Volumes of spheres and geometric number theory

The attached sheets, taken from the book [1] (a library reference book), illustrate how one can get some very famous and very beautiful results in number theory from not much more than the volume of the 4-dimensional sphere, a little algebra and geometric reasoning. Here is some extra background information to make reading the document easier. I'll assume you're acquainted with some basic notions from linear algebra and group theory, but ask me if you're nor sure of something.

Lattices

DEFINITION 1 : Let $B = \{v_1, ..., v_n\}$ be a basis for $\mathbf{R}^n$. The n-dimensional *lattice with basis B* is the subset L_B of $\mathbf{R}^n$ consisting of all linear combinations

$$\sum_{i=1}^{n} n_i v_i, \tag{1}$$

where each n_i is an integer (positive or negative).

DEFINITION 2 : The subset F of $\mathbf{R}^n$ is called a *fundamental domain* for the lattice L_B if, for every $x \in \mathbf{R}^n$, there exists a unique $l \in L_B$ such that $x - l \in F$.

The *standard* fundamental domain for the lattics L_B in Definition 1 is the set of all vectors

$$F_0 = \left\{ \sum_{i=1}^{n} c_i v_i : 0 \leq c_i < 1 \text{ for all } i \right\}. \tag{2}$$

Clearly, F_0 IS a fundamental domain. This f.d. is commonly denoted by $\mathbf{R}^n/L$ and is called an n-dimensional *torus.* Note that the volume of F_0 is the determinant of the $n \times n$ matrix with $v_1, ..., v_n$ as its' columns. Note also that any translate of a fundamental domain is a fundamental domain.

Multiplicative group mod p

Let p be a prime. Let $G = \{1, 2, ..., p - 1\}$. These numbers can be multiplied modulo p and since p is prime the product of any two is never zero (mod p). Also, it follows from the Euclidean algorithm that each number has a *multiplicative inverse*, i.e.: for each $r \in G$ there exists $s \in G$ such that $rs \equiv 1 \bmod p$. Hence G is a group under multiplication. Note that G has $p-1$ elements - we say that G has *order* $p-1$ and write $|G| = p-1$. It can be proven that G is a *cyclic* group, that is there exists $g \in G$ such that $G = \{g, g^2, g^3, ..., g^{p-1} = 1\}$. We say that the element g has *order* $p-1$ and write $o(g) = p-1$. In general, the order of an element $x \in G$ is the least $n > 0$ such that $x^n = 1$. A theorem in group theory called *Lagrange's theorem* implies that the order of each element divides the group order. For an element $x \in G$, the subset $S_x = \{x, x^2, ..., x^{o(x)}\}$ of G is closed under multiplication and is thus called a *subgroup* of G. Lagrange's theorem implies that $|S_x|$ divides $|G|$. The integer $\frac{|G|}{|S_x|}$ is called the *index* of S_x in G.

Reference

[1] I. Stewart and D. Tall, Algebraic Number Theory, Chapman and Hall (1979).