10/13/04

Recalled Lemmas 1, 2.

Lemma 3. There is a constant K depending on a, b, c s.t. $h(2P) \geq 4h(P) - K \quad \forall P \in C(\mathbb{Q})$.

Overview of proof: 1. discard a finite # of pts. $\in C(\mathbb{Q})$.
2. Use duplication formula.
3. Reduce to a new Lemma 3'.

1. We can take K larger than $4h(P)$ $\forall$ pts in a finite set. Choose to ignore the set of points $\{P : 2P = \mathcal{O}\}$.

2. $P(x, y) \quad 2P = (\xi, \eta)$

Duplication formula: $\xi + 2x = \lambda^2 - a \qquad \lambda = \dfrac{f'(x)}{2y}$

$$\Rightarrow \quad \xi = \frac{[f'(x)]^2 - (8x + 4a) f(x)}{4} = \frac{x^4 + \ldots}{4x^3 + \ldots}$$

3. $h(P) = h(x) \qquad h(2P) = h(\xi)$ $\qquad$ $f(x), f'(x)$ have no common roots.

$h(\xi) \geq 4h(x) - K$.

Lemma 3' Let $\phi(x)$, $\psi(x)$ be poly with integer coefficients and no common complex roots. Let d be the max degree of ϕ and ψ.

a). There is a constant $R \geq 1$ depending on ϕ, ψ s.t. $\forall$ rational nos $\frac{m}{n}$, $\gcd\left(n^d \phi\left(\frac{m}{n}\right), n^d \psi\left(\frac{m}{n}\right)\right)$ divides R.

b. There are constants k_1, k_2 depending on ϕ, ψ, s.t.
$\forall$ rational numbers $\frac{m}{n}$ which are not roots of ψ,

$$\underbrace{d\,h\left(\tfrac{m}{n}\right) - k_1 \le h\left(\frac{\phi(\frac{m}{n})}{\psi(\frac{m}{n})}\right)} \le d\,h\left(\tfrac{m}{n}\right) + k_2 .$$

Will apply with.
$d = 4$
$\phi = x^4 + \dots$
$\psi = 4x^3 + \dots$

Proof of part (a)
NB. $\deg(\phi), \deg(\psi) \le d$.
$\therefore\ n^d \phi(\frac{m}{n}),\ n^d \psi(\frac{m}{n}) \in \mathbb{Z}$.

ϕ and ψ are interchangable.
w.l.o.g choose $\deg \phi = d$, $\deg \psi = e \le d$.

$$\Phi = n^d \phi\left(\tfrac{m}{n}\right) = a_0 m^d + a_1 m^{d-1} n + \dots + a_d n.$$
$$\Psi = n^d \psi\left(\tfrac{m}{n}\right) = b_0 m^e n^{d-e} + \dots + b_e n^d.$$

$\phi(x), \psi(x)$ have no common roots
i.e. relatively prime in the Euclidean ring $\mathbb{Q}[x]$.
ϕ, ψ generate a unit ideal.

$\Rightarrow \exists$ poly $F(x), G(x) \in \mathbb{Q}[x]$
s.t. $\boxed{F(x) \cdot \phi(x) + G(x) \cdot \psi(x) = 1}$ $\quad *$.

Let $A \in \mathbb{Z}$ s.t. A is large enough so that $AF(x)$, $AG(x)$ have integer coefficients.

Let D be $\max\{\deg F(x), \deg G(x)\}$.

<u>NB</u> A, D do not depend on m, n.

$x = \frac{m}{n}$. multiply by An^{D+d}.

$$n^D A F(x) \cdot n^d \phi\left(\tfrac{m}{n}\right) + n^D A G(x) \cdot n^d \psi(x) = An^{D+d}.$$

Let $\gamma(m,n)$ s.t. $\gamma = \gcd(\Phi, \Psi)$.

we want to show

$\exists\, R \geq 1$ s.t. $\gamma \mid R \quad \forall \frac{m}{n}$

$$\underbrace{n^D A\, F(x)}_{\text{integers}}\, \Phi + \underbrace{n^D A\, G(x)}_{\text{integers}}\, \Psi = An^{D+d}. \qquad (1)$$

From (1) we see that $\gamma \mid An^{D+d}$.

Plan: Will show: $\gamma \mid An^{D+d-1} a_0$

$\cdots\ \gamma \mid An^{D+d-2} a_0^2$

$\vdots$

$\gamma \mid Aa_0^{D+d}$

$\gamma \mid An^{D+d} \qquad \gamma \mid \Phi(m,n)$

$$\Rightarrow \gamma \mid An^{D+d-r}\,\Phi(m,n) = Aa_0 m^d n^{D+d-1} + Aa_1 m^d n^{D+d} + \dots + Aa_0 n^{D+2d-}$$

Every term except for the 1st contains An^{D+d}

$\therefore \quad \gamma \mid A a_0 m^d n^{D+d-1}$

so $\gamma \mid \gcd\left(An^{D+d},\ A a_0 m^d n^{D+d-1}\right) =$
$An^{D+d-1} \gcd(n, a_0 m^d)$.

but $(m,n) = 1$
$\Rightarrow \quad \gamma \mid An^{D+d-1} a_0.$

Using $\gamma \mid A a_0 n^{D+d-2}\, \Phi(m,n)$

$\Rightarrow \gamma \mid A a_0^2 n^{D+d-2}$ (Same steps)

$\vdots$

$\Rightarrow \gamma \mid A a_0^{D+d}$ $\square$

Overview of proof of b.

1. exclude a finite # of points.
2. want the height of $\xi = \dfrac{\Phi(\frac{m}{n})}{\Psi(\frac{m}{n})}$

$H(\xi) = \max\{\Phi, \Psi\}$ except for possible common factors.

3. From (a) $\exists$ R s.t. $H(\xi) \geq \frac{1}{R} \max\{\Phi, \Psi\}$.
$\geq \frac{1}{2R}\left(|n^d||\phi| + |n^d \psi|\right)$

4. Consider $\dfrac{H(\varphi)}{H(\frac{m}{n})^d} \geq \dfrac{1}{2R} \dfrac{(|\phi(\frac{m}{n})| + |\psi(\frac{m}{n})|)}{\max\{|\frac{m}{n}|^d, 1\}}.$

5. P is a function of a real variable t.

$$P(t) = \frac{|\phi(t)| + |\psi(t)|}{\max\{t^d, 1\}}$$

$\deg \phi, \psi \leq d \Rightarrow P(t)$ has a non zero limit as $t \to \infty$.

$$\lim_{t\to\infty} P = \begin{cases} |a_0| & \text{if } \deg \psi < d \\ |a_0| + |b_0| & \text{if } \deg \psi = d \end{cases}$$

Outside some closed interval P is bounded away from zero.
But inside a closed interval ~~we have a continuous~~
(e.g. closed set of real line)
continuous function on a compact set $\Rightarrow P$ ~~at~~tains its max and min.

min value of $P > 0$
$\exists$ a constant $C > 0$ s.t. $P(t) > C \quad \forall \ t \in \mathbb{R}$.

$\Rightarrow H(\varphi) \geq \frac{C}{2R} H(\frac{m}{n})^d$

$\Rightarrow h(\varphi) \geq d\, h(\frac{m}{n}) - K_1 \qquad K_1 = \log \frac{2R}{C}.$