Lecture 11: (No class next week) 30/5/2018

The ABC Conjecture (1985) Masser & Oesterle

Def:

The radical of an integer n is $\text{rad}(n) = \prod_{\substack{p \mid n \\ \text{prime}}} p$

e.g. $\text{rad}(12) = 2 \cdot 3 \quad (12 = 2^2 \cdot 3)$

$\text{rad}(\pm p_1^{e_1} \cdots p_r^{e_r}) = p_1 p_2 \cdots p_r, \quad p_i \neq p_j$ primes, $e_j \geq 1$

ABC conjecture: $\forall \varepsilon > 0, \exists K(\varepsilon) > 0$,

Suppose A, B, C are coprime integers, $A + B = C$. Then,

$$\max\{|A|, |B|, |C|\} \leq K(\varepsilon) \, \text{rad}(ABC)^{1+\varepsilon}$$

or

$\forall \varepsilon > 0$, there are at most finitely many sols $A, B, C \in \mathbb{Z}$ coprime with $A + B = C$, $\max(|A|, |B|, |C|) > \text{rad}(ABC)^{1+\varepsilon}$

Applications:

1) Asymptotic Fermat last theorem: $\exists N_0$ s.t $\forall N \geq N_0$ there are no integer solutions of $x^N + y^N = z^N$, $xyz \neq 0$.

solved $\boxed{\forall N}$ by A. Wiles (1994)

History:

$N = 2$, Pythagarean triples $x^2 + y^2 = z^2$: $\exists$ infinitely many coprime triples.

$(3, 4, 5)$ $(5, 12, 13)$, ...

17th century Fermat $\overset{\text{conj}}{}$: If $N \geq 3$ then no interesting integer sols $1^N + 0^N = 1^N$.

Fermat: $N = 4, 3$.

Fermat is as easy as ABC

$A = x^N$, $B = y^N$, $C = z^N$, $A + B = C$, x, y, z coprime $\Rightarrow A, B, C$ coprime

Fix $\varepsilon > 0$, $\exists K(\varepsilon) > 0$ s.t $C = z^N < K(\varepsilon) \cdot \text{rad}(x^N y^N z^N)^{1+\varepsilon}$

$$\operatorname{rad}(x^N y^N z^N) = \operatorname{rad}(xyz) \le xyz \le z^3$$

$\Longrightarrow$ $z^N \le K(\varepsilon)\, z^{3(1+\varepsilon)}$ (assume $N > 3$)

$\Longrightarrow$ $z^{N-3-3\varepsilon} < K(\varepsilon) \Longrightarrow z < K(\varepsilon)^{\frac{1}{N-3-3\varepsilon}}$. take $\varepsilon = \frac{1}{6}$. $K = K(\frac{1}{6})$

$1 < z \le K^{\frac{1}{N-3\frac{1}{2}}}$. For $N >> 1$, $K^{\frac{1}{N-7/2}} < 2$. get $1 < z < 2$.

Contradiction. ▨

2) Catalan's conjecture: (1844)

There are no consecutive perfect powers except (9,8).

i.e. $x^m - y^n = 1$, $x, y \ge 2$, $m, n \ge 2 \Longrightarrow 3^2 - 2^3 = 1$

exercise: $m = n$.

Euler (1750): $(m,n) = (2,3)$ or $(3,2)$

- Can assume m, n are prime ($X^6 = (X^2)^3$)

V.A. Lebesgue (1850): $X^p - Y^2 = 1$ no solutions.

Nagell (1921): $\min(m,n) \ne 3$

Chao Ko (1964): $x^2 - y^q = 1$, $q > 2$ prime, no solution except $(9,8)$

Cassels (1960): $p, q \ge 3$ prime, then $x^p - y^q = 1 \Rightarrow q \mid x,\ p \mid y$

(1976) Tijdeman:

At most finitely many sols. Size is $<< e^{e^{e^{e^{1976}}}}$ (improved $< 10^{21}$)

(2002) P. Mihailescu solved Catalan.

Pillai's conjecture (1931):

Every integer is a difference of perfect powers finitely often.

Fix $k \ne 0$. $x^m - y^n = k$ only finitely many sols.

(x, y, m, n), $x, y, m, n \ge 2$. (OPEN)

ABC $\Longrightarrow$ Catalan:

$$\underset{C}{x^m} = \underset{A}{y^n} + \underset{B}{1}$$

$A = y^n$, $B = 1$, $C = x^m$ clearly coprime.

$\forall \varepsilon > 0\ \exists K(\varepsilon) > 0$ s.t. $(x^m)^{1-\varepsilon} < K(\varepsilon)\, \mathrm{rad}(x^m \cdot 1 \cdot y^n) =$

$$= K(\varepsilon)\, \mathrm{rad}(xy)$$

Case 1: $m < n$.

$y = (x^m - 1)^{1/n} < x^{m/n}$, $m/n < 1$

$\Longrightarrow\ x^{m(1-\varepsilon)} < K(\varepsilon)\, \mathrm{rad}(xy) \le K(\varepsilon) \cdot xy < K(\varepsilon)\, x^{\overbrace{1+\frac{m}{n}}^{\le 2}}$.

$\Longrightarrow\ x^{(m-1-\frac{m}{n}) - \varepsilon} < K(\varepsilon)$

Since $m \ge 2$, $\frac{m}{n} < 1$, $m - 1 - \frac{m}{n} > 0 \Longrightarrow \boxed{x << 1}$

So finitely many sols. (Tijdeman).

Work for Pillais conj. as well. ABC $\Longrightarrow$ Pillai.

Exercise: $m = n$, or $m > n$. $\boxtimes$

Whats Known for ABC:

C. Stewart, R. Tijdeman, Yu Kunrui (1993):

$$\mathrm{Max}(|A|, |B|, |C|) < \exp\left(\mathrm{rad}(ABC)^{1/3}\right)$$

The ABC Theorem in $\mathbb{C}[t]$: (R. Mason 1983, Stothers 1981)

For $f \in \mathbb{C}[t]$, $\deg f > 0$, $f(t) = c \cdot \prod^r (t - \alpha_j)^{n_j}$, $\alpha_1, \dots, \alpha_r \in \mathbb{C}$ distinct.

$$\mathrm{rad}(f) := \prod_{j=1}^{r} (t - \alpha_j)$$

Note: $\mathrm{rad}(f \cdot g) = \mathrm{rad}(f) \cdot \mathrm{rad}(g)$ if $\gcd(f, g) = 1$.

ABC thm.:

$f, g, h \in \mathbb{C}[t]$ coprime $f + g = h$. Then

$$\max(\deg(f), \deg(g), \deg(h)) \le \deg \mathrm{rad}(f \cdot g \cdot h) - 1$$

Compare ABC for $\mathbb{Z}$: $A + B = \overset{\text{coprime}}{C}$. Then,

$$\max(\log |A|, \log |B|, \log |C|) \lesssim_{\varepsilon} (1 + \varepsilon) \log \mathrm{rad}(ABC)$$

Note:

For $\mathbb{C}[t]$ do not need $\varepsilon > 0$.

Exercise

Need ε for $\mathbb{Z}$. $\exists A_k, B_k, C_k$ coprime, $A_k + B_k + C_k$ s.t

$\max(A_k, B_k, C_k) \gg R_k \deg R_k$, $R_k = \mathrm{rad}(A_k B_k C_k)$

$A_k = 3^{2^k} - 1$, $B_k = 1$ $C_k = 3^{2^k}$

Observation:

$f \in \mathbb{C}[t]$, $\deg f > 0$.

$$\mathrm{rad}(f) = \frac{f}{\gcd(f, f')}$$

$f = (t-\alpha)^n g(t)$, $t - \alpha \nmid g(t) \iff g(\alpha) \neq 0$.

$f' = n(t-\alpha)^{n-1} g + (t-\alpha)^n \cdot g' = (t-\alpha)^{n-1} \cdot h(t)$, $t - \alpha \nmid h$.

This way we see $\gcd(f, f') = \prod (t - \alpha_j)^{n_j - 1}$

Pf of ABC:

$A + B = C$ coprime pols $A, B, C \in \mathbb{C}[t]$

$\implies A' + B' = C'$. Then $A'C - AC' = A'B - AB'$

Since $A'(A+B) - A(A'+B') = A'B - AB'$

Note:

$$\underset{\text{coprime}}{\gcd(A, A') \cdot \gcd(B, B')} \text{ divides } A'B - AB'$$

Likewise: $\gcd(C, C') \mid AB' - A'B$ $(= AC' - A'C)$

These are all coprime $\implies \gcd(A, A') \gcd(B, B') \gcd(C, C') \mid A'B - AB'$

$$\implies \frac{C}{\mathrm{rad}(C)} = \gcd(C, C') \mid \frac{A' \frac{B}{\gcd(B, B')}}{\gcd(A, A')} - \frac{A}{\gcd(A, A')} \cdot \frac{B'}{\gcd(B, B')}$$

$$\qquad\qquad\qquad\qquad \| $$

$$\frac{A'}{\gcd(A, A')} \mathrm{rad}(B) - \mathrm{rad}(A) \cdot \frac{B'}{\gcd(B, B')}$$

take degrees of both sides:

$$\deg(C) - \deg \mathrm{rad}(C) \leq \max \begin{cases} \deg A' + \deg \mathrm{rad} B - \deg \gcd(A, A'), & \deg \mathrm{rad}(A) + \deg(B') - \deg \gcd(B, B') \end{cases} (\leq)$$

$$\leq \max\Big(\underbrace{\deg(A) - 1 + \deg \operatorname{rad} B - \deg \gcd(A,A')}, \quad * \Big) =$$

$$= \deg \frac{A}{\gcd(A,A')} = \deg \operatorname{rad}(A) \Big)$$

$$= \deg \operatorname{rad}(A) + \deg \operatorname{rad}(B) - 1 \underset{A,B \text{ coprime}}{=} \deg \operatorname{rad}(A \cdot B) - 1$$

$$\implies \deg(C) - \deg \operatorname{rad}(C) \leq \deg \operatorname{rad}(AB) - 1$$

coprime to A,B $\implies \deg(C) \leq \deg \operatorname{rad}(ABC) - 1$

$\blacksquare$

<u>Application</u>: FLT for $\mathbb{C}[t]$:

$f^N + g^N = h^N$, $N \geq 3$ f, g, h coprime, $\deg > 0$. No solutions.

(Proved: Liouville 1851)

$A = f^N$, $B = g^N$, $C = h^N$

$$\max(\deg f^N, \deg h^N, \deg g^N) \leq \deg \operatorname{rad}(f^N \cdot g^N \cdot h^N) - 1 =$$

$$N \cdot \max(\deg f, \deg g, \deg h) \qquad = \deg \operatorname{rad}(f \cdot g \cdot h) - 1$$

Say $\deg f = \max(\deg f, \deg g, \deg h)$

$$N \cdot \deg f \leq \deg \operatorname{rad}(fgh) - 1 \leq \deg(fgh) - 1 = $$

$$= \deg f + \deg g + \deg h - 1 \leq 3 \deg f - 1$$

$\implies (N-3)\deg(f) \leq -1$ Contradiction if $N \geq 3$, $\deg f > 0$.

$\blacksquare$

Exercise: Catalan $f^m - g^n = 1$, $m, n \geq 2$, $f, g \notin \mathbb{C}$.

<u>The theorem of Langevin & Elkies</u>

$F(x,y) \in \mathbb{Z}[x,y]$ a homogeneous pol. of degree d.

$$F(x,y) = \sum_{\substack{i+j=d \\ i,j \geq 0}} a_{ij} x^i y^j, \quad a_{ij} \in \mathbb{Z}$$

<u>Thm.</u>: (The ABC conjecture implies)

Assume $F(x,y) \in \mathbb{Z}[x,y]$ has no repeated factors. Then for all $\varepsilon > 0$ $\exists C_{F,\varepsilon} > 0$ s.t $\forall$ coprime $(m,n) \in \mathbb{Z}^2$, $\gcd(m,n) = 1$ s.t $F(m,n) \neq 0$. $\operatorname{rad}(F(m,n)) \geq C_{F,\varepsilon} \cdot \max(|m|, |n|)^{\deg F - 2 - \varepsilon}$

Example: $F(x,y) = x \cdot y(x+y)$

$\mathrm{rad}(m \cdot n(m+n)) \gg \max(m,n)^{1-\varepsilon}$

$A = m$, $B = n$ $C = m+n$ $\mathrm{rad}(ABC) \gg C^{1-\varepsilon}$

$\Longrightarrow$ get ABC conj.

NB $F(x,y) = y^d f(x/y)$, $f \in \mathbb{Z}[t]$

(for example $xy(x+y) = y^3 \underbrace{\frac{x}{y}\left(\frac{x}{y}+1\right)}_{t(t+1) = f(t)}$

no repeated factors $\Leftrightarrow$ f has no repeated roots.

$F(x,y) = y^* \prod (x - \alpha_j y)$

We will use this to prove Roth's thm.

Louville's thm (1850)

α is a real algebraic number of degree d. Then

$\forall (m,n) \in \mathbb{Z}^2$, $m/n \neq \alpha$ $\left|\alpha - \frac{m}{n}\right| \geq \frac{c(\alpha)}{n^d}$, $c(\alpha) > 0$

$\alpha \in \mathbb{Q}$ is algebraic if $\exists f(t) \in \mathbb{Q}[t]$, $f \neq 0$ s.t $f(\alpha) = 0$.

Example:

$d = 1 \Longrightarrow \alpha = \frac{a}{b} \in \mathbb{Q}$.

$$\left|\alpha - \frac{m}{n}\right| = \left|\frac{a}{b} - \frac{m}{n}\right| = \frac{|an - bm|}{bn}$$

If $\alpha \neq \frac{m}{n}$, then $an - bm \neq 0$ but it is an integer so $|an-bm| \geq 1$

The set of all polynomials $f \in \mathbb{Q}[t]$ s.t $f(\alpha) = 0$ is an ideal in $\mathbb{Q}[t]$. Since $\mathbb{Q}[t]$ is a PID this ideal has a unique monic generator $f_\alpha(t)$. $\deg(\alpha) := \deg(f_\alpha)$

Ex.: $\alpha = a/b \in \mathbb{Q}$ the $f_\alpha(t) = t - a/b \in \mathbb{Q}[t]$ so $\deg \alpha = 1$

$\alpha = \sqrt{2}$, $f_{\sqrt{2}}(t) = t^2 - 2$ $\deg(\sqrt{2}) = 2$.

Construction:

Let $f_\alpha(t) \in \mathbb{Q}[t]$ be the minimal polynomial of α. Let

$$F(x,y) = a_0 y^d f_\alpha(x/y) \in \mathbb{Z}[x,y]$$

e.g. $f(t) = t^2 - 2$, $F(x,y) = x^2 - 2y^2$, $f(t) = t - 1/3$, $F(x,y) = 3x - y$

So we get a homegeneous pol. $F_\alpha(x,y) \in \mathbb{Z}[x,y]$ With no repeated factors (because $f_\alpha(t)$ is irreducible & hence has no repeated roots)

Lemma:

$$|F_\alpha(m,n)| \ll |n|^d \left|\alpha - \frac{m}{n}\right|$$

$d = \deg \alpha = \deg F_\alpha$

Assume the lemma. We find: if $\alpha \neq m/n$ then $F(m,n) \neq 0$, Because $F(m,n) = 0 \iff f(m/n) = 0 \iff t - m/n \mid f(t)$ impossible since $\alpha \neq \frac{m}{n}$.

$\implies |F(m,n)| \geq 1$ because $F(m,n) \in \mathbb{Z}$

Hence from lemma we find

$$1 \leq |F(m,n)| \ll |n|^d |\alpha - m/n|$$

$\iff |\alpha - \frac{m}{n}| \gg \frac{1}{n^d}$ Liouville's thm.

$\blacksquare$

Roth's Thm. (1950):

α real algebraic.

$$\forall \varepsilon > 0 \ \exists\, C(\alpha,\varepsilon) > 0 \text{ s.t } \forall \tfrac{m}{n} \neq \alpha \quad \left|\alpha - \frac{m}{n}\right| \geq \frac{C(\alpha,\varepsilon)}{n^{2+\varepsilon}}$$

Thue 1920's Improved Liouville, Then Siegel, then Dyson.

ABC $\Rightarrow$ Roth:

By Lemma, $n^d\left|\alpha - \frac{m}{n}\right| \gg |F(m,n)| \geq \operatorname{rad} F(m,n) \gg$

Fancy ABC $\gg \max(m,n)^{d-2-\varepsilon} \gg n^{d-2-\varepsilon}$ if $\left|\alpha - \frac{m}{n}\right| < 1$

$$\Rightarrow \left|\alpha - \frac{m}{n}\right| \underset{\alpha,\varepsilon}{\gg} \frac{1}{n^{2+\varepsilon}}$$

$\blacksquare$

NB: Liouville is sharp for $d=2$: it says $\left|\sqrt{2} - \frac{m}{n}\right| \gg \frac{1}{n^2}$

but if we take the continued fraction expansion of

$\sqrt{2} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots}}$ & truncate $\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$ then

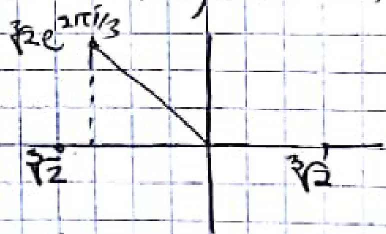
$$\left|\sqrt{2} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$

Application (Thue):

The equation $x^3 - 2y^3 = 1$ has only finitely many integer solutions.

$$1 = x^3 - 2y^3 = y^3\left(\left(\frac{x}{y}\right)^3 - 2\right) = y^3\left(\frac{x}{y} - \sqrt[3]{2}\right)\left(\frac{x}{y} - \sqrt[3]{2}e^{\frac{2\pi i}{3}}\right)\left(\frac{x}{y} - \sqrt[3]{2}e^{-\frac{2\pi i}{3}}\right)$$

$$1 \geq y^3\left|\frac{x}{y} - \sqrt[3]{2}\right| \cdot D^2, \quad D = \operatorname{Im}\left(\sqrt[3]{2}\, e^{2\pi i/3}\right)$$



$\Rightarrow \left|\sqrt[3]{2} - \frac{x}{y}\right| \ll \frac{1}{y^3}$ Contradicts Roth if $y \gg 1$

$$\frac{1}{y^3} \gg \left|\sqrt[3]{2} - \frac{x}{y}\right| \underset{\text{Roth}}{\gg} \frac{1}{y^{2+1/2}} \iff y^{1/2} \ll 1.$$

Pf of Lemma:

Factor $F(x,y) = c \cdot \prod(x - \alpha_j y) = c \cdot y^d \prod\left(\frac{x}{y} - \alpha_j\right)$

Assume $\left|\frac{m}{n} - \alpha_1\right| \leq \left|\frac{m}{n} - \alpha_j\right| \quad \forall j = 2, \dots, d$

$$\left|\frac{m}{n} - \alpha_2\right| \leq \left|\frac{m}{n} - \alpha_1\right| + |\alpha_1 - \alpha_2| \ll 2|\alpha_1 - \alpha_2|$$

So $F(m,n) = n^d\left|\alpha_1 - \frac{m}{n}\right| \prod_{j=2} \left|\alpha_j - \frac{m}{n}\right| \ll n^d\left|\alpha_1 - \frac{m}{n}\right|$

ABC $\Rightarrow$ "Mordell's conj."