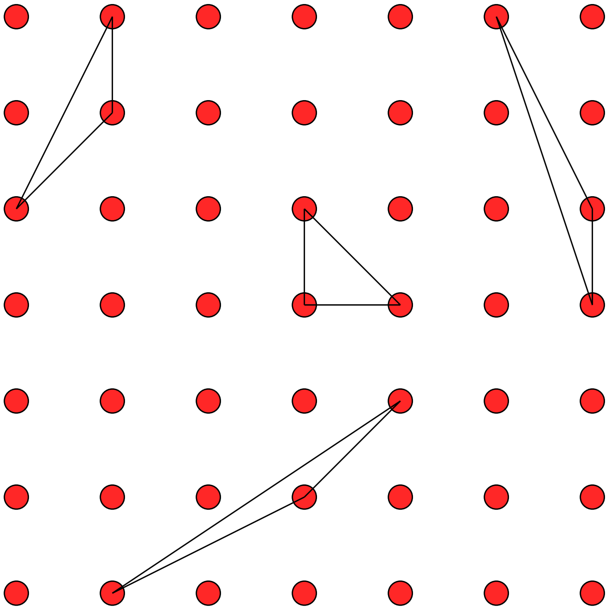
Geometry of Numbers

prepared by Oleg Ivrii

Integral Triangles

An integral triangle (a triangle in the plane whose vertices have integer coordinates) is called *simple* if it contains no integral points in the interior or on its sides. The "Geometry of Numbers" is a theory built around the following fact: *every simple triangle has area 1/2.* Equivalently, a *simple parallelogram has area 1.*



1. Prove the statement just made. *Hint:* consider a large circle and notice that the number of parallelograms is about equal to the number of integral points.

2. The boundary of an integral triangle does not contain integral points (excluding the vertices) and there is exactly one integral point in the interior. Show that this point is the centroid.

3. An integral polygon has i integral points in the interior and b on the boundary. Prove Pick's formula: the area of the polygon is $A = i + \frac{b}{2} - 1$.

4. A king walks on an 8 × 8 chessboard: starting from one square, visiting each square exactly once and returning to the starting square. The path traced out by the king's movement is a non-intersecting loop (every move, a king walks in a straight line from the center of one square to the center of another). Find the area enclosed within the loop.

5. If P is a polygon, let kP be the polygon obtained from P by dilation with coefficient k from the origin. Also, let $A(P)$ denote the area of polygon P and $n(P)$ denote the number of integral points lying inside P or on the boundary of P.

   (a) Prove $2A(P) = n(2P) - 2n(P) + 1$.

   $*$ (b) Find an analogous formula for polyhedra in $\mathbb{R}^3$.

6. The *Farey sequence* $\mathfrak{F}_n$ is the sequence of fractions (written in lowest terms) between 0 and 1 which have denominators not exceeding n. For example $\mathfrak{F}_5$ is

$$\frac{0}{1}, \quad \frac{1}{5}, \quad \frac{1}{4}, \quad \frac{1}{3}, \quad \frac{2}{5}, \quad \frac{1}{2}, \quad \frac{3}{5}, \quad \frac{2}{3}, \quad \frac{3}{4}, \quad \frac{4}{5}, \quad \frac{1}{1}.$$

   Show that if $\frac{p_1}{q_1}, \frac{p_2}{q_2}$ are two consecutive fractions then $|p_1q_2 - q_1p_2| = 1$.

   Hint: To the Farey fraction h/k, assign the point (h, k) in the plane. Also observe that the area of the triangle with vertices $(0, 0), (p_1, q_1)$ and (p_2, q_2) is $\frac{1}{2}|p_1q_2 - q_1p_2|$.

7. Given two fractions $\frac{a}{b}, \frac{c}{d}$, their *mediant* is the fraction $\frac{a+c}{b+d}$. Given three consecutive Farey fractions $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}$, show that $\frac{p_2}{q_2}$ is the mediant of $\frac{p_1}{q_1}$ and $\frac{p_3}{q_3}$.

8. Another interpretation of Farey fractions due to Ford: given a Farey fraction $\frac{h}{k}$ draw a circle with center $(\frac{h}{k}, \frac{1}{2k^2})$. Show that two Ford circles are either tangent or do not intersect while Ford circles of neighbouring Farey fractions must be tangent to each other.

Convex Figures

9. Given two convex domains $A, B \subset \mathbb{R}^2$, we can form their *Minkowski sum* $A+B$ which consists of all points in the plane which can be represented as $a+b$ with $a \in A$ and $b \in B$. Show that the sum of two convex domains is again convex.

10. Suppose $X \subset \mathbb{R}^2$ has area greater than 1, show that it intersects one of its integral translates.

11. Prove this result due to Minkowski: Suppose $X \subset \mathbb{R}^2$ is a convex figure containing and symmetric with respect to the origin and area greater than 4. Show that it contains other integral points.

$*$ 12. An orchard is in a shape of a circle has radius $50m$. The gardener stands in the center, which also happens to be the origin. Trees grow at integral points and have some thickness. Can the gardener see some boundary point of the orchard if

   (a) the width of the trees are $\frac{1}{50}$?

   (b) what about $\frac{1}{\sqrt{2501}}$?

13. Given a polynomial $F(x_1, x_2, \ldots x_n) = \sum_\alpha C_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, we define its *Newton polygon* $\mathfrak{D}_F$ to be the convex hull of the points $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for which coefficient $C_\alpha \neq 0$. Show that $\mathfrak{D}_{FG} = \mathfrak{D}_F + \mathfrak{D}_G$ (here we are using Minkowski sum).

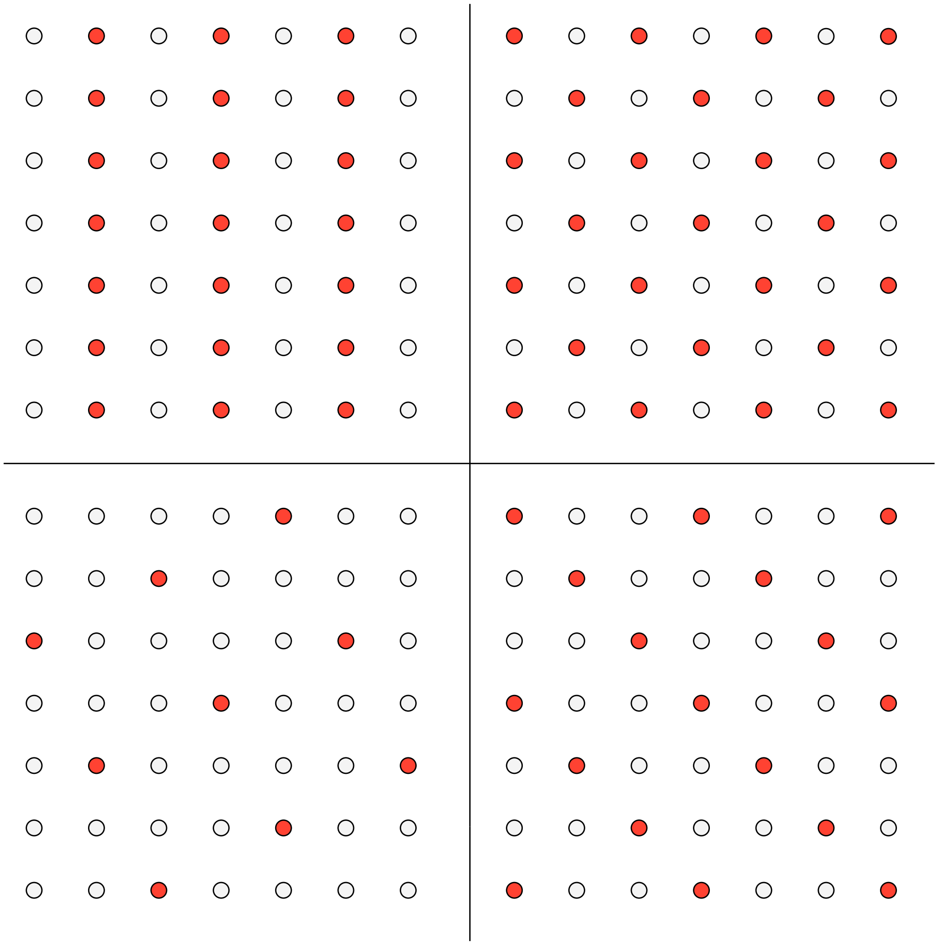
14. (a) For a polynomial $F(x_1, x_2, \ldots x_n) = \sum_\alpha C_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ with integer coefficients, we define its *content* $c(F)$ to be the greatest common divisor of the coefficients. Show that $c(F)c(G) = c(FG)$.

   Hint: Assume $c(F) = c(G) = 1$. You want to show that $c(FG) = 1$ as well. If $c(FG) \neq 1$, then some prime divides all coefficients of FG. Look at the Newton polygon of FG modulo that prime.

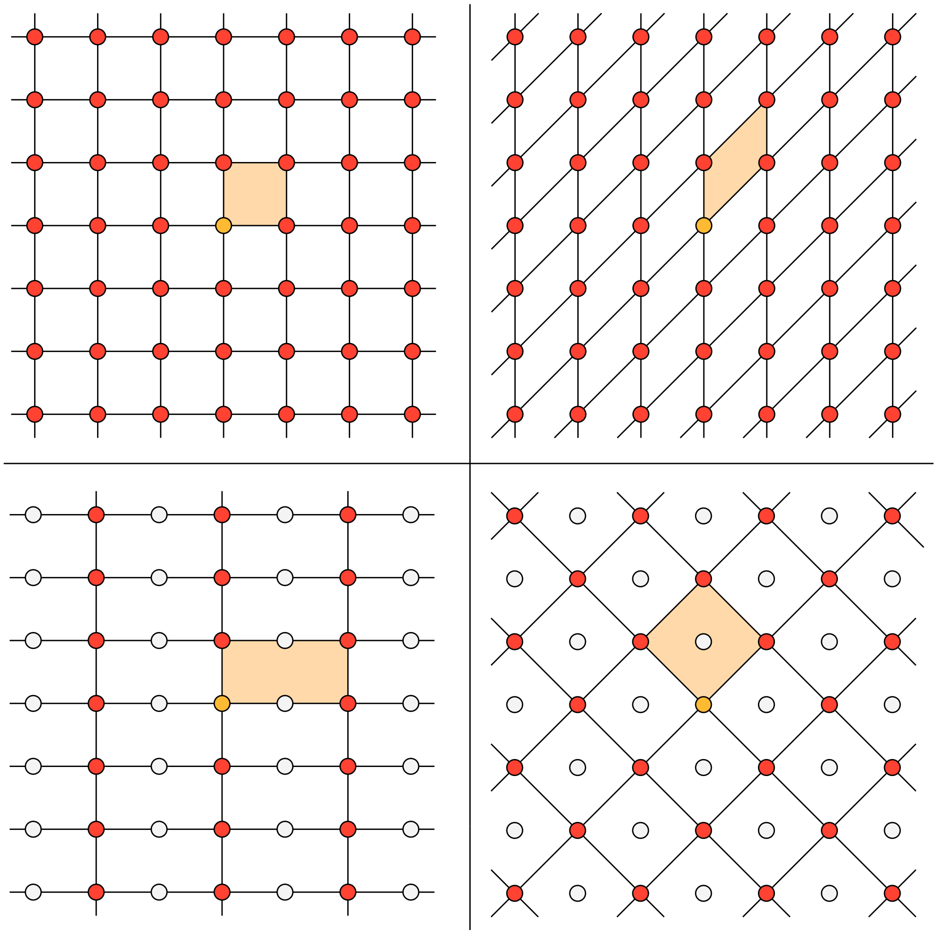
   (b) Prove *Gauss' Lemma*: Suppose a polynomial $F(x_1, x_2, \ldots x_n)$ with integer coefficients factors can be expressed as a product of two polynomials with rational coefficients. Then it call be refactored into two polynomials with integer coefficients.

Lattices

A lattice $\mathscr{L}$ may be described as a set of points "equally spaced in two directions" (below are four examples). We have previously worked with the lattice $\mathscr{I}$ containing all integral points, but results are general to arbitrary lattices. It is easily shown that all $\mathscr{L}$-simple parallelograms have the same area, which we denote $[\mathscr{L} : \mathscr{I}]$ and say that the lattice $\mathscr{L}$ bloats the integral lattice $[\mathscr{L} : \mathscr{I}]$ times. In the examples, this number $[\mathscr{L} : \mathscr{I}]$ is 2, 2, 5 and 3 respectively. Of course, $[\mathscr{I} : \mathscr{I}] = 1$.



A way to visualize a lattice is by "assigning a basis", that is calling a specific $\mathscr{L}$-simple parallelogram *fundamental*.



The number $[\mathscr{L} : \mathscr{I}]$ of course represents the number of integral points inside the fundamental parallelogram (provided we do not count the integral points lying on the top and right sides to avoid double-counting).

If $\mathscr{L} \supset \mathscr{M} \supset \mathscr{N}$ are three lattices then clearly $[\mathscr{N} : \mathscr{L}] = [\mathscr{N} : \mathscr{M}][\mathscr{M} : \mathscr{L}]$ (think about what this means).

Formally, a lattice $\mathscr{L}$ is given by two linearly independent vectors $(p_1, q_1), (p_2, q_2)$ – the sides of the fundamental parallelogram – called the *generators*. In this case, $\mathscr{L}$ is precisely the set of points $k_1(p_1, q_1) + k_2(p_2, q_2)$ where k_1, k_2 span over the integers. For instance, the lattice $\mathscr{I}$ can be spanned by vectors $(0, 1), (1, 0)$ or by the pair $(1, 1), (0, 1)$.

Gauss' Lemma

A very interesting result due to Gauss says that a prime number of type $4k+1$ can be written as the sum of two squares (of course primes of type $4k+3$ cannot be written as a sum of two squares).

15. A number y is a *quadratic residue* modulo n if there is an integer x for which $x^2 \equiv y \mod n$. If you want, you can take these results for granted, they can be found in any elementary text on number theory:

   (a) The number -1 is a quadratic residue modulo a prime p if and only if it is of type $4k+1$ (that is $x^2 = -1$ can be solved modulo p).

   $*$ (b) The number -2 is a quadratic residue modulo a prime p if and only if it is of type $8k+1, 8k+3$.

$*$ 16. Let $\mathscr{M}$ be the lattice generated by the vectors $(0,p), (p,0)$ and $\mathscr{L}$ be the set of points $y \equiv tx$ where $t^2 \equiv -1 \mod p$. Denote the point of $\mathscr{L}$ lying in the first quadrant (i.e with $x \geq 0, y \geq 0$) closest to the origin by $P(x,y)$.

   (a) Show that the point $Q(-y,x)$ also belongs to $\mathscr{L}$.

   (b) Show that $\mathscr{L}$ is a lattice. Conclude that $[\mathscr{M} : \mathscr{L}] = p$.

   (c) Show that the triangle POQ is an $\mathscr{L}$-simple right-angled triangle.

   (d) Prove Gauss Lemma by calculating the area of POQ in two different ways.

17. (a) A prime number p of type $8k+1, 8k+3$ can be represented in a unique way as a sum $a^2 + 2b^2$ (clearly if p is of the form, it must be either $8k+1, 8k+3$).

   (b) Classify the primes which can be represented by the quadratic form $a^2 + kb^2$.

18. It is easy to see that $x^2 \equiv 2 \pmod 7$ has two solutions. Show that they can be extended to solve $x^2 \equiv 2 \pmod{7^k}$ for any k.

19. Let m be an odd positive integer. Show that there exists integers a, b such that $a^2 + b^2 \equiv -1 \pmod m$.

   Hint: First prove when $m = p$ is an odd prime by pigeon-hole, then extend to $m = p^k$ prime powers by induction and $m = \prod_i p_i^{k_i}$ by the Chinese remainder theorem.

20. Let $\mathscr{L}$ be a lattice in $\mathbb{R}^4$ generated by vectors $a_1 = (m, 0, 0, 0)$, $a_2 = (0, m, 0, 0)$, $a_3 = (a, b, 1, 0)$, $a_4 = (b, -a, 0, 1)$ where m is a given integer and a, b are numbers constructed in problem 19.

    (a) The fundamental parallelepiped of $\mathscr{L}$ has volume m^2.

    (b) The length of every vector in $\mathscr{L}$ is divisible by m.

    (c) The volume of a ball in $\mathbb{R}^4$ of radius r is $\frac{\pi^2 r^4}{2}$.

    (d) Apply the 4-dimensional version of Minkowski's theorem (problem 11) to the ball centered at the origin and radius $\sqrt{2m} - \epsilon$ to show that m can be written as the sum of 4 squares.

Waring's Problem

Problem 20 shows that every number is the sum of 4 squares. In 1770, Waring asked the following question: is every number the sum of some fixed number of cubes? forth-powers? arbitrary n-th powers? The answer to these questions turns out to be yes. In 1908, Hurwitz suggested that Waring's problem can be solved by means of polynomial identities (see problem 21 for examples). A year later, Hilbert had completed the Hurwitz programme by showing that they exist.

21. (a) Using the fact that every number is the sum of 4 squares and the *Lagrange identity* (check it)

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2 = \frac{1}{6} \sum_{1 \le i < j \le 4} \{(x_i + x_j)^4 + (x_i - x_j)^4\}$$

    prove that every number is the sum of at most $53 = 48 + 5$ fourth powers (hint: express $n = 6m + r$, $0 \le r \le 5$).

    (b) Prove analogous result for sixth powers using *Fleck formula*:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)^3 = \frac{1}{60} \sum_{i<j<k} (x_i \pm x_j \pm x_k)^6 + \frac{1}{30} \sum_{i<j} (x_i \pm x_j)^6 + \frac{3}{5} \sum_i x_i^6.$$

    ($\pm$ means that we have a term with "+" and a similar term with "−")

(c) Prove analogous result for eighth powers using *Hurwitz formula*:

$$(x_1^2+x_2^2+x_3^2+x_4^2)^4 = \frac{1}{840}(x_1 \pm x_2 \pm x_3 \pm x_4)^8 + \frac{1}{5040}\sum_{i<j<k}(2x_i \pm x_j \pm x_k)^8$$
$$+\frac{1}{84}\sum_{i<j}(x_i \pm x_j)^8 + \frac{1}{840}\sum_{i}(2x_i)^6.$$

A more elementary solution given by Linnik using the notion of Schnirel'man density.

22. Given two sets A, B of natural numbers containing 0, we can take their sumset $A+B$ to be the set of numbers which can be represented as $a+b$ with $a \in A$, $b \in B$. For a set A, we can define its *counting function* $A(n)$ which measures the number of elements of A between 1 and n. We define the *Schnirel'man density* σ_A to be $\inf_{n>0} \frac{A(n)}{n}$.

    Notice that if a set has Schnirel'man density 1, it must contain all natural numbers. Also, if a set does not contain 1, it has Schnirel'man density 0.

    (a) Suppose that $\sigma_A + \sigma_B \geq 1$. Show that $A + B = \mathbb{N}$.

    (b) Show that $\sigma_{A+B} \geq \sigma_A + \sigma_B - \sigma_A\sigma_B$.

    Remark: In fact it turns out that $\sigma_{A+B} \geq \min(1, \sigma_A + \sigma_B)$, but this is much harder to prove.