A Counting Formula for Primitive Tetrahedra in $\mathbf{Z}^3$

Mizan R. Khan

1. INTRODUCTION. A *primitive polytope* is a polytope in n-dimensional Euclidean space $\mathbf{R}^n$ whose vertices are (integer) lattice points (points of $\mathbf{Z}^n$) but it does not contain any other lattice points in its interior or on its boundary. Pick's theorem coupled with the fact that any primitive (convex) polygon has at most 4 vertices (by Theorem 2.1) allows us to infer that a convex polygon in $\mathbf{Z}^2$ is primitive if and only if it is a triangle of area $\frac{1}{2}$ or a parallelogram of area 1. In $\mathbf{Z}^3$ matters are very different. Specifically, there is no bound on the volume of a primitive tetrahedron (see Section 3); but there is an elegant characterization of primitive tetrahedra that was discovered more than 30 years ago. This characterization gives us a simple formula that counts the number of equivalence classes of primitive tetrahedra of a given volume. The goal of this paper is to state and prove this formula.

We begin by defining the terms *lattice polytope*, *vertex*, and *primitive*.

Definition 1.1. A *lattice polytope* is the closed convex hull in $\mathbf{R}^n$ of a finite set $\{u_1, \dots, u_m\}$ of points of $\mathbf{Z}^n$, i.e., it is the set

$$\{t_1 u_1 + \cdots + t_m u_m : u_1, \dots, u_m \in \mathbf{Z}^n, 0 \le t_1, \dots, t_m \le 1, t_1 + \cdots + t_m = 1\}.$$

A *vertex* of a polytope is a point of the polytope that cannot be written as a convex combination of other points of the polytope.

Remark. The lattice polytopes we consider always have *non-zero volume*.

Definition 1.2. A lattice polytope in $\mathbf{R}^n$ is *primitive* if the only lattice points it contains are its vertices.

Reeve ([**8**] and [**9**]) and Reznick [**10**] use the term *fundamental* instead of primitive; Scarf [**13**] uses the term *integral polyhedron*. Our preference for using the adjective *primitive* instead of *fundamental* or *integral* stems from the usage in [**14**]. The interested reader should look at [**14**, pp. 98–99] for a discussion of primitive sets of vectors and the connection with constructing a reduced basis of a lattice.

Section 2 is a brief discussion of primitivity in $\mathbf{Z}^n$. We explain why a primitive polytope in $\mathbf{Z}^n$ has no more than 2^n vertices and why a primitive parallelepiped in $\mathbf{Z}^n$ has unit volume. Section 3 is a comparison of primitive triangles in $\mathbf{Z}^2$ with primitive tetrahedra in $\mathbf{Z}^3$. The goals of this section are to explain why there is no bound on the volume of primitive tetrahedra and to present a geometric characterization of primitive tetrahedra. In Section 4 we discuss unimodular maps and state an analytic version of the geometric characterization. Section 5 is where we discuss a formula that counts the number of equivalence classes of primitive tetrahedra for a fixed volume; the equivalence relation is defined via unimodular maps. The formula is in Theorem 5.3 and is proved with the aid of Burnside's lemma. The final section describes Howe's generalization of Theorem 4.2, which describes all primitive polyhedra, not just primitive tetrahedra. Except for the results in Section 2, we confine our remarks to dimension 3 because the characterizations of primitive tetrahedra do not extend to higher dimensions.

To conserve space we typically write lattice points as row vectors, but in our matrix calculations we view lattice points as column vectors.

2. PRIMITIVITY IN $\mathbf{Z}^n$. We begin by showing that the number of vertices of a primitive polytope is bounded, a result that appears as Theorem 1.2 in [**13**].

Theorem 2.1. *A primitive polytope in* $\mathbf{R}^n$ *has at most* 2^n *vertices.*

Proof: If there are more than 2^n vertices in a lattice polytope P, then there are two vertices $v = (v_1, v_2, \dots, v_n)$, $w = (w_1, w_2, \dots, w_n)$ such that $v_i \equiv w_i \pmod 2$, $i = 1, \dots, n$. The lattice point $(v + w)/2$ belongs to P, so P is not primitive. ∎

We now discuss lattice *parallelepipeds* in $\mathbf{R}^n$. We like to think of the lattice points in a lattice parallelepiped as the cosets of a quotient group. Suppose P is the parallelepiped $P = \{u + t_1 v_1 + t_2 v_2 + \cdots + t_n v_n\colon\ u, v_1, v_2, \dots, v_n \in \mathbf{Z}^n,\ 0 \le t_1, t_2, \dots, t_n \le 1\}$. We can consider the sublattice $(\mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \cdots \oplus \mathbf{Z}v_n)$ and view the lattice points in P as the cosets of the quotient group $\mathbf{Z}^n/(\mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \cdots \oplus \mathbf{Z}v_n)$. We have found the following result very useful.

Theorem 2.2. *Let $v_1, \dots, v_n$ be a set of linearly independent points of $\mathbf{Z}^n$. Then the quotient group $\mathbf{Z}^n/(\mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \cdots \oplus \mathbf{Z}v_n)$ has order $|\det A|$, where A is the $n \times n$ matrix whose k-th column is v_k, i.e., the order equals the volume of the parallelepiped spanned by $v_1, v_2, \dots, v_n$.*

For a proof see [**14**, Theorem 20, p. 49]. Let us illustrate Theorem 2.2 and the remarks preceding it by examining the parallelogram P in $\mathbf{Z}^2$ whose vertices are $(0,0)$, $(1,3)$, $(2,2)$, and (3.5).

The area of P equals 4. Therefore the quotient group $\mathbf{Z}^2/(\mathbf{Z}(1,3) \oplus \mathbf{Z}(2,2))$ has order 4.

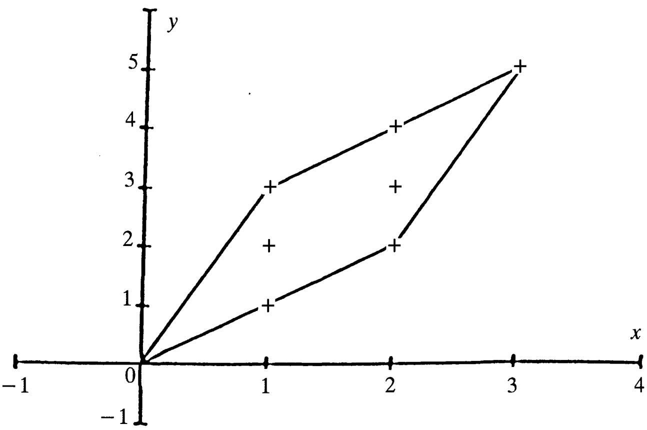

Figure 1. The parallelogram with vertices $(0,0)$, $(1,3)$, $(2,2)$, and $(3,5)$.

The 8 lattice points in P represent the cosets of $\mathbf{Z}^2/(\mathbf{Z}(1,3) \oplus \mathbf{Z}(2,2))$ in the following way: the zero coset can be represented by any one of the 4 vertices; the lattice points $(1,1)$ and $(2,4)$ represent the same coset (this coset is its own inverse); the lattice points $(1,2)$ and $(2,3)$ represent distinct cosets with one being the inverse of the other. Clearly, the quotient group is isomorphic to $\mathbf{Z}/4\mathbf{Z}$.

From Theorem 2.2 and our observation about viewing lattice points as cosets, we can easily prove the following theorem about parallelepipeds in $\mathbf{Z}^n$.

Theorem 2.3. *The parallelepiped* $P = \{u + t_1v_1 + t_2v_2 + \cdots + t_nv_n\colon u, v_1, v_2, \ldots, v_n \in \mathbf{Z}^n, 0 \le t_1, t_2, \ldots, t_n \le 1\}$ *is primitive if and only if volume*$(P) = 1$

3. PRIMITIVE TRIANGLES vs. PRIMITIVE TETRAHEDRA. We now compare primitive triangles in $\mathbf{Z}^2$ with primitive tetrahedra in $\mathbf{Z}^3$. Any primitive triangle in $\mathbf{Z}^2$ has area $\frac{1}{2}$. This is the simplest case of Pick's theorem.

Theorem 3.1 [Pick [7]]. *Let P be a lattice polygon in $\mathbf{Z}^2$. If there are I lattice points in the interior of P and B lattice points on the boundary of P, then area*$(P) = I + \frac{1}{2}B - 1$.

We refer the reader to **[1]** for two elementary and elegant proofs of Theorem 3.1; **[2]** and **[3]** are two recent expositions on Pick's theorem in the MONTHLY.

Reeve **[8]** observed that the tetrahedron with vertices $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, and $(1,1,c)$ is primitive for any non-zero integer c. Consequently, there is no bound on the volume of a primitive tetrahedron and a direct generalization of Pick's theorem to $\mathbf{R}^3$ is impossible. However, by replacing $\mathbf{Z}^3$ with the *fractional* lattice $\frac{1}{n}\mathbf{Z}^3$ for a fixed positive integer n, he was able to find a three-dimensional analogue of Pick's theorem; we do not pursue this direction. In addition to **[8]** and **[9]**, the interested reader should look at **[6]**, where Reeve's theorem is extended to higher dimensions. Other related references are listed on the first page of **[2]**.

Another way to show that primitive triangles in $\mathbf{Z}^2$ have area equal to $\frac{1}{2}$ is to use Theorem 2.3. It is instructive to see how the argument proceeds and why it cannot be extended to give an upper bound on the volume of primitive tetrahedra.

Suppose $T = \{u + t_1v_1 + t_2v_2\colon u, v_1, v_2 \in \mathbf{Z}^2, 0 \le t_1, t_2 \le 1, t_1 + t_2 \le 1\}$ is a lattice point triangle containing the lattice point w. Let x be the coset of $\mathbf{Z}^2/(\mathbf{Z}v_1 \oplus \mathbf{Z}v_2)$ that w represents. *There is at least one lattice point in the triangle* $\{u + t_1v_1 + t_2v_2\colon u, v_1, v_2 \in \mathbf{Z}^2, 0 \le t_1, t_2 \le 1, t_1 + t_2 \ge 1\}$ *that represents the inverse* $-x$. It follows that T is primitive if and only if the associated parallelogram $P = \{u + t_1v_1 + t_2v_2\colon u, v_1, v_2 \in \mathbf{Z}^2, 0 \le t_1, t_2 \le 1\}$ is primitive. Using Theorem 2.3 we conclude that T is primitive if and only if *area*$(T) = \frac{1}{2}$.

Now let T_1 be the tetrahedron

$$T_1 = \{u + t_1v_1 + t_2v_2 + t_3v_3\colon u, v_1, v_2, v_3 \in \mathbf{Z}^3, 0 \le t_1, t_2, t_3 \le 1, t_1 + t_2 + t_3 \le 1\}.$$

The preceding argument shows that T_1 is primitive if and only if the tetrahedron

$$T_2 = \{u + t_1v_1 + t_2v_2 + t_3v_3\colon u, v_1, v_2, v_3 \in \mathbf{Z}^3, \\ 0 \le t_1, t_2, t_3 \le 1, 2 \le t_1 + t_2 + t_3 \le 3\}$$

is primitive. But we cannot conclude that the parallelepiped

$$P = \{u + t_1v_1 + t_2v_2 + t_3v_3\colon u, v_1, v_2, v_3 \in \mathbf{Z}^3, 0 \le t_1, t_2, t_3 \le 1\}$$

is primitive since, in addition to T_1 and T_2, there are four other tetrahedra inside P that need not be primitive. Therefore, we cannot find a bound for the volume of P and use it to give a bound on the volume of T_1.

Recall that the volume of any lattice point tetrahedron is $c/6$, where c is a positive integer. Suppose

$$T_1 = \{u + t_1v_1 + t_2v_2 + t_3v_3 \colon u, v_1, v_2, v_3 \in \mathbf{Z}^3, 0 \le t_1, t_2, t_3 \le 1, t_1 + t_2 + t_3 \le 1\}$$

is a primitive tetrahedron and $vol(T_1) = c/6$ with $c \ge 2$. The parallelepiped

$$P = \{u + t_1v_1 + t_2v_2 + t_3v_3 \colon u, v_1, v_2, v_3 \in \mathbf{Z}^3, 0 \le t_1, t_2, t_3 \le 1\}$$

has volume c. By Theorem 2.2 there are $c - 1$ non-zero cosets in the quotient group $\mathbf{Z}^3/(\mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \mathbf{Z}v_3)$. *It now follows that there are $c - 1$ lattice points in the interior of P and each one represents a distinct coset of $\mathbf{Z}^3/(\mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \mathbf{Z}v_3)$.* This assertion is based on the following two observations:

1. A coset has a unique representative in P if and only if the representative lies in the interior of P.
2. There are no lattice points on the boundary of P other than the vertices. Suppose $w = u + t_1v_1 + t_2v_2 + t_3v_3$ is a lattice point lying on the boundary of P that is not a vertex of P. There are two possible cases. Case 1: Exactly 1 member of the set $\{t_1, t_2, t_3\}$, say t_3, is an integer. In this case, either the lattice point $u + t_1v_1 + t_2v_2$, or the lattice point $u + (1 - t_1)v_1 + (1 - t_2)v_2$ lies on one of the faces of T_1. Since $t_1, t_2 \notin \mathbf{Z}$, neither lattice point is a vertex of P. Case 2: Exactly 2 members of the set $\{t_1, t_2, t_3\}$, say t_2 and t_3, are integers. In this case, the lattice point $u + t_1v_1$ lies on one of edges of T_1. Since $t_1 \notin \mathbf{Z}$, $u + t_1v_1$ is not a vertex of T_1. Therefore, if P contains a lattice point on its boundary that is not a vertex, then T_1 is not primitive.

Thus there are $c - 1$ lattice points in the interior of P. How are these $c - 1$ lattice points arranged inside P? The answer to this question gives us a geometric characterization of primitive tetrahedra in $\mathbf{Z}^3$.

Theorem 3.2. *Consider the tetrahedron*

$$T = \{u + t_1v_1 + t_2v_2 + t_3v_3 \colon u, v_1, v_2, v_3 \in \mathbf{Z}^3, 0 \le t_1, t_2, t_3 \le 1, t_1 + t_2 + t_3 \le 1\}$$

and the parallelepiped

$$P = \{u + t_1v_1 + t_2v_2 + t_3v_3 \colon u, v_1, v_2, v_3 \in \mathbf{Z}^3, 0 \le t_1, t_2, t_3 \le 1\}.$$

Then T is primitive if and only if all the non-vertex lattice points in P lie in the interior of one of the three diagonal parallelograms of P that do not intersect the interior of T, i.e., one of the parallelograms with vertices $\{u + v_1, u + v_2, u + v_1 + v_3, u + v_2 + v_3\}$, $\{u + v_2, u + v_3, u + v_2 + v_1, u + v_3 + v_1\}$, or $\{u + v_3, u + v_1, u + v_3 + v_2, u + v_1 + v_2\}$.

The sufficiency of the stated criterion is trivial and all the work lies in proving its necessity. We have been unable to construct a direct geometric proof and we pose this as a problem to our readers. We prove Theorem 3.2 by proving an analytic version, Theorem 4.2.

4. UNIMODULAR MAPS.

Before we can describe an analytic version of Theorem 3.2, we need to define the concept of a unimodular map.

Definition 4.1. The map $f\colon\mathbf{R}^n \to \mathbf{R}^n$ is a *unimodular map* if (i) f is affine, (ii) f preserves volume, and (iii) f maps points in $\mathbf{Z}^n$ to points in $\mathbf{Z}^n$.

We leave it to the reader to check the following properties of unimodular maps.

Theorem 4.1. *Let $f: \mathbf{R}^n \to \mathbf{R}^n$ be a map and let P be a lattice polytope in $\mathbf{Z}^n$.*

(i) *f is unimodular if and only if $f(u) = Mu + v$, where $M \in GL_n(\mathbf{Z})$, i.e., M is a $n \times n$ matrix with integer entries and* $\det(M) = \pm 1$, *and $v \in \mathbf{Z}^n$.*
(ii) *If f is unimodular, then f is invertible and f^{-1} is unimodular.*
(iii) *If f is unimodular then $f(P)$ and $f^{-1}(P)$ are lattice polytopes. Furthermore, f maps interior points of P to interior points of $f(P)$, boundary points of P to boundary points of $f(P)$, and vertices of P to vertices of $f(P)$.*
(iv) *If P is primitive, then both $f(P)$ and $f^{-1}(P)$ are primitive.*

Unimodular maps define an equivalence relation on the set of lattice polytopes and so we can consider equivalence classes of lattice polytopes.

Definition 4.2. Two lattice polytopes P_1, P_2 in $\mathbf{R}^n$ are *unimodularly equivalent* if there is a unimodular map $f:\mathbf{R}^n \to \mathbf{R}^n$ such that f maps P_1 to P_2. If P_1, P_2 are unimodularly equivalent we write $P_1 \cong P_2$.

Any two primitive triangles in $\mathbf{Z}^2$ are unimodularly equivalent. One way to prove this is to apply Theorem 2.2. Suppose the triangles

$$T_1 = \{u_1 + t_1 v_1 + t_2 v_2 : u_1, v_1, v_2 \in \mathbf{Z}^2, 0 \le t_1, t_2 \le 1, t_1 + t_2 \le 1\}$$

and

$$T_2 = \{u_2 + t_1 w_1 + t_2 w_2 : u_2, w_1, w_2 \in \mathbf{Z}^2, 0 \le t_1, t_2 \le 1, t_1 + t_2 \le 1\}$$

are primitive. Then the associated parallelograms

$$P_1 = \{u_1 + t_1 v_1 + t_2 v_2 : u_1, v_1, v_2 \in \mathbf{Z}^2, 0 \le t_1, t_2 \le 1\}$$

and

$$P_2 = \{u_2 + t_1 w_1 + t_2 w_2 : u_2, w_1, w_2 \in \mathbf{Z}^2, 0 \le t_1, t_2 \le 1\}$$

are primitive. Let A be the 2×2 matrix whose first column is v_1 and whose second column is v_2; and let B be the 2×2 matrix whose first column is w_1 and whose second column is w_2. Since P_1 and P_2 are primitive parallelograms, $A, B \in GL_2(\mathbf{Z})$. The unimodular map $f(x) = BA^{-1}x + (u_2 - BA^{-1}u_1)$ maps T_1 to T_2 (and P_1 to P_2). This argument can be used to show that any two primitive parallelepipeds in $\mathbf{Z}^n$ are unimodularly equivalent.

We now describe an analytic version of Theorem 3.2, which appears as Corollary 5.7 in [**10**]. From here on, $T_{a,b,c}$ denotes the tetrahedron with vertices $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, and (a,b,c), with $(a,b,c) \in \mathbf{Z}^3$ and $c \neq 0$.

Theorem 4.2 [Reeve-White-Howe-Scarf-Reznick]. *A tetrahedron T is primitive if and only if $T \cong T_{0,0,1}$ or $T \cong T_{1,b,c}$ with $1 \le b < c$ and* $\gcd(b, c) = 1$.

We refer the reader to [**10**] for a proof of Theorem 4.2, and to [**11**] and [**13**] for proofs of variants of it. It is surprising that such an elegant and simple theorem is not better known.

5. THE COUNTING FORMULA. Unimodular maps preserve volume; consequently, the number of distinct (unimodular) equivalence classes of primitive tetrahedra is infinite. We are led to consider the following question.

For a given positive integer c, is there a counting formula for the number of distinct (unimodular) equivalence classes of primitive tetrahedra of volume $c/6$? The answer lies in determining the relationship between the integers x and b when $T_{1,b,c} \cong T_{1,x,c}$. The relationship is described in the following variant of Theorem 5.6 in **[10]**.

Theorem 5.1. *Let* $b, b^{-1}, c, x \in \mathbf{Z}$ *with* $1 \le x, b, b^{-1} < c$, $\gcd(b,c) = \gcd(x,c) = 1$, *and* $bb^{-1} \equiv 1 (\mathrm{mod}\, c)$. *The primitive tetrahedra* $T_{1,b,c}$ *and* $T_{1,x,c}$ *are unimodularly equivalent if and only if* $x \in \{b, c-b, b^{-1}, c-b^{-1}\}$.

Proof: ($\Rightarrow$) We can view a unimodular map from $T_{1,b,c}$ to $T_{1,x,c}$ as a map between the vertices of $T_{1,b,c}$ and $T_{1,x,c}$. There are 24 possible maps. An examination of each of these shows that $x \in \{b, c-b, b^{-1}, c-b^{-1}\}$.

For example, suppose we look at the unimodular map

$$(0,0,0) \mapsto (0,1,0),\ (1,0,0) \mapsto (1,x,c),\ (0,1,0) \mapsto (0,0,0),\ (1,b,c) \mapsto (1,0,0).$$

This map has the form

$$\begin{pmatrix} 1 & 0 & 0 \\ x-1 & -1 & a \\ c & 0 & -1 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

with the conditions that $a \in \mathbf{Z}$ and $x - b + ac = 0$. Since $|x - b| < c$, it follows that $a = 0$ and therefore $x = b$.

($\Leftarrow$) $T_{1,b,c} \cong T_{1,c-b,c}$ via the unimodular map

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

$T_{1,b,c} \cong T_{1,b^{-1},c}$ via the unimodular map

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & b^{-1} & \dfrac{1 - bb^{-1}}{c} \\ 0 & c & -b \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

and $T_{1,b,c} \cong T_{1,c-b^{-1},c}$ via the unimodular map

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & c - b^{-1} & -\dfrac{b(c - b^{-1}) + 1}{c} \\ 0 & c & -b \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}. \qquad \blacksquare$$

Before proceeding to the statement of the counting formula, it is instructive to determine the number of equivalence classes of primitive tetrahedra of volume $c/6$ for some specific values of c. We do so for $c = 13$ and $c = 14$. We start with the case $c = 13$. Because of Theorem 4.2 we need consider only the 12 primitive tetrahedra $T_{1,1,13}, T_{1,2,13}, T_{1,3,13}, \ldots, T_{1,12,13}$ and determine which are unimodularly equivalent. Theorem 5.1 ensures that $T_{1,1,13}, \cong T_{1,12,13}$, $T_{1,2,13} \cong T_{1,6,13} \cong T_{1,7,13} \cong T_{1,11,13}$, $T_{1,3,13} \cong T_{1,4,13} \cong T_{1,9,13} \cong T_{1,10,13}$, and $T_{1,5,13} \cong T_{1,8,13}$, so there are 4 equivalence classes of primitive tetrahedra of volume $13/6$. For $c = 14$, we need to consider only the 6 primitive tetrahedra $T_{1,1,14}$, $T_{1,3,14}$, $T_{1,5,14}$, $T_{1,9,14}$,

$T_{1,11,14}$, and $T_{1,13,14}$. Since $T_{1,1,14} \cong T_{1,13,14}$ and $T_{1,3,14} \cong T_{1,5,14} \cong T_{1,9,14} \cong T_{1,11,14}$, there are 2 equivalent classes of primitive tetrahedra of volume $14/6$.

We now prove the counting formula by combining Theorem 5.1 with Burnside's lemma.

Theorem 5.2 (Burnside's lemma). *Let a finite group G act on a finite set X and have N orbits. Then*

$$N = \frac{1}{|G|} \sum_{g \in G} |X_g|,$$

where $X_g = \{x\colon g(x) = x,\ x \in X\}$, i.e., X_g is the set of fixed points of g.

See [**12**, Theorem 2.71, p. 125] for a proof, as well as an explanation of why it is referred to by some as *not-Burnside's* lemma.

We are now ready to state and prove the counting formula.

Theorem 5.3. *Suppose n is an integer greater than 2, $T(n)$ is the number of distinct equivalence classes of primitive tetrahedra of volume $n/6$, $f(x) \in (\mathbf{Z}/n\mathbf{Z})[x]$, and $N(f(x) \equiv 0 \pmod n)$ denotes the number of solutions of the congruence $f(x) \equiv 0 \pmod n$ in $\mathbf{Z}/n\mathbf{Z}$. Then*

$$T(n) = \frac{\phi(n) + N\big(x^2 - 1 \equiv 0 \pmod n\big) + N\big(x^2 + 1 \equiv 0 \pmod n\big)}{4}.$$

In particular, if n is a prime p, then

$$T(p) = \left[\frac{p}{4}\right] + 1 = \begin{cases} \dfrac{p+3}{4} & \text{if } p \equiv 1 \pmod 4 \\[2ex] \dfrac{p+1}{4} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof: Let $U = \{x\colon 1 \le x < n,\ \gcd(x,n) = 1\}$ be the set of units of $\mathbf{Z}/n\mathbf{Z}$ and let $G = \{g_1, g_2, g_3, g_4\}$ be the group of bijections of U, where $g_1(x) = x$, $g_2(x) = n - x$, $g_3(x) = x^{-1}$, and $g_4(x) = n - x^{-1}$ for any element $x \in U$. The cardinality of U is $\phi(n)$, the Euler phi function evaluated at n, and $G \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Theorem 5.2 says that $T(n)$ equals the number of orbits of U under the action of G. Let $U_i = \{x\colon g_i(x) = x,\ x \in U\}$, $i = 1,2,3,4$. Since g_1 is the identity it fixes all of U. When $n > 2$, g_2 has no fixed points. The fixed points of g_3 are the solutions of the congruence $x^2 \equiv 1 \pmod n$ and the fixed points of g_4 are the solutions of the congruence $x^2 \equiv -1 \pmod n$. Thus,

$$|U_1| = \phi(n),\ |U_2| = 0,\ |U_3| = N\big(x^2 - 1 \equiv 0 \pmod n\big),$$
$$|U_4| = N\big(x^2 + 1 \equiv 0 \pmod n\big).$$

We now apply Burnside's lemma to obtain the formula

$$T(n) = \frac{\phi(n) + N\big(x^2 - 1 \equiv 0 \pmod n\big) + N\big(x^2 + 1 \equiv 0 \pmod n\big)}{4}. \qquad \blacksquare$$

Theorem 4.2 shows that if T is a primitive tetrahedron of volume $1/6$ then $T \cong T_{0,0,1}$, and if T is a primitive tetrahedron of volume $1/3$ then $T \cong T_{1,1,2}$; so in the exceptional cases when $n = 1,2$ we have $T(n) = 1$. The reader can observe that $\phi(n)$, $N(x^2 - 1 \equiv 0 \pmod n)$, and $N(x^2 + 1 \equiv 0 \pmod n)$ are multiplicative functions of n. We now cite a result from the theory of quadratic residues that gives a formula for $N(x^2 - 1 \equiv 0 \pmod n)$ and $N(x^2 + 1 \equiv 0 \pmod n)$.

Theorem 5.4. *Let $n = 2^k m$, with $n \geq 2$ and $\gcd(m, 2) = 1$. If $m > 1$, let the prime divisors of m be $p_1, \ldots, p_t$; otherwise set $t = 0$. Then*

$$N(x^2 - 1 \equiv 0 \pmod n) = \begin{cases} 2^t & \text{if } k = 0, 1 \\ 2^{t+1} & \text{if } k = 2 \\ 2^{t+2} & \text{if } k \geq 3, \end{cases}$$

and

$$N(x^2 + 1 \equiv 0 \pmod n)$$
$$= \begin{cases} 2^t \text{ if } k \leq 1 \text{ and } p_i \equiv 1 \pmod 4 \text{ for any } i \in \{1, \ldots, t\} \\ 0 \text{ if } k \geq 2 \text{ or there exists an } i \in \{1, \ldots, t\} \text{ such that } p_i \equiv 3 \pmod 4. \end{cases}$$

See [**5**, Chapter 2, Section 8; Chapter 3, Section 5] for a proof.

6. HOWE'S THEOREM.

We now describe Howe's theorem on primitive polyhedra. Theorem 2.1 shows that any primitive polyhedron in $\mathbf{R}^3$ has at most 8 vertices. Howe proved that any primitive polyhedron with eight vertices is, up to a unimodular map, the convex hull of a square and a parallelogram.

Theorem 6.1 [Howe]. *Let P be a primitive polyhedron with eight vertices. Then there is a unimodular map that maps P to the polyhedron whose vertices are $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(0,1,1)$, $(1,a,b)$, $(1,c,d)$, and $(1, a+c, b+d)$ with $a, b, c, d, \in \mathbf{Z}$, $a, b, c, d \geq 0$ and $ad - bc = 1$. Furthermore, any primitive polyhedron with fewer than eight vertices can be embedded in one with eight vertices.*

We refer the reader to the article by Scarf [**13**] for a proof of this theorem. It should be noted that the four vertices $(0,0,0)$, $(0,1,0)$, $(0,0,1)$, and $(0,1,1)$ lie on the plane $x = 0$ and form a square of area 1. The other four vertices $(1,0,0)$, $(1,a,b)$, $(1,c,d)$, and $(1, a+c, b+d)$ lie on the parallel plane $x = 1$ and form a parallelogram of area 1.

The problem of characterizing primitive tetrahedra was independently studied in 1957 by Reeve [**8**] and in 1964 by White [**15**]; Theorem 4.2 arises from combining their results. In 1977, Howe independently discovered Theorem 4.2 and its generalization, Theorem 6.1. He did not publish his work and it was Scarf [**13**] who first publicized Howe's theorem. Over the years, other mathematicians have rediscovered Theorem 4.2. For example, Therese Hart, Karen Rogers, and I discovered it in 1991 and wrote up our results in the unpublished manuscript [**4**]. We then came across Reznick's [**10**] article where we learnt of the work of Reeve, White, and others. The contents of [**4**] are included in Chapter 2 of K. Rogers' doctoral dissertation [**11**]. The last chapter of this dissertation contains some partial results on primitive simplices in $\mathbf{Z}^4$.

We leave the reader with the following question: Are there analogues of the counting formula for primitive polyhedra with 5, 6, 7, and 8 vertices?

ACKNOWLEDGMENTS. I am grateful to K. Rogers for showing me her proof of Theorem 4.2 and some of the unimodular equivalences of $T_{a,b,c}$. The use of Burnside's lemma to prove the counting formula was suggested by a referee and is an undoubted improvement on my initial proof. The referees and my friend Sergio Alvarez made extensive suggestions on improving the exposition.

REFERENCES

1. D. DeTemple, Pick's formula: a retrospective, *Mathematics Notes from Washington State University*, Vol. 32, Nos.3-4 (November, 1989).
2. R. Diaz and S. Robins, Pick's formula via the Weierstrass $\wp$-function, *Amer. Math. Monthly* **102** (1995) 431–437.
3. B. Grunbaum and G. C. Shephard, Pick's theorem, *Amer. Math. Monthly* **100** (1993) 150–161.
4. T. Hart, M. Khan, and K. Rogers, Primitive tetrahedra in $\mathbf{Z}^3$ (unpublished manuscript).
5. Hua Loo Keng, *Introduction to Number Theory*, translated from the Chinese by P. Shiu, Springer-Verlag, 1982.
6. I. G. MacDonald, The volume of a lattice polyhedron, *Proc. Camb. Phil. Soc.* **59** (1963) 719–726.
7. G. Pick, Geometrisches zur Zahlenlehre, *Sitzungber. Lotos* (Prague) **19** (1899) 311–319.
8. J. E. Reeve, On the volume of lattice polyhedra, *Proc. London Math. Soc.* (3) **7** (1957) 378–395.
9. J. E. Reeve, A further note on the volume of lattice polyhedra, *J. London Math. Soc.* **34** (1959) 57–62.
10. B. Reznick, Lattice point simplices, *Discrete Mathematics* **60** (1986) 219–242.
11. K. M. Rogers, Primitive simplices in $\mathbf{Z}^3$ and $\mathbf{Z}^4$ (Ph.D. dissertation), Columbia University, 1993.
12. J. Rotman, *A first course in abstract algebra*, Prentice-Hall, 1996.
13. H. E. Scarf, Integral polyhedra in three space, *Math. Oper. Res.* **10** (1985) 403–438.
14. C. L. Siegel, *Lectures on the Geometry of Numbers*; notes by B. Friedman; rewritten by K. Chandrasekharan with the assistance of R. Suter, Springer-Verlag, 1989.
15. G. K. White, Lattice tetrahedra, *Canad. J. Math.* **16** (1964) 389–396.

MIZAN R. KHAN received his B.Sc. and M.Sc. in Mathematics from the London School of Economics under the tutelage of Haya Freedman. He received his Ph.D. from the University of Massachusetts, Amherst, where he wrote a dissertation in computational number theory under the direction of David Hayes. Before coming to Eastern Connecticut State University, he held visiting positions at Mt. Holyoke College and Trinity College.
Department of Mathematics and Computer Science, Eastern Connecticut State University, Willimantic, CT 06226
khanm@ecsuc.ctstateu.edu