MATH453 Elementary Number Theory

Lecture 2: Congruence and The Division Algorithm

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

2.1 Congruence and Sum of Two Squares

Recall that $a \equiv b \mod c$ if and only if $c \mid (a-b)$.

If $p \equiv 1 \mod 4$, we will show that $p = a^2 + b^2$ for some integers a and b. Such pair of a, b where $a, b \in \mathbb{Z}$ is called a ***lattice point***.

Theorem 2.1 (Fermat's theorem on sum of two squares)**.** An odd prime p can be expressed as $p = x^2 + y^2$ with integers x and y if and only if $p \equiv 1 \mod 4$.

Let $r_2(n)$ denote the number of representations of n as a sum of two squares. We would like to study the behavior of $\sum_{n \le x} r_2(n)$.

We start with **Gauss's attempt** in trying to bound $\sum_{n \le x} r_2(n)$. As we can see, each lattice point can be represented as the coordinate (m, n) of a point on a plane. If we draw a circle with radius r, then all lattice points within the circle have the property

$$m^2 + n^2 \le r^2$$

Then, the problem of bounding $\sum_{n \le x} r_2(n)$ for some x is the same as finding the number of lattice points within the circle centered at $(0, 0)$ with radius $\sqrt{x}$. Because of this, the problem is also known as ***Gauss circle problem***.

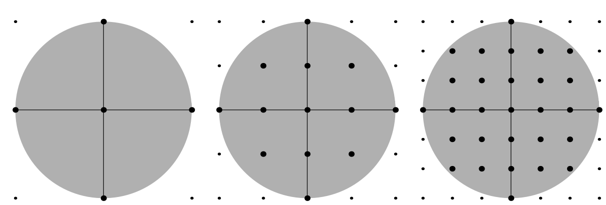

Figure 2.1: Gauss's circle problem

Theorem 2.2 (Gauss's solution)**.**

$$\sum_{n \le x} r_2(n) = \pi x + O(\sqrt{x}) = \pi x + \underbrace{E(x)}_{\text{error term}}$$

So, $E(x) \in O(x^{1/2})$.

Proof. We associate each representation of a number as two squares with a square on the plane, enclosed within the circle of radius $\sqrt{x}$.

Then, the number of such lattice points is bounded above by the area of the larger circle and bounded below by the smaller circle.

$$\pi(\sqrt{x}-1)^2 \leq \sum_{n\leq x} r_2(n) \leq \pi(\sqrt{x}+1)^2$$

We can further rearrange this to get

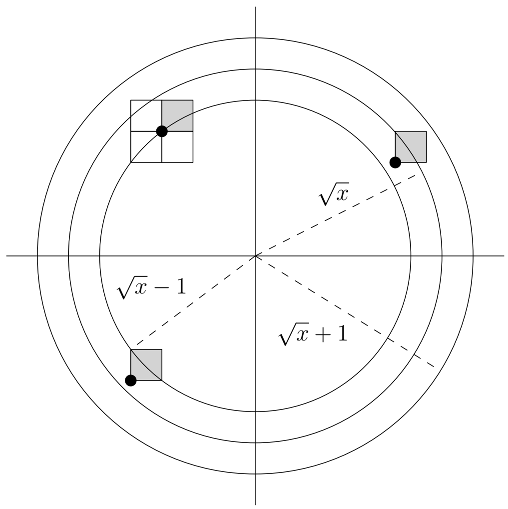

Figure 2.2: Using area to bound the number lattice points.

$$\pi(x-2\sqrt{x+1}) \leq \sum_{n\leq x} r_2(n) \leq \pi(x+2\sqrt{x}+1)$$

Then, $\sum_{n\leq x} r_2(n) = \pi x + O(\sqrt{x})$. ■

Over the years, there have been numerous improvements on bounding the error term.

Theorem 2.3 (Sierpinski 1906).

$$\sum_{n\leq x} r_2(n) = \pi x + O(x^{1/3})$$

2.2 Integer Partition

Next, we will consider the integer partition. A ***partition*** of an integer $n \in \mathbb{Z}^+$ is one way of representing n as a sum of **more than one** (possibly repeating) integers.

We define $P(n)$ to be the number of ways of writing $n \in \mathbb{Z}^+$ as a sum of positive integers (ways to partition n).

For example, $P(4) = 5$ because $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$. Note that 4 itself does not count since we need at least 2 integers for it to be a valid partition.

Conjecture (Ramanujan's Conjecture on Integer Partition). $P(5n+4) \equiv 0 \mod 5$, $P(7n+5) \equiv 0 \mod 7$, $P(11n+6) \equiv 0 \mod 11$.

2.3 Division Algorithm

2.3.1 Propositions About Division

Before we talk about the division algorithm, we first introduce some useful propositions about division.

Proposition 2.1. $a \mid b$ and $b \mid c \implies a \mid c$.

Proof. The proof is straightforward from the definition of the division relation.

Since $a \mid b$, $\exists c_1 \in \mathbb{Z}. b = c_1 a$. Similarly, $\exists c_2 \in \mathbb{Z}. c = c_2 b$ since $b \mid c$. We can then rewrite c as $c = c_2 b = c_1 c_2 a = (c_1 c_2)a$. Since c_1 and c_2 are all integers, $c_1 c_2$ is also an integer. Then, by definition, $a \mid c$. ■

Proposition 2.2. If $c \mid a$ and $c \mid b$, then $\forall m, n \in \mathbb{Z}. c \mid (ma + nb)$.

Proof. Again, this is immediate from the definition and basic arithmetics.

Since $c \mid a$, $\exists c_1 \in \mathbb{Z}. a = c_1 c$. Since $c \mid b$, $\exists c_2 \in \mathbb{Z}. b = c_2 c$.

Let $m, n \in \mathbb{Z}$ be arbitrary. Then, $ma + mb = mc_1 c + nc_2 c = c(mc_1 + nc_2)$. By definition, $c \mid (ma + mb)$. ■

2.3.2 Floor and Ceiling

Definition 2.1 (Floor). The floor of x, denoted $\lfloor x \rfloor$, is the greatest integer less than or equal to x.

Similarly, we define the ceiling as follows

Definition 2.2 (Ceiling). The ceiling of x, denoted $\lceil x \rceil$, is the smallest integer greater than or equal to x.

Remark. In his lecture notes, Professor Berndt used $[\cdot]$ for floor. I decided to use the more standard notation in my notes to avoid confusion.

Lemma 2.4. For $x \in \mathbb{R}$, $x - 1 < \lfloor x \rfloor \leq x$.

Proof. By contradiction. Suppose not, then there exists some $x \in \mathbb{R}$ such that $x - 1 \geq \lfloor x \rfloor$. Take such x and add 1 to both sides of the inequality, yielding $x \geq \lfloor x \rfloor + 1$. But by definition, $\lfloor x \rfloor$ is the greatest integer less than or equal to x. The fact that $\lfloor x \rfloor + 1$, which is strictly greater than $\lfloor x \rfloor$, is also less than or equal to x contradicts the definition of floor. Therefore, the original lemma holds. ■

2.3.3 The Division Algorithm

The **division algorithm** is also known as the **quotient remainder theorem**. The statement is as follows.

> **Theorem 2.5** (The Division Algorithm). Let $a, b \in \mathbb{Z}$ such that $b > 0$. Then, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

Proof. We divide the proof into two parts: existence and uniqueness. We first prove **existence** by construction.

Take $q = \lfloor a/b \rfloor$ and $r = a - b\lfloor a/b \rfloor$. Then, we have

$$a = b\left\lfloor \frac{a}{b} \right\rfloor + r$$

This proves that $a = bq + r$. Next, we show that $0 \leq r < b$. By Lemma 2.4,

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}$$

Since $b > 0$, we can multiply both sides by b, yielding

$$a - b < \left\lfloor \frac{a}{b} \right\rfloor b \leq a$$

Mutiply by -1 and reversing the signs, and then add a to both sides

$$\begin{aligned} b - a > -\left\lfloor \frac{a}{b} \right\rfloor b &\geq -a \\ b > -\left\lfloor \frac{a}{b} \right\rfloor b + a &\geq 0 \end{aligned}$$

Since $r = a - b\lfloor a/b \rfloor$, by substitution, $b > r \geq 0$. This proves the existence of such q, r.

Next, we prove the **uniqueness** of such q and r by contradiction. Suppose for contradiction that there exists some $q' \neq q$ and $r' \neq r$ such that $a = bq' + r'$ and $0 \leq r' < b$. Then,

$$a - a = 0 = b(q - q') + (r - r')$$

$|r - r'| < b$ because both $r < b$ and $r' < b$. WLOG, suppose $r' > r$. Then, $r' - r = b(q' - q)$ by rearranging the previous inequality. This implies that $r' - r$ is a multiple of b. But since $r' - r$ is strictly less than b,

$$0 \leq r' - r < b$$

$r' - r$ must be 0. This contradicts the assumption that $r \neq r'$. Similarly, $q = q'$ since $r = r'$, which is also a contradiction. ∎