u)\tau(e_2, u')$ form a primitive row.*

Proof. We write $v = (v_1, v_2, \dots, v_k)$. First we want to find a $u \in U$ such that $\mathbb{Z}v_1' + \mathbb{Z}v_3 + \mathbb{Z}v_4 \neq 0$, where $v' = (v_i') = v\tau(e_1, u)$ (note that $v_i' = v_i$ for $i = 2, 3, 4$). If $\mathbb{Z}v_1 + \mathbb{Z}v_3 + \mathbb{Z}v_4 \neq 0$, we can take $u = 0$.

Otherwise, since v is Q-unimodular, $\mathbb{Z}v_2 + \mathbb{Z}(v, w)_Q \neq 0$ for some $w \in U$. For $v' = (v_i') = v\tau(e_1, cw)$ with $c \in \mathbb{Z}$, we have $v_1' = v_1 - (v, w)_Q c - Q(w)v_2c^2$ is a nonconstant polynomial in c (with $v_1 = 0$), so it takes a nonzero value for some c. Therefore we can set $u = cw$ with this c.

Now we want to find $u' \in U$ such that

$$(v_1'', v_2'', v_3'', v_4'') = (v_1', v_2'', v_3, v_4') \in \mathrm{Um}_4 \mathbb{Z},$$

where

$$w'' = (v_i'') = v'\tau(e_2, u') = v\tau(e_1, u)\tau(e_2, u').$$

Since v' is Q-unimodular, there is a $w' \in U$ such that

$$(v_1', v_2, v_3, v_4, (v', w')_Q) \in \mathrm{Um}_5 \mathbb{Z}.$$

Since $\mathbb{Z}v_1' + \mathbb{Z}v_3 + \mathbb{Z}v_4 \neq 0$, there is a $c' \in \mathbb{Z}$ such that

$$(v_1', v_2 - c'(v', w')_Q, v_3, v_4) \in \mathrm{Um}_4 \mathbb{Z}.$$

We set $u' = c'w'$. Then $v'\tau(e_2, u') = (v''_i)$ with

$$(v''_1, v''_2, v''_3, v''_4) = (v'_1, v_2 - c'(v', w')_Q - c'^2 Q(w')v'_1, v_3, v_4) \in \mathrm{Um}_4\,\mathbb{Z}. \quad \square$$

LEMMA 3.2. *Let $k \geq 4$, $Q_0 \in \mathbb{Z}$, Q' any quadratic form in $k-4$ variables, and $Q(x_1, \ldots, x_k) = x_1x_2 + x_3x_4 + Q'(x_5, \ldots, x_k)$. Then the set X' of integer solutions for the equation $Q(x) = Q_0$ with $(x_1, x_2, x_3, x_4) \in \mathrm{Um}_4\,\mathbb{Z}$ is a polynomial family with $k+88$ parameters.*

Proof. When $k = 4$, see Examples 6 and 8. Assume now that $k \geq 5$. Let $v = (v_i) \in X'$. Set $D = v_1v_2 + v_3v_4 \in \mathbb{Z}$. We can write

$$\begin{pmatrix} v_1 & v_3 \\ -v_4 & v_2 \end{pmatrix} = \alpha^{-1} \begin{pmatrix} 1 & 0 \\ 0 & D \end{pmatrix} \beta$$

with $\alpha, \beta \in \mathrm{SL}_2\,\mathbb{Z}$. Then we can write

$$(1, D, 0, 0, v_5, \ldots, v_k) = (1, Q_0, 0, \ldots, 0)\tau(e_2, \textstyle\sum_{i=5}^k v_i e_i).$$

Therefore X is parametrized by $k-5$ parameters $v_5, \ldots, v_k$ and two matrices in $\mathrm{SL}_2\,\mathbb{Z}$. By Theorem 1, X is a polynomial family with $k - 4 + 2 \cdot 46 = k + 88$ parameters. $\square$

Combining Lemmas 3.1 and 3.2, we obtain Corollary 4.

LEMMA 3.3. *Under the conditions of Lemma 3.2, assume that $k \geq 6$ and that $Q'(x_5, \ldots, x_k) = x_5x_6 + Q''(x_7, \ldots, x_k)$. Then the set X' is a polynomial family with $k+2$ parameters.*

Proof. Let $(v_i) \in X'$. There is an orthogonal transformation $\alpha \in \mathrm{SO}_4\,\mathbb{Z}$ (coming from $\mathrm{Spin}_4\,\mathbb{Z} = \mathrm{SL}_2\,\mathbb{Z} \times \mathrm{SL}_2\,\mathbb{Z}$; see Example 8) such that

$$(v_1, v_2, v_3, v_4)\alpha = (1, v_1v_2 + v_3v_4, 0, 0).$$

We set $(w_1, w_2, w_3, w_4) = (0, 1, 0, 0)\alpha^{-1}$ and

$$w = e_1w_1 + e_2w_2 + e_3w_3 + e_4w_4 \in \mathbb{Z}^k.$$

Then $Q(w) = 0 = (w, v)_Q$.

Consider the row $v' = (v'_i) = v\tau(v_5, (1-v_5)w)$. For $i = 1, 2, 3, 4$, we have $v'_i = v_i + (1-v_5)w_i$. Also $v'_5 = 1$, and $v'_i = v_i$ for $i \geq 6$.

So $v'\tau(e_6, -\sum_{i \neq 5,6} v'_i) = e_5$; hence X' is parametrized by $4 + (k-2) = k+2$ parameters. $\square$

Combining Lemmas 3.1 and 3.3, we obtain:

PROPOSITION 3.4. *Let $k \geq 6$, $Q_0 \in \mathbb{Z}$, Q'' a quadratic form in $k-6$ variables, and $Q(x_1, \ldots, x_k) = x_1x_2 + x_3x_4 + x_5x_6 + Q''(x_7, \ldots, x_k)$. Then the set of all Q-unimodular solutions for the equation $Q(x) = Q_0$ is a polynomial family with $3k-6$ parameters.*

4. **Chevalley-Demazure groups**

We prove here Corollary 17. Let $n \geq 2$, and take $e_1, \dots, e_n$ as the standard basis of $\mathbb{Z}^n$.

First we prove by induction on n that $\mathrm{SL}_n \mathbb{Z}$ admits a polynomial factorization with $39 + n(3n+1)/2$ parameters. The case $n = 2$ is covered by Theorem 1. Let $n \geq 3$.

We consider the orbit $e_n \mathrm{SL}(n, \mathbb{Z})$.

The orbit admits a parametrization by $2n$ parameters by Proposition 2.3. Moreover, there is a polynomial matrix $\alpha \in E_n(\mathbb{Z}[y_1, \dots, y_{2n}])$ that is a product of $2n$ elementary matrices, such that $\mathrm{Um}_n \mathbb{Z} = e_n \alpha(\mathbb{Z}^{2n})$.

The stationary group of e_n consists of all matrices of the form

$$\begin{pmatrix} \beta & v \\ 0 & 1 \end{pmatrix}, \quad \text{where } v^T \in \mathbb{Z}^{n-1}.$$

By the induction hypothesis, the stationary group can be parametrized by $39 + (n-1)(3n-2)/2 + n - 1$ parameters. Thus $\mathrm{SL}_n \mathbb{Z}$ can be parametrized by $39 + (n-1)(3n-2)/2 + n - 1 + 2n = 39 + n(3n+1)/2$ parameters.

Now we consider the symplectic groups $\mathrm{Sp}_{2n} \mathbb{Z}$. We prove Corollary 17(c) by induction on n. When $n = 1$, $\mathrm{Sp}_2 \mathbb{Z} = \mathrm{SL}_2 \mathbb{Z}$. Assume now that $n \geq 2$.

As in [2], using that $\mathrm{sr}(\mathbb{Z}) = 2$, we have a matrix

$$\alpha \in \mathrm{Sp}_{2n}(\mathbb{Z}[y_1, \dots, y_{4n}]) \quad \text{such that } e_{2n}\alpha = \mathrm{Um}_{2n} \mathbb{Z}.$$

The stationary group consists of all matrices of the form

$$\begin{pmatrix} \beta & 0 & v \\ v^T & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{where } v^T \in \mathbb{Z}^{2n-2} \text{ and } c \in \mathbb{Z},$$

so by the induction hypothesis it is parametrized by

$$2(n-1)^2 + 2(n-1) + 41 + 2n - 1$$

parameters. Therefore $\mathrm{Sp}_{2n} \mathbb{Z}$ is parametrized by

$$2(n-1)^2 + 2(n-1) + 39 + 2n - 1 + 4n = 3n^2 + 2n + 41$$

parameters.

Now we discuss polynomial parametrizations of the spinor groups

$$\mathrm{Spin}_{2n} \mathbb{Z} = \mathrm{Spin}(Q_{2n}, \mathbb{Z}) \quad \text{for } n \geq 3.$$

We prove Corollary 17(d) by induction on n. When $n = 3$, $\mathrm{Spin}_{2n} \mathbb{Z} = \mathrm{SL}_4 \mathbb{Z}$. Namely $\mathrm{SL}_4 \mathbb{Z}$ acts on alternating 4×4 integer matrices preserving the pfaffian, which is a quadratic form of type $x_1x_2 + x_3x_4 + x_5x_6$; see e.g. [21].

Assume now that $n \geq 4$. The group $\mathrm{Spin}_{2n}\,\mathbb{Z}$ acts on $\mathbb{Z}^{2n}$ via $\mathrm{SO}_{2n}\,\mathbb{Z}$. The orbit $e_{2n}\,\mathrm{SO}_{2n}\,\mathbb{Z}$ of e_{2n} is the set of all unimodular ($= Q_{2n}$-unimodular) solutions for the equation $Q_{2n} = 0$. By Proposition 3.4, the orbit is parametrized by $6n-6$ parameters. Also, the matrices $\tau(*,*)$ come from $\mathrm{Spin}_{2n}\,\mathbb{Z}$, so there is a polynomial matrix in $\mathrm{Spin}_{2n}\,\mathbb{Z}$ with $6n-6$ parameters that parametrizes the orbit. The stationary subgroup in $\mathrm{SO}_{2n}\,\mathbb{Z}$ consists of the matrices of the form

$$\begin{pmatrix} \beta & 0 & v \\ v^t & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{where } v^T \in \mathbb{Z}^{2n-2},\ c = Q_{2n-2}(v^T) \in \mathbb{Z},\ \beta \in \mathrm{SO}_{2n-2}\,\mathbb{Z}.$$

By the induction hypothesis, the stationary subgroup of e_1 in $\mathrm{Spin}_{2n}\,\mathbb{Z}$ is parametrized by

$$4(n-1)^2 - (n-1) + 34 + 2n - 2$$

parameters. So $\mathrm{Spin}_{2n}\,\mathbb{Z}$ is a polynomial family with

$$4(n-1)^2 - (n-1) + 36 + 2n - 2 + 6n - 3 = 4n^2 - n + 36$$

parameters.

Finally, we prove Corollary 17(b) by induction on n. When $n = 2$, $\mathrm{Spin}_5\,\mathbb{Z} = \mathrm{Sp}_4\,\mathbb{Z}$ (the group $\mathrm{Sp}_4\,\mathbb{Z} \subset \mathrm{SL}_4\,\mathbb{Z}$ acts on the alternating matrices as above, fixing a vector of length 1) and the formula works.

Let now $n \geq 3$. The orbit $e_1\,\mathrm{SO}_{2n+1}\,\mathbb{Z}$ of e_1 is the set of all unimodular ($= Q_{2n}$-unimodular) solutions of the equation $Q_{2n+1} = 0$. By Proposition 3.4, the orbit is parametrized by $3(2n+1) - 6 = 6n - 3$ parameters. Moreover, the matrices $\tau(*,*)$ come from $\mathrm{Spin}_{2n}\,\mathbb{Z}$, so there is a polynomial matrix in $\mathrm{Spin}_{2n}\,\mathbb{Z}$ with $6n-3$ parameters that parametrizes the orbit. The stationary subgroup of e_1 in $\mathrm{SO}_{2n+1}\,\mathbb{Z}$ consists of the matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ c & 1 & v \\ v^T & 0 & \beta \end{pmatrix}, \quad \text{where } v \in \mathbb{Z}^{2n-1},\ c = Q_{2n-1}(v) \in \mathbb{Z},\ \beta \in \mathrm{SO}_{2n-1}\,\mathbb{Z}.$$

By the induction hypothesis, the stationary subgroup of e_1 in $\mathrm{Spin}_{2n-1}\,\mathbb{Z}$ is parametrized by $4(n-1)^2 + 41 + 2n - 1$ parameters. So $\mathrm{Spin}_{2n}\,\mathbb{Z}$ is a polynomial family with

$$4(n-1)^2 + 41 + 2n - 1 + 6n - 3 = 4n^2 + 41$$

parameters.

Remark 4. As in Corollary 18, for any square-free integer D or $D = 0$, we obtain a polynomial parametrization of the set of all integer n by n matrices with determinant D. If D is not square-free, the set of matrices is a finite union of polynomial families.

5. **Congruence subgroups**

In this section we fix an integer $q \geq 2$. Denote by $G(q)$ the subgroup of $\mathrm{SL}_2\,\mathbb{Z}$ consisting of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $b, c \in q\mathbb{Z}$ and $a-1,\ d-1 \in q^2\mathbb{Z}$. This group is denoted by $G(q\mathbb{Z}, q\mathbb{Z})$ in [18]. Note that $\mathrm{SL}_2(q^2\mathbb{Z}) \subset G(q) = G(-q) \subset \mathrm{SL}_2\, q\mathbb{Z}$.

We parametrize $G(q)$ by the solutions of $x_1 + x_4 + q^2 x_1 x_4 - x_2 x_3 = 0$ as

$$x_1, x_2, x_3, x_4 \mapsto \begin{pmatrix} 1 + q^2 x_1 & q x_2 \\ q x_3 & 1 + q^2 x_4 \end{pmatrix}.$$

We use the polynomial matrices $\Phi_4(y_1, y_2, y_3, y_4)$ and $\Phi_5(y_1, y_2, y_3, y_4, y_5)$ defined in Section 1. We denote by $X_4(q) \subset \Phi_4(1+q^2\mathbb{Z}, q\mathbb{Z}, q\mathbb{Z}, 1+q^2\mathbb{Z}) \subset G(q)$ the set of matrices of the form $\alpha\alpha^T$ with $\alpha \in G(q)$. Notice that $X_4(q)^T = X_4(q)^{-1} = X_4(q)$.

We denote by $X_5(q) \subset \Phi_5(q^2\mathbb{Z}, q\mathbb{Z}, q\mathbb{Z}, q^2\mathbb{Z}, \mathbb{Z}) \subset G(q)$ the set of matrices of the form

$$\begin{pmatrix} 1 + aq^2 e & bqe^2 \\ cq & 1 + dq^2 e \end{pmatrix} \begin{pmatrix} 1 + aq^2 e & cq^2 e^2 \\ bq & 1 + dq^2 e \end{pmatrix}$$

with

$$a, b, c, d, e \in \mathbb{Z} \quad \text{and} \quad \begin{pmatrix} 1 + aq^2 e & bqe^2 \\ cq & 1 + dq^2 e \end{pmatrix} \in \mathrm{SL}_2\,\mathbb{Z}.$$

Set

$$Y_5(q) = (X_5(q)^{-1})^T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} X_5(q) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Notice that $X_5(q)^T = Y_5(q)^{-1} = Y_5(q)$ and $Y_5(q)^T = X_5(q)^{-1} = X_5(q)$

We also use the polynomial matrices Δ_i, Γ_i defined in Section 1. Notice that

$$\Delta_i(q\mathbb{Z}^i), \Gamma_i(q\mathbb{Z}^i) \subset G(q)$$

and that

$$\Delta_{2i}(q\mathbb{Z}^{2i})^T = \Delta_{2i}(q\mathbb{Z}^{2i}), \qquad \Delta_{2i}(q\mathbb{Z}^{2i})^{-1} = \Gamma_{2i}(q\mathbb{Z}^{2i}),$$
$$\Delta_{2i-1}(q\mathbb{Z}^{2i-1})^T = \Gamma_{2i-1}(q\mathbb{Z}^{2i-1}), \quad \Delta_{2i-1}(q\mathbb{Z}^{2i-1})^{-1} = \Delta_{2i-1}(q\mathbb{Z}^{2i-1})$$

for all integers $i \geq 1$.

LEMMA 5.1. *Let*

$$a, c, e \in \mathbb{Z}, \quad e \neq 0, \quad \alpha = \begin{pmatrix} 1 + aq^2 e & cqe \\ * & * \end{pmatrix} \in G(q).$$

Then there are $\delta_i \in \Delta_i(q\mathbb{Z}^i)$, $\varepsilon \in \{1, -1\}$, and $\varphi \in X_5(q)$ such that

$$\alpha\delta_3\varphi\delta_2 = \begin{pmatrix} * & * \\ \varepsilon cq & 1 + aq^2 e \end{pmatrix}.$$

Proof. As in the proof of Lemma 1.1 above, we find $u, v \in \mathbb{Z}$ such that $|c + u(1 + aq^2e)|$ is a prime $\equiv 3$ modulo 4 and $a + vq^2c_1 = \varepsilon a_1^2$, where

$$c_1 := c + u(1 + aq^2e), \quad a_1 \in \mathbb{Z}, \quad \varepsilon \in \mathrm{GL}_1\,\mathbb{Z}.$$

Set $\delta_3 = (uqe)^{1,2}(vq)^{2,1}(-c_1eq)^{1,2} \in \Delta_3(q\mathbb{Z}^3)$. Then, for some $b_1, d_1 \in \mathbb{Z}$,

$$\alpha\delta_3 = \begin{pmatrix} 1 + \varepsilon a_1^2 q^2 e & c_1qe \\ * & * \end{pmatrix} (-c_1eq)^{1,2} = \begin{pmatrix} 1 + \varepsilon a_1^2 q^2 e & -\varepsilon c_1 e^2 q^3 a_1^2 \\ b_1 & d_1 \end{pmatrix}$$
$$=: \beta \in G(q).$$

Note that

$$\beta^{-1} = \begin{pmatrix} d_1 & \varepsilon c_1 a_1^2 q^3 e^2 \\ -b_1 & 1 + \varepsilon a_1^2 q^2 e \end{pmatrix}.$$

Set

$$\theta := \begin{pmatrix} d_1 & -b_1 a_1^2 e^2 q^2 \\ \varepsilon c_1 q & 1 + \varepsilon a_1^2 q^2 e \end{pmatrix} = \begin{pmatrix} * & * \\ \varepsilon c_1 q & 1 + (a + vc_1)q^2 e \end{pmatrix}.$$

Then $\varphi := \beta^{-1}\theta \in X_5(q)$ and $\theta = \beta\varphi$.

Now

$$\theta(-\varepsilon evq)^{1,2}(-\varepsilon uq)^{2,1} = \begin{pmatrix} * & * \\ \varepsilon c_1 q & 1 + aq^2 e \end{pmatrix} (-\varepsilon uq)^{2,1}$$
$$= \begin{pmatrix} * & * \\ \varepsilon(c + u(1 + aeq^2))q & 1 + ae \end{pmatrix} (-\varepsilon u)^{2,1} = \begin{pmatrix} * & * \\ \varepsilon cq & 1 + aq^2 e \end{pmatrix},$$

so we can take $\delta_2 := (-\varepsilon evq)^{1,2}(-\varepsilon uq)^{2,1} \in X_2(q)$. $\square$

LEMMA 5.2 (reciprocity). *Let $a, b \in \mathbb{Z}$ and*

$$\alpha = \begin{pmatrix} 1 + aq^2 & (1 + bq^2)q \\ * & * \end{pmatrix} \in G(q).$$

Then there are $\varphi, \varphi' \in X_5(q)$ such that

$$q^{1,2}\alpha(-q)^{1,2}\varphi(-q)^{1,2}\varphi'(-q)^{1,2} = \begin{pmatrix} 1 + bq^2 & -(1 + aq^2)q \\ * & * \end{pmatrix}.$$

Proof. We have

$$\alpha' = \alpha(-q)^{1,2} = \begin{pmatrix} 1 + aq^2 & (b - a)q^3 \\ c & d \end{pmatrix} \in G(q).$$

Set $$\varphi := \alpha'^{-1} \begin{pmatrix} 1 + aq^2 & cq^2 \\ (b - a)q & d \end{pmatrix}^{-1} \in X_5(q);$$

hence $$\alpha'' = \alpha'\varphi = \begin{pmatrix} 1 + aq^2 & cq^2 \\ (b - a)q & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -cq^2 \\ -(b - a)q & 1 + aq^2 \end{pmatrix}.$$

Now $\quad q^{1,2}\alpha''(-q)^{1,2} = \begin{pmatrix} d' & c'q^2 \\ -(b-a)q & 1+bq^2 \end{pmatrix}.$

Set $$\varphi' := \begin{pmatrix} d' & c'q^2 \\ -(b-a)q & 1+bq^2 \end{pmatrix}^{-1} \begin{pmatrix} d' & -(b-a)q^3 \\ c' & 1+bq^2 \end{pmatrix}^{-1} \in X_5(q);$$

hence

$$\beta := q^{1,2}\alpha''(-q)^{1,2}\varphi' = \begin{pmatrix} d' & -(b-a)q^3 \\ c' & 1+bq^2 \end{pmatrix}^{-1} = \begin{pmatrix} 1+bq^2 & (b-a)q^3 \\ -c' & d' \end{pmatrix}.$$

Finally, $\quad \beta(-q)^{1,2} = \begin{pmatrix} 1+bq^2 & -(1+aq^2)q \\ * & * \end{pmatrix}.$ □

LEMMA 5.3. *Let* $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G(q)$ *. Then there are*

$$\theta \in X_4(q), \quad \delta_i \in \Delta_i(q\mathbb{Z}^i), \quad \gamma_1 \in \Gamma_1 q\mathbb{Z}, \quad \mu, \mu' \in Y_5(q), \quad \varepsilon = \pm 1$$

such that

$$(-q)^{2,1}\alpha^2\psi\delta_3\varphi\delta_2 q^{2,1}\psi q^{2,1}\mu'\gamma_1 = \begin{pmatrix} * & * \\ \varepsilon b^2 & a \end{pmatrix}.$$

Proof. Set $\theta = (\alpha^T\alpha)^{-1} \in X_4(q)$. Then

$$\alpha^2\theta = \alpha(\alpha^{-1})^T = \begin{pmatrix} 1+b(c-b) & a(b-c) \\ d(c-b) & 1-c(b-c) \end{pmatrix}.$$

By Lemma 5.1 with $e = (b-c)/q$, there are $\delta_i \in \Delta_i(q\mathbb{Z}^i)$, $\varepsilon \in \{1, -1\}$, and $\varphi \in X_5(q)$ such that

$$\alpha\psi\delta_3\varphi\delta_2 = \begin{pmatrix} * & * \\ \varepsilon aq & 1+b(c-b) \end{pmatrix} =: \beta.$$

Now we apply Lemma 5.2 to the matrix

$$(\beta^{-1})^T = \begin{pmatrix} 1+b(c-b) & -\varepsilon aq \\ * & * \end{pmatrix}$$

and find $\mu, \mu' \in Y_5(q)$ such that

$$\rho = (-q)^{2,1}\beta q^{2,1}\mu q^{2,1}\mu' q^{2,1} = \begin{pmatrix} * & * \\ -\varepsilon(1+b(c-b))q & a \end{pmatrix}.$$

Since $1+b(c-b) = ad-b^2$, we have

$$\rho(\varepsilon dq)^{2,1} = \rho\gamma_1 = \begin{pmatrix} * & * \\ \varepsilon b^2 & a \end{pmatrix}.$$ □

LEMMA 5.4. *Let*

$$a, c, e \in \mathbb{Z}, \quad e \neq 0, \quad \alpha = \begin{pmatrix} 1+aq^2e & cqe \\ * & * \end{pmatrix} \in G(q), \quad \varepsilon' \in \{\pm 1\}.$$

Then there are $\delta_i \in \Delta_i(q\mathbb{Z}^i)$ and $\varphi \in X_5(q)$ such that

$$\alpha\delta_5\varphi\delta_2 = \begin{pmatrix} * & * \\ \varepsilon' cq & 1 + aq^2 e \end{pmatrix}.$$

Proof. We find u, v as in the proof of Lemma 5.1. Now we find $w \in \mathbb{Z}$ such that $|c_2|$ is a prime $\equiv 1 \bmod 4$, where $c_2 := c_1 + (1 + \varepsilon a_1^2 q^2 e)w$. Then there are $z, a_2 \in \mathbb{Z}$ such that $\varepsilon a_1^2 + zc2 = \varepsilon' a_2^2$. We set

$$\delta_5 := (uqe)^{1,2}(vq)^{2,1}(wqe)^{1,2}(zq)^{2,1}(-c_2 eq)^{1,2} \in \Delta_5(q\mathbb{Z}^3).$$

Then

$$\alpha\delta_5 = \begin{pmatrix} 1 + \varepsilon' a_2^2 q^2 e & c_2 qe \\ * & * \end{pmatrix} (-c_3 eq)^{1,2} = \begin{pmatrix} 1 + \varepsilon' a_2^2 q^2 e & -\varepsilon' c_2 e^2 q^3 a_1^2 \\ b_1 & d_1 \end{pmatrix} \in G(q).$$

The rest of our proof is the same as that of Lemma 5.1. □

LEMMA 5.5. *Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G(q)$. Then there are $\delta_i \in \Delta_i(q\mathbb{Z}^i)$, $\gamma_3 \in \Gamma_3(q\mathbb{Z}^3)$, $\varphi \in X_5(q)$, $\theta \in X_4(q)$, and $\psi \in Y_5(q)$ such that*

$$\delta_1\theta\alpha^2\delta_5\varphi\delta_4\psi\gamma_3 = \begin{pmatrix} a^2 & \pm b \\ * & * \end{pmatrix}.$$

Proof. By Lemma 5.4 with $e = \varepsilon = 1$, we find

$$\rho = \delta_5\varphi\delta_2 \in \Delta_5(q\mathbb{Z}^5)X_5(q)\Delta_2(q\mathbb{Z}^2)$$

such that

$$\alpha\rho = \begin{pmatrix} * & * \\ b & a \end{pmatrix} = \begin{pmatrix} d' & c' \\ b & a \end{pmatrix}.$$

Set $\theta = (\alpha^{-1})^T\alpha^{-1} \in X_4(q)$. Then

$$\theta\alpha = (\alpha^{-1})^T = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

Set

$$\delta_1 = \begin{pmatrix} d' & c' \\ -b & a \end{pmatrix} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}^{-1} \in \Delta_1(q\mathbb{Z}).$$

Then

$$\delta_1\theta\alpha^2\rho = \begin{pmatrix} d' & -c' \\ -b & a \end{pmatrix} \begin{pmatrix} d' & c' \\ b & a \end{pmatrix} = \begin{pmatrix} * & * \\ b(a-d') & a^2 - bc' \end{pmatrix}$$
$$= \begin{pmatrix} d'' & c'' \\ b(a-d') & 1 + a(a-d') \end{pmatrix} =: \beta \in G(q)$$

because $ad' - bc' = 1$.

By Lemma 5.1,

$$(\beta^{-1})^T\delta_3\varphi'\delta_2' = \begin{pmatrix} * & * \\ \pm b & 1+a(a-d') \end{pmatrix}$$

with $\delta_i, \delta_i' \in \Delta_i(q\mathbb{Z}^i)$ and $\varphi' \in X_5(q)$; hence

$$\beta\gamma_3'\psi\gamma_2 = \begin{pmatrix} 1+a(a-d') & \pm b \\ * & * \end{pmatrix}\begin{pmatrix} a^2-bc' & \pm b \\ * & * \end{pmatrix}$$

with $\gamma_i, \gamma_i' \in \Gamma_i(q\mathbb{Z}^i)$ and $\psi \in Y_5(q)$.

Finally, we set $\delta_4 = \delta_2\gamma_3' \in \Delta_4(q\mathbb{Z}^4)$ and $\gamma_3 = \gamma_2(\pm c')^{2,1} \in \Gamma_3(q\mathbb{Z}^3)$ to obtain the conclusion. □

LEMMA 5.6. *Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G(q)$. Then there are $\delta_i \in \Delta_i(q\mathbb{Z}^i)$, $\gamma_1 \in \Gamma_1(q\mathbb{Z})$, $\varphi, \varphi' \in X_5(q)$, $\theta \in X_4(q)$, and $\psi \in Y_5(q)$ such that*

$$(-q)^{1,2}\alpha^2\theta\delta_3\varphi\delta_2\psi q^{1,2}\varphi'\gamma_1 = \begin{pmatrix} * & * \\ \pm b^2 q & a \end{pmatrix}.$$

Proof. Set $\theta = \alpha^{-1}(\alpha^{-1})^T \in X_4(q)$, so

$$\alpha\theta = (\alpha^{-1})^T = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}, \quad \alpha^2\theta = \alpha\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \begin{pmatrix} 1-b(b-c) & a(b-c) \\ * & * \end{pmatrix}.$$

By Lemma 5.1 with $e = (b-c)/q$, there are $\delta_i \in \Delta_i(q\mathbb{Z}^i)$ and $\varphi' \in X_5(q)$ such that

$$\alpha^2\theta\delta_3\varphi\delta_2 = \begin{pmatrix} * & * \\ \pm(1-b(b-c))q & a \end{pmatrix} =: \beta.$$

Now we apply Lemma 5.2 to the matrix $(\beta^T)^{-1} = \left(\begin{smallmatrix} 1-b(b-c) & \pm aq \\ * & * \end{smallmatrix}\right)$ instead of α. So

$$q^{1,2}(\beta^T)^{-1}\varphi(-q)^{1,2}\varphi'(-q)^{1,2} = \begin{pmatrix} a & \pm(1-b(b-c))q \\ * & * \end{pmatrix}, \quad \text{with } \varphi, \varphi' \in X_5(q);$$

hence

$$(-q)^{2,1}\beta q^{1,2}\psi q^{2,1}\psi' q^{2,1} = \begin{pmatrix} * & * \\ \pm(1-b(b-c))q & a \end{pmatrix} =: \beta', \quad \text{with } \psi, \psi' \in Y_5(q).$$

Since $(1-b(b-c)) = ad - b^2$, we have

$$\beta'\gamma_1' = \begin{pmatrix} * & * \\ \pm b^2 q & a \end{pmatrix} \quad \text{for } \gamma_1' = (\mp dq)^{2,1} \in \Gamma_1(q\mathbb{Z}).$$

Finally, we set $\gamma_1 := q^{2,1}\gamma_1' \in \Gamma(\mathbb{Z})$, $\delta_2 = \delta_2' q^{2,1}$. □

COROLLARY 5.7. *Let $\beta \in G(q)$. Then there are*

$$\delta_i \in \Delta_i(q\mathbb{Z}^i), \qquad \varphi, \varphi' \in X_5(q), \qquad \psi \in Y_5(q),$$
$$\gamma_i \in \Gamma_i(q\mathbb{Z}^i), \qquad \theta \in X_4(q), \qquad \alpha = \left(\begin{smallmatrix} a & bq \\ cq & d \end{smallmatrix}\right) \in G(q)$$

such that $\delta_2\beta\delta_2'\psi(-q)^{1,2}\varphi\gamma_2\varphi'\delta_3 = \alpha^2$, *where* $|b|$ *and* $|c|$ *are positive odd primes not dividing* q, *and* $\mathrm{GCD}(|b|-1, |c|-1) = 2$.

Proof. Let $\beta = \left(\begin{smallmatrix} a' & b'q \\ c'q & d' \end{smallmatrix}\right)$. The case $c' = 0$ is trivial, so we assume that $c' \neq 0$. We find $u, v, b \in \mathbb{Z}$ such that $a := d' + c'uq^2$ is an odd prime and $\pm b^2q^2 = c' + av$. Replacing, if necessary, b by $b + wa$, we can assume that b is a positive odd prime not dividing q.

Then

$$\beta' := \beta(uq)^{1,2}(vq)^{2,1} = \beta\delta_2' = \begin{pmatrix} * & * \\ \pm b^2q^3 & a \end{pmatrix}.$$

Now we find $c, d \in \mathbb{Z}$ such that $\alpha := \left(\begin{smallmatrix} a & bq \\ cq & d \end{smallmatrix}\right) \in G(q)$, c is a positive odd prime not dividing q, and $\mathrm{GCD}(b-1, c-1) = 2$.

By Lemma 5.6, we know there are $\delta_i \in \Delta_i(q\mathbb{Z}^i)$, $\gamma_1' \in \Gamma_1(q\mathbb{Z})$, $\varphi' \in X_5(q)$, $\theta' \in X_4(q)$, and $\psi' \in Y_5(q)$ such that

$$\alpha' := (-q)^{1,2}\alpha^2\theta\delta_3\varphi\delta_2\psi q^{1,2}\varphi'\gamma_1' = \begin{pmatrix} * & * \\ \pm b^2q^3 & a \end{pmatrix}.$$

Conjugating, if necessary, this equality by the matrix $\mathrm{diag}(-1, 1)$, which leaves invariant the sets $\Delta_i(q\mathbb{Z}^i)$, $\Gamma_i(q\mathbb{Z}^i)$, $X_5(q)$, $X_4(q)$, and $Y_5(q)$, we can assume that the matrices α' and β' have the same last row. Then $\gamma_1'' = \alpha'\beta'^{-1}$ belongs to $\Gamma_1(q\mathbb{Z})$, and $\gamma_1''\beta' = \alpha'$; hence

$$\gamma_1''\beta\delta_2 = \delta_1'\alpha^2\theta'\delta_3'\varphi'\delta_2'\gamma_3'\psi'\gamma_3'' = \begin{pmatrix} * & * \\ \pm b^2q & a \end{pmatrix}.$$

Now we set $\delta_2 := q^{1,2}\gamma_1''$, $\delta_2' = \delta_2''\gamma_1'^{-1}$, $\psi = \psi'^{-1}$, etc. □

LEMMA 5.8. *Let* $\alpha = \left(\begin{smallmatrix} a & b \\ * & * \end{smallmatrix}\right) \in G(q)$ *with* $m \geq 1$ *an integer. Then there are* $\delta_i \in \Delta_i(q\mathbb{Z}^i)$, $\gamma_6 \in \Gamma_6(q\mathbb{Z}^6)$, $\theta \in X_4(q)$, $\varphi, \varphi' \in X_5(q)$, *and* $\psi \in Y_5(q)$ *such that*

$$\delta_1\theta\alpha^{2m}\delta_5\varphi\delta_4\psi\gamma_6\varphi'\delta_3 = \begin{pmatrix} * & * \\ \pm b & a^{2m} \end{pmatrix}.$$

Proof. As in the proof of Lemma 1.2,

$$\beta := \alpha^m = f1_2 + g\alpha = \begin{pmatrix} f + ga & gb \\ * & * \end{pmatrix} \quad \text{and} \quad f^2 - 1 \in g\mathbb{Z}.$$

By Lemma 5.5, there are $\delta_i \in \Delta_i(q\mathbb{Z}^i)$, $\gamma_3 \in \Gamma_3(q\mathbb{Z}^3)$, and $\varphi \in X_5(q)$ such that

$$\delta_1\theta\beta^2\delta_5\varphi\delta_4\psi\gamma_3 =: \beta' = \begin{pmatrix} (f + ga)^2 & \pm gb \\ * & * \end{pmatrix}.$$

Now by Lemma 5.1 with $e = g$, there are $\delta_i, \delta'_i \in \Delta_i(q\mathbb{Z}^i)$ and $\varphi' \in X_5(q)$ such that

$$\beta'\delta'_3\varphi'\delta_2 =: \beta'' = \begin{pmatrix} * & * \\ \pm b & (f+ga)^2 \end{pmatrix}.$$

Since $(f+ga)^2 \equiv a^{2m} \bmod b$, we have

$$\beta''\delta'_1 = \begin{pmatrix} * & * \\ \pm b & a^{2m} \end{pmatrix} \quad \text{with } \delta'_1 \in \Delta_1(qbfZ).$$

Now we set $\gamma_6 := \gamma_3\delta'_3$ and $\delta_3 := \delta_2\delta'_1$ to finish our proof. □

PROPOSITION 5.9.

$$G(q) = C_6X_5D_4Y_5C_6X_5C_6X_4C_5Y_5C_4X_5D_6Y_5D_6X_4C_3X_5D_2X_5q^{1,2}Y_5C_2,$$

where $D_i = \Delta_i(q\mathbb{Z}^i),\ C_i = \Gamma_i(q\mathbb{Z}^i),\ X_5 = X_5(q),\ Y_5 = Y_5(q),\ X_4 = X_4(q).$

Proof. Let $\beta \in G(q)$. By Corollary 5.7,

$$\alpha^2 \in D_2\beta D_2Y_5(-q)^{1,2}X_5C_2X_5C_3$$

or (using that $D_{2i}^{-1} = C_{2i}$ and $D_{2i-1}^{-1} = D_{2i-1}$)

$$\beta \in C_2\alpha^2C_3X_5D_2X_5q^{1,2}Y_5C_2, \quad \text{with } \alpha = \begin{pmatrix} a & bq \\ cq & d \end{pmatrix},$$

primes $|b|, |c|$ not dividing q, and $\mathrm{GCD}(|b|-1, |c|-1) = 2$. We pick positive $m \in (|b|-1)\mathbb{Z}$ and $n \in (|c|-1)\mathbb{Z}$ such that $n - m = 1$. Then $a^{2m} \equiv 1 \bmod bq$, and $a^{2n} \equiv 1 \bmod cq$ and $n - m = 1$.

By Lemma 5.8,

$$\sigma_1 = \begin{pmatrix} * & * \\ \pm b & a^{2m} \end{pmatrix} \in D_1X_4\alpha^{2m}D_5X_5D_4Y_5C_6X_5D_3.$$

Since $a^{2m} \equiv 1 \bmod b$, we obtain easily that $\sigma_1 \in D_3$. So

$$\alpha^{2m} \in X_4D_1D_3D_3X_5D_6Y_5C_4X_5D_5 = X_4D_6X_5D_6Y_5C_4X_5D_5.$$

Hence $\qquad \alpha^{-2m} \in D_5X_5D_4Y_5C_6X_5C_6X_4.$

Similarly $\qquad (\alpha^T)^{2n} \in= X_4D_6X_5D_6Y_5C_4X_5D_5.$

Hence $\qquad \alpha^{2n} \in= C_5Y_5C_4X_5D_6Y_5D_6X_4.$

Therefore

$$\begin{aligned}\beta &\in C_2(\alpha^{-2m}\alpha^{2n})C_3X_5D_2X_5q^{1,2}Y_5C_2 \\ &\subset C_2(D_5X_5D_4Y_5C_6X_5C_6X_4)(C_5Y_5C_4X_5D_6Y_5D_6X_4)C_3X_5D_2X_5q^{1,2}Y_5C_2 \\ &= C_6X_5D_4Y_5C_6X_5C_6X_4C_5Y_5C_4X_5D_6Y_5D_6X_4C_3X_5D_2X_5q^{1,2}Y_5C_2.\end{aligned}$$

We used that $C_2D_5 = C_6$. □

Counting parameters yields the following result:

COROLLARY 5.10. *$G(q)$ is a polynomial family with* 93 *parameters. Also, there are polynomials $f_i \in \mathbb{Z}[y_1, \ldots, y_{93}]$ such that*

$$\alpha := \begin{pmatrix} 1+q^2 f_1 & q f_2 \\ q f_3 & 1+q^2 f_4 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}[y_1, \ldots, y_{93}]) \quad \textit{and} \quad \alpha(\mathbb{Z}^{93}) = G(q).$$

Now to prove Theorem 13. Consider an arbitrary principal congruence subgroup $\mathrm{SL}_2(q\mathbb{Z})$. The factor group $\mathrm{SL}_2(q\mathbb{Z})/\mathrm{SL}_2(q^2\mathbb{Z})$ is commutative, so it is easy to see that it is generated by the images of $G(q)$ and $1^{2,1}\Delta_1(q\mathbb{Z})(-1)^{2,1}$. Using Corollary 5.11, we conclude that $\mathrm{SL}_2(q\mathbb{Z})$ is a polynomial family with 94 parameters. More precisely:

COROLLARY 5.11. *$\mathrm{SL}_2(q\mathbb{Z})$ is a polynomial family which has* 94 *parameters. Moreover, there are polynomial $f_i \in \mathbb{Z}[y_1, \ldots, y_{94}]$ such that*

$$\alpha := \begin{pmatrix} 1+q f_1 & q f_2 \\ q f_3 & 1+q f_4 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}[y_1, \ldots, y_{94}]) \quad \textit{and} \quad \alpha(\mathbb{Z}^{94}) = \mathrm{SL}_2(q\mathbb{Z}).$$

Example 5.12. Let H be the subgroup of $\mathrm{SL}_2\,\mathbb{Z}$ in Example 14. The group $G(2)$ is a normal subgroup of index 4 in H. The group H is generated by $G(2)$ together with the subgroup $(-1)^{2,1}\Delta_1(\mathbb{Z})1^{2,1}$. So H is a polynomial family with 94 parameters.

PROPOSITION 5.13. *Every polynomial family $H \subset \mathbb{Z}^k$ has the "strong approximation" property that if $t \in \mathbb{Z}$ with $t \geq 2$, $p_1^{s(1)}, \ldots, p_t^{s(t)}$ are powers of distinct primes p_i, and $h_i \in H$ for $i = 1, \ldots, t$, then there is an $h \in H$ such that $h \equiv h_i \bmod p_i^{s(i)}$ for $i = 1, \ldots, t$.*

Proof. Suppose $H = \alpha(\mathbb{Z}^N)$ with $\alpha \in \mathbb{Z}[y_1, \ldots, y_N]$.

Let $t \in \mathbb{Z}$ with $t \geq 2$, let $p_1^{s(1)}, \ldots, p_t^{s(t)}$ be powers of distinct primes p_i, and let $h_i \in H$ for $i = 1, \ldots, t$.

We have $h_i = \alpha(u^{(i)})$ for $i = 1, \ldots, t$ with $u^{(i)} \in \mathbb{Z}^N$. By the Chinese Remainder Theorem, there is a $u \in \mathbb{Z}^N$ such that $u \equiv u^{(i)} \bmod p_i^{s(i)}$ for $i = 1, \ldots, t$.

Set $h = \alpha(u)$. Then $h \equiv h_i \bmod p_i^{s(i)}$ for $i = 1, \ldots, t$. □

COROLLARY 5.14. *Let H be a subgroup of $\mathrm{SL}_2\,\mathbb{Z}$ generated by $\mathrm{SL}_2(6\mathbb{Z})$ and the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then H is not a polynomial family.*

Proof. We do not have the strong approximation property for H. Namely, take $t = 2$, $p_1 = 2$, $p_2 = 3$, and $s(1) = s(2) = 1$. The image of H in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ is a cyclic group of order 2, and the image of H in $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is a cyclic group of order 4. The strong approximation for H (see Proposition 5.13) would imply that the order of the image of H in $\mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z})$ is at least 8, while the image is in fact a cyclic group of order 4. □

COROLLARY 5.15. *Let $X \subset \mathbb{Z}$ be an infinite set of positive primes. Then X is not a polynomial family.*

Proof. Suppose X is a polynomial family. Let p_1 and p_2 be distinct primes in X. By Proposition 5.13, there is a $z \in X$ such that $z \equiv p_1 \bmod p_1$ and $z \equiv p_2 \bmod p_2$. Then z is divisible by both p_1 and p_2 and hence is not prime. This contradiction shows that X is not a polynomial family. □

Remark 5. By [12, Part VIII, Prob. 97], no nonconstant integer-valued polynomial with rational coefficients takes only prime values. This fact implies easily Corollary 5.15. Two easy solutions to the problem are given, and the result is attributed by Euler to Goldbach.

References

[1] H. BASS, K-theory and stable algebra, *Inst. Hautes Études Sci. Publ. Math.* (1964), 5–60. MR 30 #4805 Zbl 0248.18025

[2] H. BASS, J. MILNOR, and J.-P. SERRE, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), *Inst. Hautes Études Sci. Publ. Math.* (1967), 59–137. MR 39 #5574 Zbl 0174.05203

[3] F. BEUKERS, The Diophantine equation $Ax^p + By^q = Cz^r$, *Duke Math. J.* **91** (1998), 61–88. MR 99f:11039 Zbl 1038.11505

[4] D. CARTER and G. KELLER, Elementary expressions for unimodular matrices, *Comm. Algebra* **12** (1984), 379–389. MR 86a:11023 Zbl 0572.20030

[5] H. DARMON and A. GRANVILLE, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* **27** (1995), 513–543. MR 96e:11042 Zbl 0838.11023

[6] S. FRISCH, Remarks on polynomial parametrization of sets of integer points, *Comm. Algebra* **36** (2008), 1110–1114. MR 2140698 Zbl pre05293057

[7] R. GAR-EL and L. N. VASERSTEIN, On the Diophantine equation $a^3 + b^3 + c^3 + d^3 = 0$, *J. Number Theory* **94** (2002), 219–223. MR 2003d:11039 Zbl 1031.11015

[8] R. K. GUY, Conference problems session conducted by J. L. Selfridge, in *Number Theory* (Ottawa, 1996) (R. GUPTA and K. S. WILLIAMS, eds.), CRM *Proc. Lecture Notes* **19**, AMS, Providence, RI, 1999, pp. 385–390. MR 1684618 Zbl 0936.11003

[9] Y. MATIYASEVICH, Hilbert's tenth problem: What was done and what is to be done, in *Hilbert's Tenth Problem*: *Relations with Arithmetic and Algebraic Geometry* (Ghent, 1999) (J. DENEF, L. LIPSHITZ, T. PHEIDAS, and J. VAN GEEL, eds.), *Contemp. Math.* **270**, Amer. Math. Soc., Providence, RI, 2000, pp. 1–47. MR 2001m:03084 Zbl 0994.03002

[10] J. L. MENNICKE, Finite factor groups of the unimodular group, *Ann. of Math.* **81** (1965), 31–37. MR 30 #2083 Zbl 0135.06504

[11] G. PAYNE and L. VASERSTEIN, Sums of three cubes, in *The Arithmetic of Function Fields* (Columbus, OH, 1991) (D. GOSS, D. R. HAYES, and M. I. ROSEN, eds.), *Ohio State Univ. Math. Res. Inst. Publ.* **2**, de Gruyter, Berlin, 1992, pp. 443–454. MR 93k:11090 Zbl 0799.11039

[12] G. PÓLYA and G. SZEGŐ, *Problems and Theorems in Analysis*, II: *Theory of Functions*, *Zeros*, *Polynomials*, *Determinants*, *Number Theory*, *Geometry*, *Grundl. Math. Wissen.* **216**, Springer-Verlag, New York, 1976. MR 53 #2 Zbl 0311.00002

[13] J.-P. SERRE, On a functorial property of power residue symbols: Correction to [2], *Inst. Hautes Études Sci. Publ. Math.* **44** (1974), 241–244. MR 50 #12972

[14] T. SKOLEM, *Diophantische Gleichungen*, *Ergeb. Math. Grenzgeb.* **4**, Springer-Verlag, New York, 1938. Zbl 0018.29302 JFM 64.0112.02

[15] A. A. SUSLIN, The structure of the special linear group over rings of polynomials, *Izv. Akad. Nauk* SSSR *Ser. Mat.* **41** (1977), 235–252, 477, In Russian; translated in *Math.* USSR-*Izv.* **11** (1977), 221–238. MR 57 #12482 Zbl 0378.13002

[16] L. N. VASERSTEIN, K_1-theory and the congruence problem, *Mat. Z.* **5** (1969), 233–244, In Russian; translated in *J. Math. Notes* **5** (1969), 141–148. MR 40 #210

[17] ———, Stabilization of unitary and orthogonal groups over a ring with involution, *Mat. Sb.* **81 (123)** (1970), 328–351, In Russian; translated in *Math.* USSR *Sb.* **10** (1970), 307–326. MR 42 #4617 Zbl 0253.20066

[18] ———, The group SL_2 over Dedekind rings of arithmetic type, *Mat. Sb.* **89(131)** (1972), 313–322, 351, In Russian; translated in *Math.* USSR *Sb.* **18** (1973), 321–332. MR 55 #8253 Zbl 0359.20027

[19] ———, Bass's first stable range condition, *J. Pure Appl. Algebra* **34** (1984), 319–330. MR 86c:18009 Zbl 0547.16017

[20] ———, Normal subgroups of orthogonal groups over commutative rings, *Amer. J. Math.* **110** (1988), 955–973. MR 89i:20071 Zbl 0654.20052

[21] L. N. VASERSTEIN and A. A. SUSLIN, Serre's problem on projective modules over polynomial rings, and algebraic K-theory, *Izv. Akad. Nauk* SSSR *Ser. Mat.* **40** (1976), 993–1054, 1199, In Russian; translated in *Math.* USSR *Izv.* **10** (1978), 937–1001. MR 56 #5560 Zbl 0338.13015

[22] U. ZANNIER, Remarks on a question of Skolem about the integer solutions of $x_1x_2 - x_3x_4 = 1$, *Acta Arith.* **78** (1996), 153–164. MR 97h:11035 Zbl 0867.11013

(Received January 16, 2006)
(Revised October 13, 2006)

E-mail address: vstein@math.psu.edu
DEPARTMENT OF MATHEMATICS, PENN STATE UNIVERSITY, UNIVERSITY PARK, PA 16802-6401, UNITED STATES