No.

Date 2013 · 12 · 24

# Introduction to zeta Functions

Daqing Wan.

Math is about solving equations.

1. Counting prime numbers

$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ $(\mathbb{Z}, +)$ cyclic abelian gp

$(\mathbb{Z} - \{0\}, \times)$ semi-abelian gp generated by prime number

Thm (fundemental thm of arithmetic)

Every $n \in \mathbb{Z}_{>0}$ $n$ can be factorized in a unique way as a product of prime powers

<u>Def</u>: For $t \in \mathbb{R}_{\geq 2}$, define

$$\pi(t) = \#\{p \text{ prime} \mid 2 \leq p \leq t\}$$

Thm $\lim_{t \to \infty} \pi(t) = \infty$

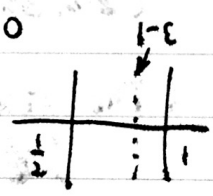
Prime number theorem: $\pi(t) = \frac{t}{\ln t}(1 + o(1))$

<u>Cor</u> Prob(random chosen $n \in \mathbb{Z}_{>0}$ to be prime) $= \frac{1}{\ln n}$

This suggests $\pi(t) \sim \int_2^t \frac{1}{\ln x} dx = Li(t) = \frac{t}{\ln t} + \frac{t}{\ln^2 t} + \frac{2t}{\ln^3 t} + \cdots + O\left(\frac{k! t}{\ln^{k+1} t}\right)$

Riemann Hypothesis (RH) $\pi(t) = \int_2^t \frac{dx}{\ln x} + O(t^{\frac{1}{2}+\varepsilon})$ $\forall \varepsilon > 0$

Equivalently, $\left|\pi(t) - \int_2^t \frac{dx}{\ln x}\right| \leq \frac{\sqrt{t} \ln t}{8\pi}$, $t \geq 2657$




Thm: $\pi(t) = \int_2^t \frac{dx}{\ln x} + O\left(t \cdot \exp\left(\frac{-A(\ln t)^{3/5}}{(\ln \ln t)^{1/5}}\right)\right)$ $A > 0$

2. Riemann Zeta function

$$\zeta(\mathbb{Z}, s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} = \prod_{p \text{ prime}} (1 + p^{-s} + p^{-2s} + \cdots) \overset{UFD}{=} \sum_{n=1}^{\infty} \frac{1}{n^s} < \infty \text{ if } Re(s) > 1$$

$\zeta(\mathbb{Z}, s)$ is $\mathbb{C}$-entire for $Re(s) > 1$

Thm (Riemann) $\zeta(\mathbb{Z}, s)$ extends to a $\mathbb{C}$-meromorphic function in $s \in \mathbb{C}$ with a simple pole at $s = 1$ i.e. $(s-1)\zeta(\mathbb{Z}, s)$ is a $\mathbb{C}$-entire function

No

Date

(there is an explicit formula for $\pi(t)$ in terms of zeros and poles of $\zeta(\mathbb{Z}, s)$)

RH: If $s \in \mathbb{C}$ s.t. $\zeta(\mathbb{Z}, s) = 0 \Rightarrow Re(s) \in \frac{1}{2}\mathbb{Z}$.

3. Hassel-Weil zeta functions

Let $A$ be a f.g. commutative $\mathbb{Z}$-algebra

$A = \mathbb{Z}[x_1, \cdots, x_n]/I$ $\quad I$ is an ideal of $\mathbb{Z}[x_1, \cdots, x_n]$

(Hilbert basis thm: $I = (f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n))$

It is difficult to count prime ideals of $A$, so we turn to maximal ideals

$X = \operatorname{Spec} A$ = the set of all the prime ideals in $A$

(Zariski topology)

$|X| = \operatorname{Specm} A$ = the set of maximal ideals in $A$

= the set of closed points in $X$

If $x \in |X|$, $\Rightarrow A/x$ is a f.g. field over $\mathbb{Z}$

$\Rightarrow A/x$ is a finite field $\mathbb{F}_{p^r}$ for some prime $p$ and $r \geq 1$

<u>Def</u>: $N(x) = \# A/x = p^r$

(剩余函数)

Def (The Hasse-Weil) Zeta function of $A$ (or $X$) is

$$\zeta(A, s) = \prod_{x \in |X|} \frac{1}{1 - N(x)^{-s}} \qquad \text{e.g. } \zeta(\mathbb{Z}, s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

Prop: $\zeta(A, s)$ is $\mathbb{C}$-analytic for $Re(s) > \dim(X)$

<u>Conj</u> (I) (Meromorphic Continuation)

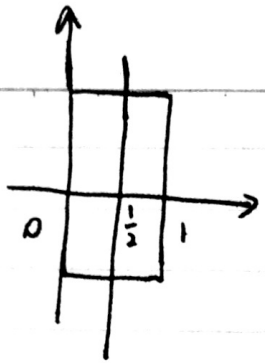
$\zeta(A, s)$ extends to a $\mathbb{C}$-meromorphic function in $s \in \mathbb{C}$

$\Rightarrow$ An explicit formula for $\pi_A(t) = \# \{x \in |X| \mid N(x) \leq t\}$

in terms of zeros and poles of $\zeta(A, s)$

<u>Conj</u> (II) (GRH) If $s \in \mathbb{C}$ st $\zeta(A, s) = 0$ or $\infty$

$\Rightarrow Re(s) \in \frac{1}{2}\mathbb{Z}$ ($\Rightarrow$ a sharp asymptotic formula for $\pi_A(t)$)




to check RH is right in the box
use the Intergration to compute the number of roots
second, check on the line $\frac{1}{2}+it$
that the sgn changes $k$ times, where $k$
is the root number (Q: what if the root on $\frac{1}{2}+it$ have multiplicity)

4. Examples

① $A = \mathbb{Z}/(n)$ $\quad n>1$ positive integer $\quad \dim = 0$

write $n = p_1^{a_1}\cdots p_k^{a_k}$ $\quad p_1<\cdots<p_k$ prime

max ideals $= (p_j) = p_j A$

$$N(p_jA) = \# A/p_jA = \# \mathbb{Z}/p_j\mathbb{Z} = p_j$$

$$\Rightarrow \zeta(A,s) = \prod_{j=1}^{k} \frac{1}{1-p_j^{-s}} \text{ is } \mathbb{C}\text{-mero in } s\in\mathbb{C}$$

no zeros

poles: $\quad 1 = p_j^{-s} \Rightarrow 1 = e^{-s\ln p_j} \Rightarrow s = -\frac{2\pi i\cdot m}{\ln p_j} \quad m\in\mathbb{Z}$

$$\operatorname{Re} s = 0 \in \tfrac{1}{2}\mathbb{Z}$$

so the conjecture holds

Q: how fast can one compute $\zeta(\mathbb{Z}/n\mathbb{Z}, s)$
($\Leftrightarrow$ integer factionization of $n$)

② $A = \mathbb{Z}[X]/(p)$ $\quad p$ prime $\quad \dim = 1$ (dim is big, the problem is diffiult)
$= \mathbb{F}_p[X]$

max ideals $= (f)$ $\quad f\in\mathbb{F}_p[X]$ irreducible of $\deg f \geq 1$

$$N(f) = \# A/(f) = p^{\deg(f)}$$

$$\text{so } \zeta(A,s) = \prod_{f \text{ irreducible}} \frac{1}{1-p^{-\deg(f)\cdot s}} = \prod_{f \text{ irr}} \frac{1}{1-(p^{-s})^{\deg f}} = Z(A, p^{-s})$$

$$\text{where } Z(A,T) = \prod_{f \text{ irr}} \frac{1}{1-T^{\deg f}} = \prod_{f \text{ irr}} (1+T^{\deg f}+T^{2\deg f}+\cdots)$$

$$\overset{\text{UFD}}{=\!=} \sum_{\substack{g\in\mathbb{F}_p[x]\\ \text{monic}}} T^{\deg g} = \sum_{d\geq 0}^{\infty} \Big(\sum_{\substack{g\in\mathbb{F}_p[x]\\ \text{monic}\\ \deg(g)=d}} 1\Big) T^d$$

No.

Date

$(g = x^d + a_1 x^{d-1} + \cdots + a_d \quad a_i \in \mathbb{F}_p)$

$$= \sum_{d=0}^{\infty} p^d T^d = \frac{1}{1-pT} \in \mathcal{O}[T]$$

$$\zeta(A,s) = Z(A, p^{-s}) = \frac{1}{1-p^{1-s}} \quad \mathbb{C}\text{-merom}$$

no zero

pole: $s = 1 + \frac{2\pi i}{\ln p} \cdot m \quad m \in \mathbb{Z}$

$\operatorname{Re} s = 1 \in \frac{1}{2}\mathbb{Z}$

Def $N_d = \#\{f \text{ monic irreducible in } \mathbb{F}_p[X] \mid \deg(f) = d\}$

$M_d = \sum_{k|d} k \cdot N_k$

$$Z(\mathbb{F}_p[X], T) = \prod_{\substack{f \text{ monic} \\ \text{irred}}} \frac{1}{1-T^{\deg f}}$$

$$= \prod_{d=1}^{\infty} \left(\frac{1}{1-T^d}\right)^{N_d} \overset{(\text{Ex})}{=} \exp\left(\sum_{d=1}^{\infty} \frac{T^d}{d} \overbrace{\left(\sum_{k|d} kN_k\right)}^{M_d}\right)$$

$$= \frac{1}{1-pT}$$

$\Rightarrow M_d = p^d \quad (d = 1, 2, 3 \cdots)$

By Möbius inverse $N_d = \frac{1}{d} \sum_{k|d} \mu(\frac{d}{k}) p^k = \frac{p^d}{d} + \mathcal{O}(p^{\frac{d}{2}+\varepsilon})$

This is prime number theorem for polynomial ring $\mathbb{F}_p[X]$

③ $A = \mathbb{Z}[X]/(p, f(x)) = \mathbb{F}_p[X]/(f(x)) \quad f \in \mathbb{F}_p[X]$ monic, $\deg(f) = d > 0 \quad \dim = 0$

write $f(x) = f_1(x)^{a_1} \cdots f_k(x)^{a_k} \quad f_1, \cdots, f_k$ monic, irreducible distinct

max ideals in $A = (f_i) = f_i A$

$$N(f_i A) = \# A/f_i A = \# \mathbb{F}_p[x]/(f_i) = p^{\deg(f_i)}$$

$$\Rightarrow \zeta(A,s) = \prod_{i=1}^{k} \frac{1}{1-(p^{\deg f_i})^{-s}} = Z(A, p^{-s})$$

$$Z(A,T) = \prod_{i=1}^{\infty} \frac{1}{1-T^{\deg f_i}}$$

$\Rightarrow \zeta(A,s)$ is $\mathbb{C}$-mero satisfies GRH

No.

Date

Question: How fast can one compute $Z(\mathbb{F}_p[x]/\mathbb{F}_p, T)$ ?

~~Then~~ Conjecture $f(x)$ in $\mathbb{F}_p[x]$ can be factorized in random polynomial time $(d \log p)^{O(1)}$

almost true, but still not proved

Question: Can one factor $f(x) \in \mathbb{F}_p[x]$ in determined poly time $O(d \log p)^{O(1)}$

This is open even if $f = x^2 - a$ (quadratic)

(yes if you assume GRH)

Conjecture: $RP = P$ (random poly time = poly time)

Question: GRH $\Rightarrow$ "$RP = P$"

Given $a \in \mathbb{F}_p$, $x^2 - a$ is reducible in $\mathbb{F}_p[x]$

$\Leftrightarrow \left(\frac{a}{p}\right) = 1$ (legendre symbol)

$\Leftrightarrow$ $a$ is a square in $\mathbb{F}_p$

$\Leftrightarrow$ $a = b^2$ in $\mathbb{F}_p$ for some $b \in \mathbb{F}_p$

Q: how to find $b$ quickly

$\Downarrow$

Special case: if $p \equiv 1 \pmod 4$ $\Rightarrow$ $-1$ is a square

how to find $\sqrt{-1}$ quickly?

Q: how fast can one find a nonsquare in $\mathbb{F}_p$ ?