Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 1, 2023

What we have seen last lecture

- Important topics in number theory
  - Infinitude of primes
  - Perfect numbers and Mersenne primes
  - Prime number theorem
  - Gaps between primes
- Divisor set
- Multiplicative functions $\sigma_k(-)$
- Euclid-Euler theorem
- Number systems
  - Rational numbers ~ (reduced) fractions
  - Irrational numbers Rational Root Thm
  - Algebraic numbers

Today's topics

- Diophantine approximation
- Dirichlet's approximation theorem
- Ford circles

Diophantine approximation

Diophantine approximation

usually irr (or a priori DON'T know)

Question

Given a real number α, approximate it by rational numbers.

A typical Diophantine approximation theorem would claim the existence or infinitude of rational numbers r approximating the given real number α within a reasonable bound $f(r)$:

$$|\alpha - r| \leqslant f(r).$$

The first theorem in the field of Diophantine approximation follows from the geometry of number line.

Theorem 9.1

Let α be a real number and b be a positive integer. Then there is an integer a such that

existence

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{2b}.$$

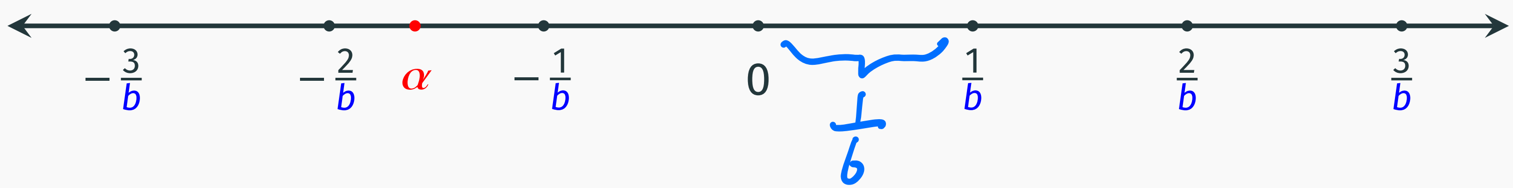
E.g. $\pi = 3.1415926\ldots$.

$\left|\pi - \frac{3}{1}\right| \approx 0.14 < \frac{1}{2}$

$\left|\pi - \frac{31}{10}\right| \approx 0.04 < \frac{1}{20} = 0.05$

Proof of the theorem

Proof. Let's first plot $\frac{1}{b}\mathbb{Z}$ on the number line:



Let's say α is between $\frac{c}{b}$ and $\frac{c+1}{b}$. One of $\frac{c}{b}$ and $\frac{c+1}{b}$ is closer to α than the other. Choose the closer one to be $\frac{a}{b}$. Then we have

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{2}\text{length of the interval } [\tfrac{c}{b}, \tfrac{c+1}{b}] = \frac{1}{2b}. \qquad \square$$

Sometimes, we have far better approximation.

Example 9.2

$\pi = 3.1415926\ldots.$

- $\frac{a}{b} = 3.14 = \frac{157}{50}$: $\left|\pi - \frac{a}{b}\right| \approx 0.00159$, while $\frac{1}{2b} = 0.01$. ($\sim 16\%$)
- $\frac{a}{b} = \frac{22}{7}$: $\left|\pi - \frac{a}{b}\right| \approx 0.0013$, while $\frac{1}{2b} \approx 0.07$. ($\sim 2\%$)
- $\frac{a}{b} = \frac{355}{113}$: $\left|\pi - \frac{a}{b}\right| \approx 0.00000027$, while $\frac{1}{2b} \approx 0.0044$. ($\sim 0.006\%$)

One motivation to study Diophantine approximation is the following phenomenon.

Guideline

If an irrational number α *can be approximated by rational numbers* **too well**, *then* α *is likely to be* **transcendental**.

E.g. $$e = \underbrace{1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}}_{\text{a rational number with denominator } n!} + \underbrace{\cdots}_{\sum_{k>n} \frac{1}{k!} \sim \frac{1}{(n+1)!}}$$

$$\frac{1}{2\cdot(n!)} \longrightarrow 0 \quad (n \to \infty)$$

Theorem 9.3 (Liouville, 1840s)

Let α be an **irrational algebraic** *number of* **degree** $\leqslant n$ *(which means it is a root of an integer polynomial of degree n). Then there is a constant $C > 0$ such that*

$$\left|\alpha - \frac{a}{b}\right| > \frac{C}{b^n} \quad \text{for all} \quad a \in \mathbb{Z}, b \in \mathbb{Z}_+.$$

No better than this!

Theorem 9.4 (Thue-Siegel-Roth, 1900s–1950s)

Let α be an **irrational algebraic** *number and ε a small positive real number. Then there is a constant $C > 0$ such that*

$\varepsilon > 0$

$$\left|\alpha - \frac{a}{b}\right| > \frac{C}{b^{2+\varepsilon}} \quad \text{for all} \quad a \in \mathbb{Z}, b \in \mathbb{Z}_+.$$

No better than this!

Dirichlet's approximation theorem

Dirichlet's approximation theorem

Theorem 9.5 (Dirichlet, 1840)

Let α be an **irrational** *number, Then there are infinitely many fractions $\frac{a}{b}$ such that*

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{2b^2}.$$

N.B. this theorem doesn't imply that for ***all*** positive integer b, there is a fraction $\frac{a}{b}$ approximating α with above error bound. (Compare it with theorem 9.1)

E.g. for $\pi = 3.1415926\ldots$:

- $b = 1$ works: $\left|\pi - \frac{3}{1}\right| \approx 0.14 < \frac{1}{2}$.
- $b = 2$ doesn't work: $\left|\pi - \frac{6}{2}\right| \approx 0.14 > \frac{1}{2 \cdot 2^2} = 0.125$.

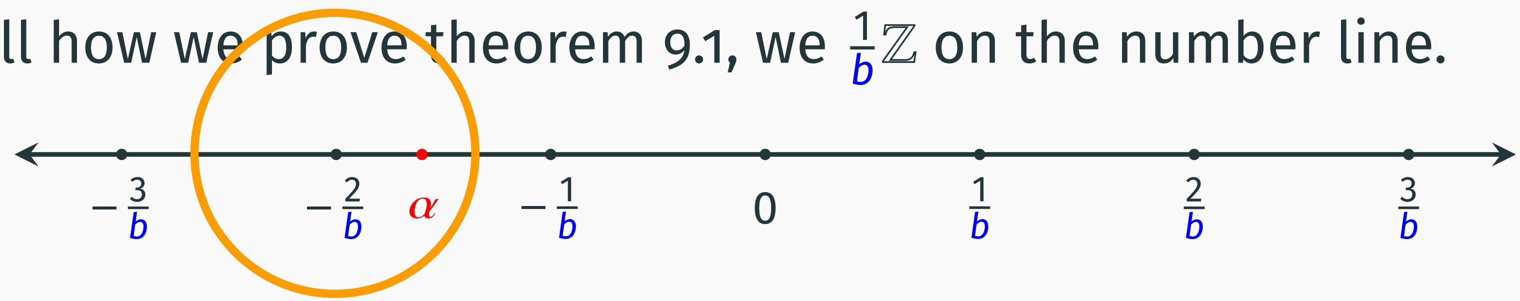
Outline of the proof

To prove this theorem, we first interpret the inequality

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{2b^2}$$

in terms of geometry: it means the point α is within distance $\frac{1}{2b^2}$ from the point $\frac{a}{b}$.

Recall how we prove theorem 9.1, we $\frac{1}{b}\mathbb{Z}$ on the number line.



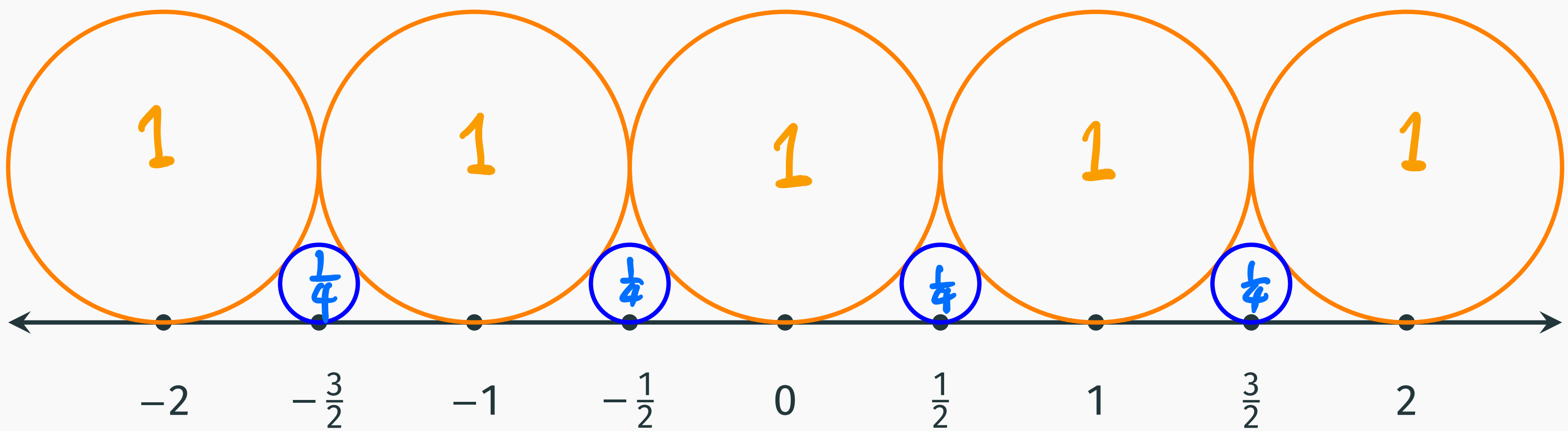
Instead of consider intervals $[\frac{c}{b}, \frac{c+1}{b}]$, we put circles of diameter $\frac{1}{b^2}$ at each $\frac{a}{b}$. So the inequality holds whenever α is covered by one of such circles.

Ford circles

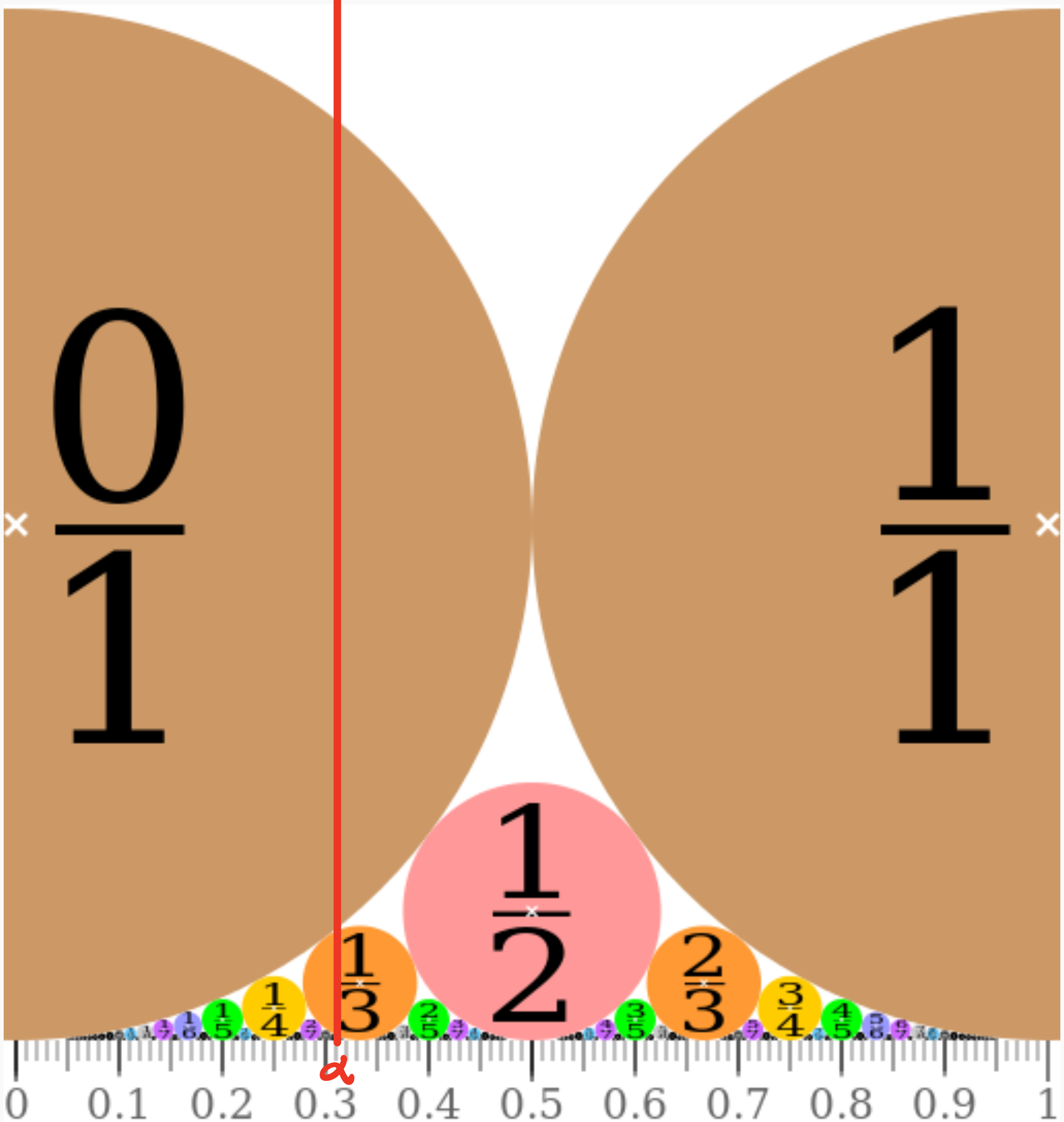
Ford circles

Definition 9.6 (Lester Ford, 1938)

A ***Ford circle*** is a circle of diameter $\frac{1}{b^2}$ atop the rational point on the number line corresponding to the reduced fraction $\frac{a}{b}$. (Integers are expressed as reduced fractions with denominator 1.)



Ford circles



The left shows Ford circles between 0 and 1. Draw a vertical line crossing α, then the inequality $\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{2b^2}$ holds whenever the line crosses the Ford circle atop $\frac{a}{b}$.

Ford circles

So to prove Dirichlet's approximation theorem, it is sufficient to show that a vertical line atop an irrational point crosses infinitely many Ford circles.

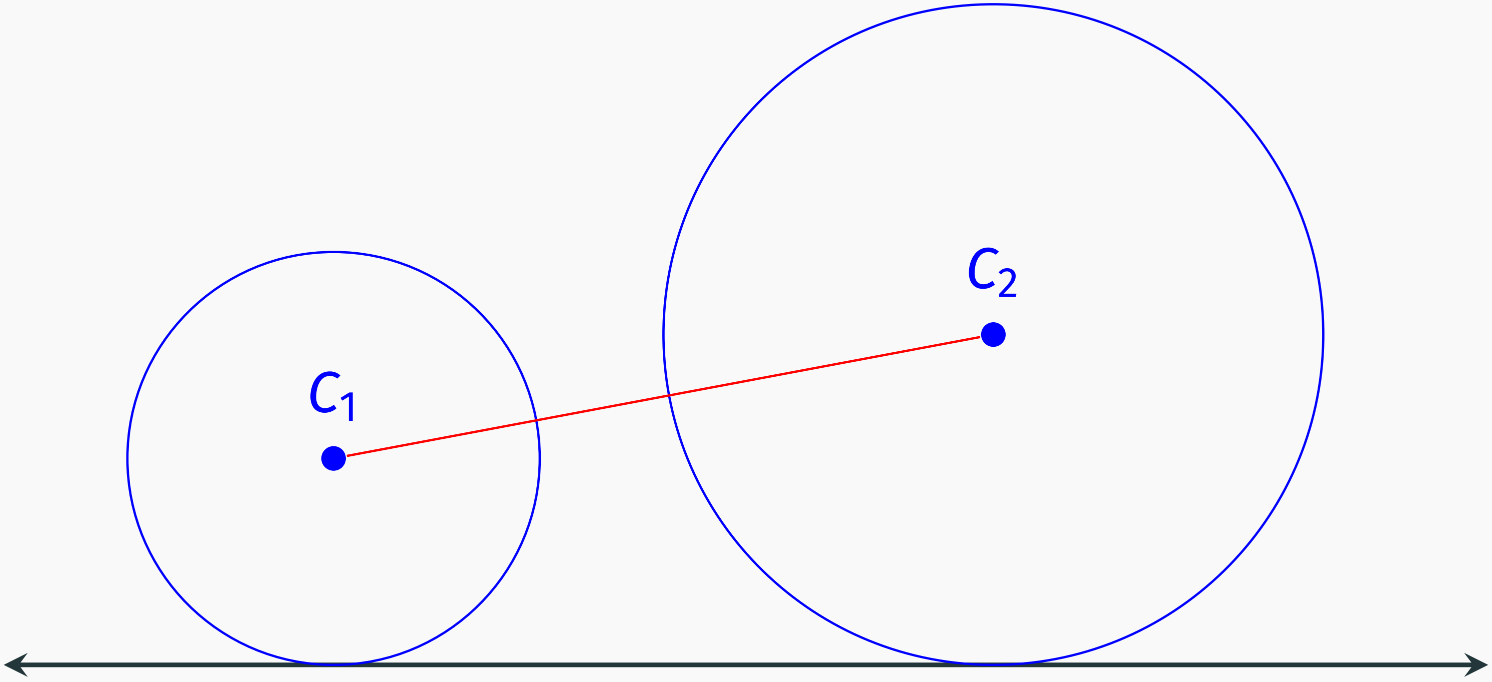
We will do this through an induction on b. For this purpose, we need a recursive description of Ford circles.

We first note that there are no overlaps between Ford circles: they are either tangent to or separated from each other.

Indeed, let C_1 and C_2 be two Ford circles atop $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ respectively. Then we know that they can be described by the equations By defn of Ford circles.

$$(x - \frac{a_1}{b_1})^2 + (y - \frac{1}{2b_1})^2 = \frac{1}{2b_1}, \quad \text{and} \quad (x - \frac{a_2}{b_2})^2 + (y - \frac{1}{2b_2})^2 = \frac{1}{2b_2}$$

repsectively. Therefore, the distance between their centers is



distance between centers
v.s.
sum of radii

Ford circles

Therefore, the distance between their centers is

$$d(C_1, C_2) = \sqrt{\left(\frac{a_2}{b_2} - \frac{a_1}{b_1}\right)^2 + \left(\frac{1}{2b_2} - \frac{1}{2b_1}\right)^2}$$

$$= \sqrt{\frac{(a_2b_1 - a_1b_2)^2}{b_1{}^2 b_2{}^2} + \left(\frac{1}{2b_2} - \frac{1}{2b_1}\right)^2}$$

$$\geq \sqrt{\frac{1}{b_1{}^2 b_2{}^2} + \left(\frac{1}{2b_2} - \frac{1}{2b_1}\right)^2}$$

$$= \frac{1}{2b_1} + \frac{1}{2b_2}.$$

$\frac{a_1}{b_1} \neq \frac{a_2}{b_2}$

$\Downarrow$

$a_2b_1 - a_1b_2 \neq 0$

radius of C_1 radius of C_2

$\Rightarrow$ No overlaps !

Kissing fractions

Kissing fractions

So when do two Ford circles tangent to each other?

Note that in the previous slide, the quality holds if and only if $|a_2 b_1 - b_2 a_1| = 1$. We thus have the following notion:

Definition 9.7

We say two fractions $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ ***kiss*** each other if

$$\left|\underset{\uparrow\atop\text{determinant}}{\det}\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}\right| = |a_2 b_1 - a_1 b_2| = 1.$$

We will use the notation $\frac{a_1}{b_1} \heartsuit \frac{a_2}{b_2}$ to denote this.

Kissing fractions

$a_1 b_2 - b_1 a_2 = \pm 1$ & Bézout Identity

N.B. $\frac{a_1}{b_1} \heartsuit \frac{a_2}{b_2}$ implies that $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ are ***reduced*** fractions (why?). Since any rational number has a unique reduced fraction expression, $\heartsuit$ is rather a relation between rational numbers.

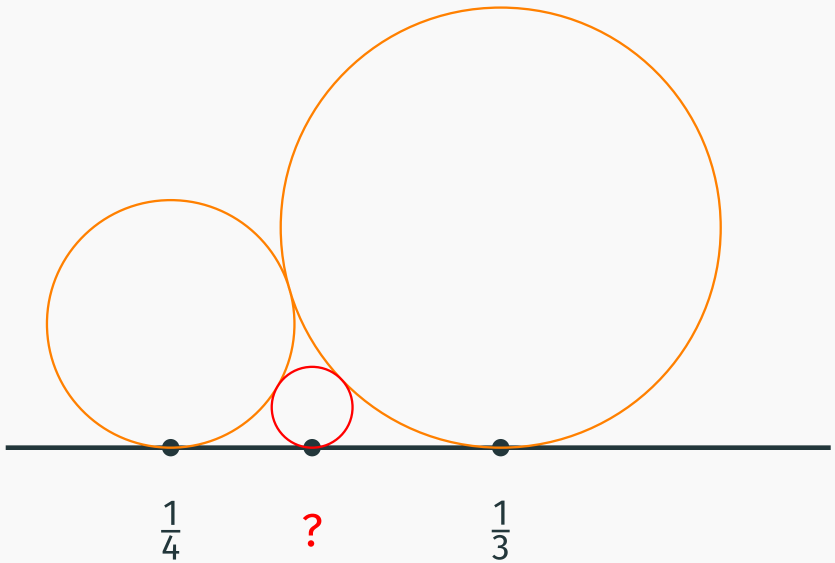
What we have proved can be interpreted as:

Lemma 9.8

Two Ford circles are tangent to each other if and only if the fractions they atop kiss each other.

Kissing fractions

In next lecture, we will show that if you have two Ford circle tangent to each other, then you can find a third one tangent to both of them.



Translating this into fractions, it means if you have a pair of kissing fractions, then there is a third one kisses both of them.