9/4/2026

The law of quadratic reciprocity

Thm (Quadratic reciprocity) Let p, q be distinct primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Equivalently,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

unless $p, q \equiv 3 \pmod 4$, in which case

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Eg. (1) $p = 3$, $q = \overset{1 \pmod 4}{13}$: $\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$.

(2) $p = 3$, $q = \overset{3 \pmod 4}{7}$: $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$.

Lattice point counting.

What is an integer lattice in $\mathbb{R}^2$?

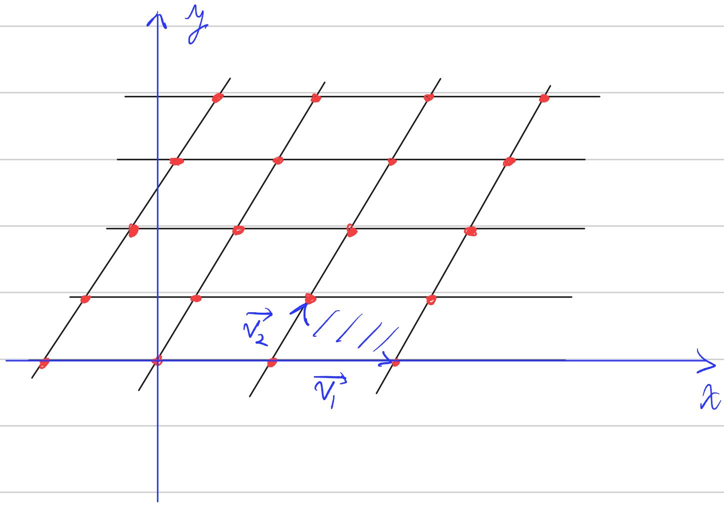
Algebraically, it is a set of the form

$$L = \{ x\vec{v_1} + y\vec{v_2} : x, y \in \mathbb{Z} \},$$

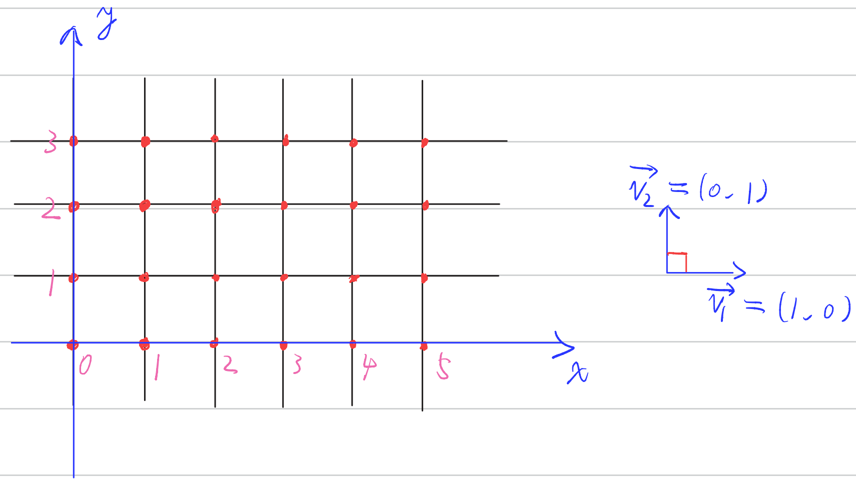
where $\vec{v_1}, \vec{v_2} \in \mathbb{R}^2$ are linearly independent vectors, so that

$$\mathbb{R}^2 = \{ x\vec{v_1} + y\vec{v_2} : x, y \in \mathbb{R} \}.$$

Geometrically, it consists of points on a grid formed by infinitely many identical parallelograms.

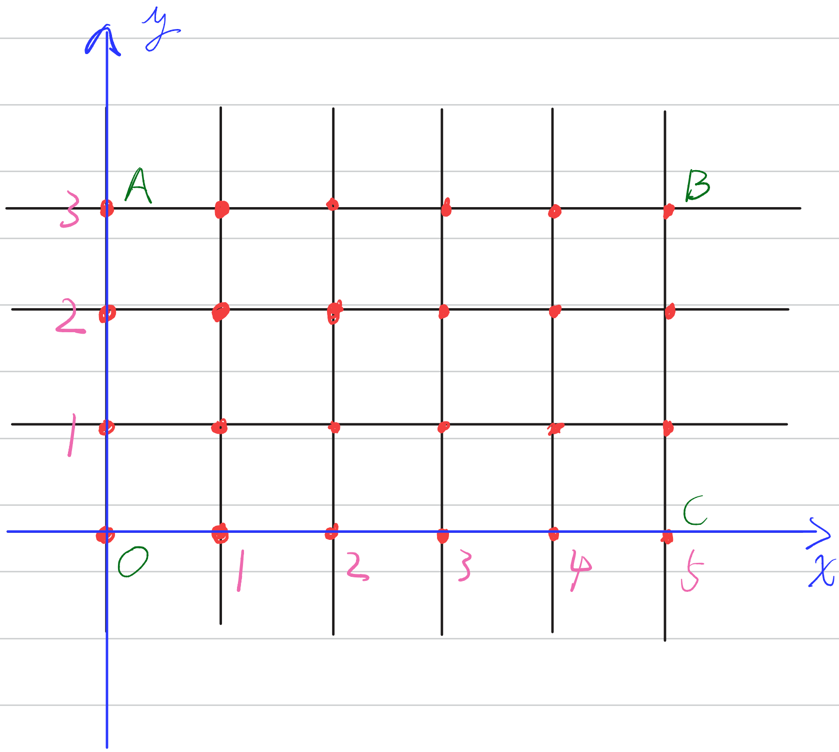


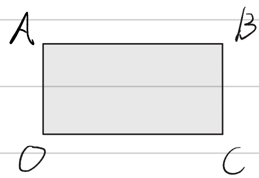
We will work with the square grid!



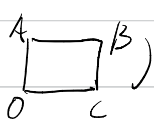
How to count lattice points?

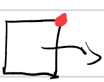
1. Lattice points in a rectangle



Q1: How many lattice points in 

, including points on AB, BC but not those on OC, OA?

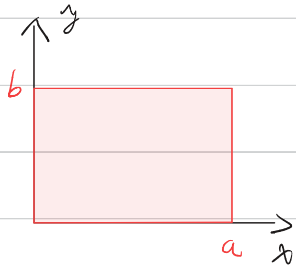
A: $15 = 5 \cdot 3 =$ Area(

) : • $\rightleftarrows$  → Area 1

Let a, b be positive integers.

Number of lattice points

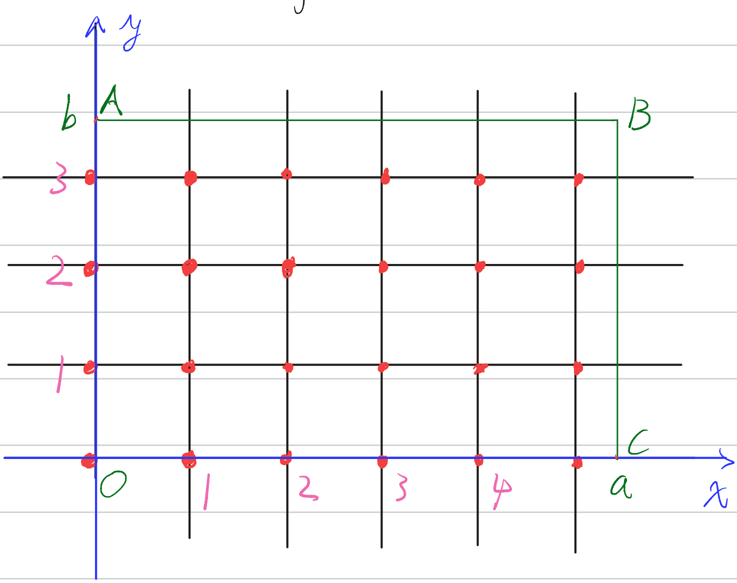
in



$= \text{Area} = ab.$

excluding those on the axies

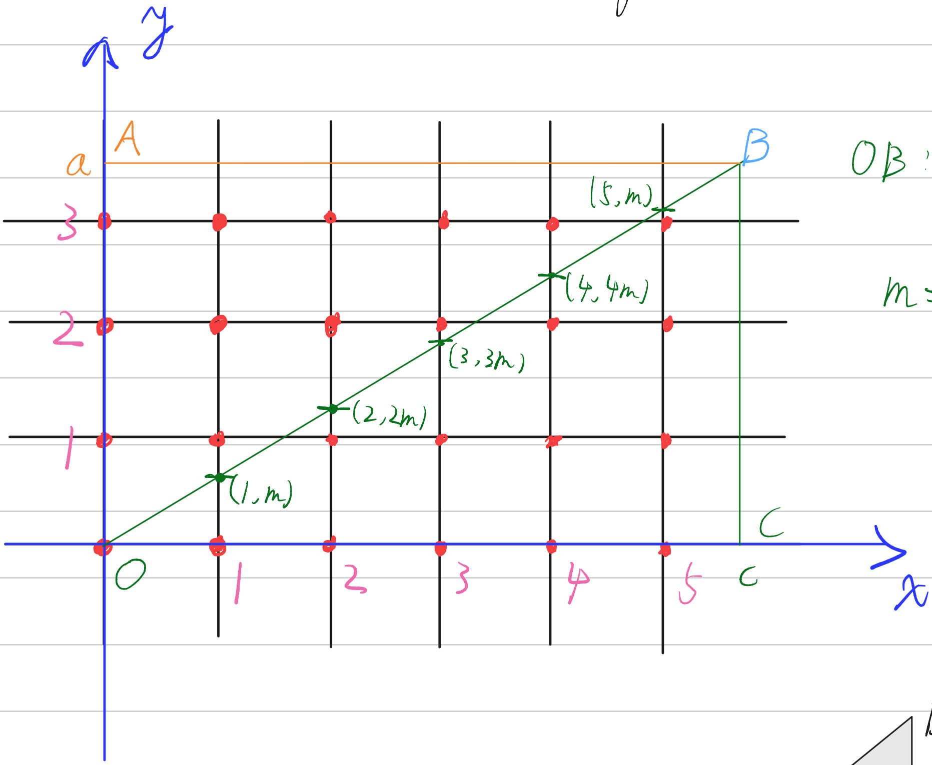
Q2: What if $a, b > 0$ are real numbers?



Number of lattice points

$= \lfloor a \rfloor \cdot \lfloor b \rfloor.$

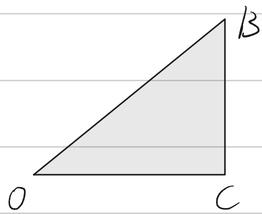
2. Lattice points in a triangle



OB : $y = mx$

$m = \frac{a}{c}$.

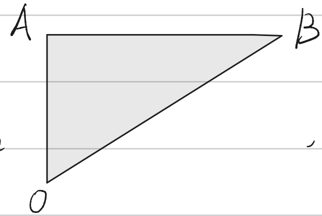
Q1: How many lattice points in



, including points on OB, BC but not those on OC?

A: $\lfloor 1 \cdot m \rfloor + \lfloor 2 \cdot m \rfloor + \lfloor 3 \cdot m \rfloor + \cdots + \lfloor \lfloor c \rfloor m \rfloor = \sum_{k=1}^{\lfloor c \rfloor} \lfloor \frac{ka}{c} \rfloor$.

Q2: How many lattice points in



, including points on OB, AB but not those on OA?

A: $\lfloor 1 \cdot \frac{1}{m} \rfloor + \lfloor 2 \cdot \frac{1}{m} \rfloor + \cdots + \lfloor \lfloor a \rfloor \cdot \frac{1}{m} \rfloor = \sum_{k=1}^{\lfloor a \rfloor} \lfloor k \cdot \frac{1}{m} \rfloor = \sum_{k=1}^{\lfloor a \rfloor} \lfloor \frac{kc}{a} \rfloor$

using OB: $x = \frac{1}{m} \cdot y$.

Recall:

Gauss's lemma: Let $p > 2$ be prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Define

$$\varepsilon_a = \begin{cases} 1, & a > 0, \\ -1, & a < 0. \end{cases}$$

Then

$$\left(\frac{a}{p}\right) = (-1)^{S(a,p)} \varepsilon_a^{\frac{p-1}{2}},$$

where

$$S(a,p) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{k\varepsilon_a a}{p} \right\rfloor + \frac{p^2-1}{8}(a-1).$$

Note: If a is odd, then $\frac{p^2-1}{8}(a-1) \equiv 0 \pmod 2$.

Eisentein's proof of quadratic reciprocity:

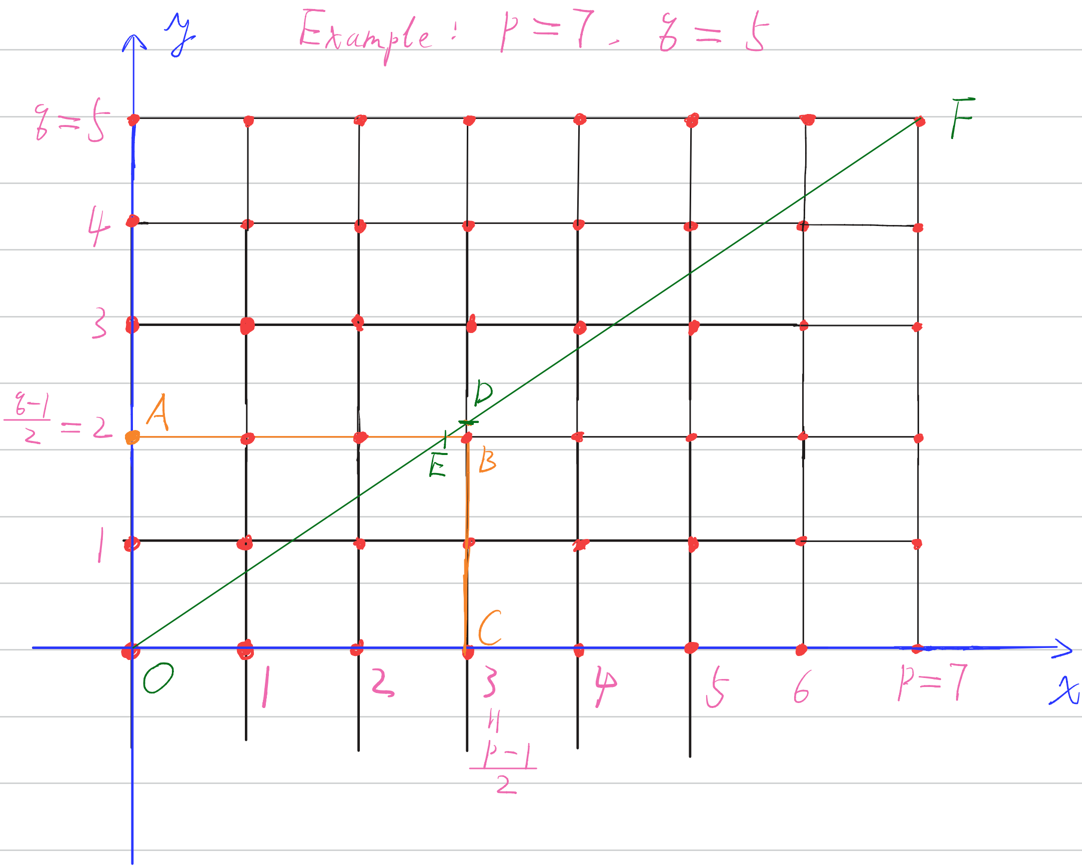
By Gauss's lemma,

$$\left(\frac{p}{q}\right) = (-1)^{S(p,q)}, \quad S(p,q) = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

$$\left(\frac{q}{p}\right) = (-1)^{S(q,p)}, \quad S(q,p) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

$$\Rightarrow \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}$$

$$\overset{?}{=} (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$



① Number of lattice points in $\square OABC$ (A, B, C, O) $= \frac{p-1}{2} \cdot \frac{q-1}{2}$.