Diversity in Parametric Families of Number Fields

Yuri Bilu, Florian Luca

Dynamics and Graphs over Finite Fields
March 30, 2016
Luminy

My co-author and some guy

Hilbert's Irreducibility Theorem

- X algebraic curve over $\mathbb{Q}$;
- $t \in \mathbb{Q}(X)$ non-constant rational function of degree $\nu \geq 2$;
- n stands for a positive integer.

Hilbert's Irreducibility Theorem *For infinitely many n the fiber $t^{-1}(n) \subset X(\bar{\mathbb{Q}})$ is $\mathbb{Q}$-irreducible;*

that is, the Galois group $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$ acts on $t^{-1}(n)$ transitively.

Hilbert's Irreducibility Theorem

- X algebraic curve over $\mathbb{Q}$;
- $t \in \mathbb{Q}(X)$ non-constant rational function of degree $\nu \geq 2$;
- n stands for a positive integer.

Hilbert's Irreducibility Theorem *For infinitely many n the fiber $t^{-1}(n) \subset X(\bar{\mathbb{Q}})$ is $\mathbb{Q}$-irreducible;*

that is, the Galois group $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$ acts on $t^{-1}(n)$ transitively.

Equivalently: *For every n pick*

$$P_n \in t^{-1}(n);$$

then for infinitely many n we have

$$[\mathbb{Q}(P_n) : \mathbb{Q}] = \nu.$$

Hilbert's Irreducibility Theorem

- X algebraic curve over $\mathbb{Q}$;
- $t \in \mathbb{Q}(X)$ non-constant rational function of degree $\nu \geq 2$;
- n stands for a positive integer.

Hilbert's Irreducibility Theorem *For infinitely many n the fiber $t^{-1}(n) \subset X(\bar{\mathbb{Q}})$ is $\mathbb{Q}$-irreducible;*

that is, the Galois group $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$ acts on $t^{-1}(n)$ transitively.

Equivalently: *For every n pick*

$$P_n \in t^{-1}(n);$$

then for infinitely many n we have

$$[\mathbb{Q}(P_n) : \mathbb{Q}] = \nu.$$

Quantitative version:

$$\left|\{n \leq N,\ [\mathbb{Q}(P_n) : \mathbb{Q}] < \nu\}\right| \ll N^{1/2}$$

Work of Dvornicich & Zannier

Hilbert's Irreducibility Theorem does not answer the following question:

Among the fields $\mathbb{Q}(P_n)$*, are there "many" distinct?*

Work of Dvornicich & Zannier

Hilbert's Irreducibility Theorem does not answer the following question:

Among the fields $\mathbb{Q}(P_n)$, are there "many" distinct?

Zannier (1998): let K be number field; then, under a suitable assumption, for any $\varepsilon > 0$

$$\left|\{n \leq N : K \subset \mathbb{Q}(P_n)\}\right| \ll_\varepsilon N^\varepsilon.$$

Work of Dvornicich & Zannier

Hilbert's Irreducibility Theorem does not answer the following question:

Among the fields $\mathbb{Q}(P_n)$, are there "many" distinct?

Zannier (1998): let K be number field; then, under a suitable assumption, for any $\varepsilon > 0$

$$\left|\{n \leq N : K \subset \mathbb{Q}(P_n)\}\right| \ll_{\varepsilon} N^{\varepsilon}.$$

Dvornicich & Zannier (1994): For large N

$$[\mathbb{Q}(P_1, \ldots, P_N) : \mathbb{Q}] \geq e^{cN/\log N}, \qquad c = c(\nu, \mathbf{g}) > 0.$$

Work of Dvornicich & Zannier

Hilbert's Irreducibility Theorem does not answer the following question:

Among the fields $\mathbb{Q}(P_n)$, are there "many" distinct?

Zannier (1998): let K be number field; then, under a suitable assumption, for any $\varepsilon > 0$

$$\left|\{n \leq N : K \subset \mathbb{Q}(P_n)\}\right| \ll_\varepsilon N^\varepsilon.$$

Dvornicich & Zannier (1994): For large N

$$[\mathbb{Q}(P_1, \ldots, P_N) : \mathbb{Q}] \geq e^{cN/\log N}, \qquad c = c(\nu, \mathbf{g}) > 0.$$

Corollary For large N

$$\left|\{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\}\right| \geq cN/\log N, \qquad c = c(\nu, \mathbf{g}) > 0.$$

Some Remarks

- Theorem of Dvornicich-Zannier is best possible:
  take X as the curve $t = u^2$; then

$$\mathbb{Q}(P_1, \dots, P_N) = \mathbb{Q}(\sqrt{1}, \sqrt{2}, \dots, \sqrt{N}) = \mathbb{Q}(\sqrt{p} : p \leq N),$$
$$[\mathbb{Q}(P_1, \dots, P_N) : \mathbb{Q}] = 2^{\pi(N)}.$$

Some Remarks

- Theorem of Dvornicich-Zannier is best possible:
  take X as the curve $t = u^2$; then

$$\mathbb{Q}(P_1, \ldots, P_N) = \mathbb{Q}(\sqrt{1}, \sqrt{2}, \ldots, \sqrt{N}) = \mathbb{Q}(\sqrt{p} : p \leq N),$$
$$[\mathbb{Q}(P_1, \ldots, P_N) : \mathbb{Q}] = 2^{\pi(N)}.$$

- The corollary does not look best possible:
  in the same example, if n runs the **square-free** numbers among $1, \ldots, N$ then the fields

$$\mathbb{Q}(P_n) = \mathbb{Q}(\sqrt{n})$$

  are pairwise distinct and there are $\approx \zeta(2)^{-1} N$ square-free numbers $n \leq N$.

Diversity Conjectures

Weak Diversity Conjecture

$$\left|\{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\}\right| \geq cN.$$

Diversity Conjectures

Weak Diversity Conjecture

$$\left|\{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\}\right| \geq cN.$$

- $P \in X(\bar{\mathbb{Q}})$ is a **ramification point** of t if $v_P(t - t(P)) > 1$;
- $\alpha \in \bar{\mathbb{Q}} \cup \{\infty\}$ is a **critical value** of t if $\alpha = t(P)$, where P is a ramification point.

Diversity Conjectures

Weak Diversity Conjecture

$$\big|\{\mathbb{Q}(P_1),\ldots,\mathbb{Q}(P_N)\}\big| \ge cN.$$

- $P \in X(\bar{\mathbb{Q}})$ is a **ramification point** of t if $v_P(t - t(P)) > 1$;
- $\alpha \in \bar{\mathbb{Q}} \cup \{\infty\}$ is a **critical value** of t if $\alpha = t(P)$, where P is a ramification point.

Strong Diversity Conjecture (Schinzel) Assume that

- either t has a finite critical value not belonging to $\mathbb{Q}$,
- or the field extension $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ is not abelian.

Then

$$[\mathbb{Q}(P_1,\ldots,P_N) : \mathbb{Q}] \ge e^{cN}.$$

Diversity Conjectures

Weak Diversity Conjecture

$$\left|\{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\}\right| \geq cN.$$

- $P \in X(\bar{\mathbb{Q}})$ is a **ramification point** of t if $v_P(t - t(P)) > 1$;
- $\alpha \in \bar{\mathbb{Q}} \cup \{\infty\}$ is a **critical value** of t if $\alpha = t(P)$, where P is a ramification point.

Strong Diversity Conjecture (Schinzel) Assume that

- either t has a finite critical value not belonging to $\mathbb{Q}$,
- or the field extension $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ is not abelian.

Then

$$[\mathbb{Q}(P_1, \ldots, P_N) : \mathbb{Q}] \geq e^{cN}.$$

Some Remarks

- The hypothesis in the Strong Conjecture is necessary.
  If $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ is abelian and the finite critical values are in $\mathbb{Q}$ then

  $$\mathbb{Q}(X) \subset L\left((t-\alpha_1)^{1/e_1}, \ldots, (t-\alpha_s)^{1/e_s}\right),$$

  where L is a number field, $\alpha_1, \ldots, \alpha_s \in \mathbb{Q}$.

Diversity Conjectures

Weak Diversity Conjecture

$$\left|\{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\}\right| \geq cN.$$

- $P \in X(\bar{\mathbb{Q}})$ is a **ramification point** of t if $v_P(t - t(P)) > 1$;
- $\alpha \in \bar{\mathbb{Q}} \cup \{\infty\}$ is a **critical value** of t if $\alpha = t(P)$, where P is a ramification point.

Strong Diversity Conjecture (Schinzel) Assume that

- either t has a finite critical value not belonging to $\mathbb{Q}$,
- or the field extension $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ is not abelian.

Then

$$[\mathbb{Q}(P_1, \ldots, P_N) : \mathbb{Q}] \geq e^{cN}.$$

Some Remarks

- The hypothesis in the Strong Conjecture is necessary.
  If $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ is abelian and the finite critical values are in $\mathbb{Q}$ then

  $$\mathbb{Q}(X) \subset L\left((t-\alpha_1)^{1/e_1}, \ldots, (t-\alpha_s)^{1/e_s}\right),$$

  where L is a number field, $\alpha_1, \ldots, \alpha_s \in \mathbb{Q}$.
- Strong Conjecture $\Rightarrow$ Weak Conjecture

Our Result

Dvornicich & Zannier: For large N

$$\left|\{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\}\right| \geq c\frac{N}{\log N}, \qquad c = c(\nu, \mathbf{g}) > 0.$$

Weak Diversity Conjecture

$$\left|\{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\}\right| \geq cN.$$

Our Result

Dvornicich & Zannier: For large N

$$\left|\{\mathbb{Q}(P_1),\dots,\mathbb{Q}(P_N)\}\right| \geq c\frac{N}{\log N}, \qquad c = c(\nu, \mathbf{g}) > 0.$$

Weak Diversity Conjecture

$$\left|\{\mathbb{Q}(P_1),\dots,\mathbb{Q}(P_N)\}\right| \geq cN.$$

Theorem (YuB, FL) (February 18, 2016) For large N

$$\left|\{\mathbb{Q}(P_1),\dots,\mathbb{Q}(P_N)\}\right| \geq \frac{N}{(\log N)^{1-\eta}}, \qquad \eta = \eta(\nu, \mathbf{g}) > 0.$$

Our Result

Dvornicich & Zannier: For large N

$$\left|\{\mathbb{Q}(P_1),\ldots,\mathbb{Q}(P_N)\}\right| \geq c\frac{N}{\log N}, \qquad c = c(\nu,\mathbf{g}) > 0.$$

Weak Diversity Conjecture

$$\left|\{\mathbb{Q}(P_1),\ldots,\mathbb{Q}(P_N)\}\right| \geq cN.$$

Theorem (YuB, FL) (February 18, 2016) For large N

$$\left|\{\mathbb{Q}(P_1),\ldots,\mathbb{Q}(P_N)\}\right| \geq \frac{N}{(\log N)^{1-\eta}}, \qquad \eta = \eta(\nu,\mathbf{g}) > 0.$$

$\eta = \dfrac{1}{10^6(\nu+\mathbf{g})\log(\nu+\mathbf{g})}$ would do.

The Argument of Dvornicich & Zannier

Traced back to Davenport, Lewis, Schinzel (1964)

Set-up

- $F(T) \in \mathbb{Z}[T]$ the primitive separable polynomial whose roots are the finite critical values of t;
- $1 \leq D = \deg F \leq 2\mathbf{g} - 2 + 2\nu$ (Riemann-Hurwitz)
- Δ_F the discriminant of F;
- $\mathcal{P}_F$ the set of $p \nmid \Delta_F$ for which $F(T)$ has a root mod p;
- $\mathcal{P}_F$ is of density $\delta_F > 0$ (Tchebotarev).
- In fact, $\delta_F \geq 1/D$ where $D = \deg F$.

The Argument of Dvornicich & Zannier

Traced back to Davenport, Lewis, Schinzel (1964)

Set-up

- $F(T) \in \mathbb{Z}[T]$ the primitive separable polynomial whose roots are the finite critical values of t;
- $1 \leq D = \deg F \leq 2\mathbf{g} - 2 + 2\nu$ (Riemann-Hurwitz)
- Δ_F the discriminant of F;
- $\mathcal{P}_F$ the set of $p \nmid \Delta_F$ for which $F(T)$ has a root mod p;
- $\mathcal{P}_F$ is of density $\delta_F > 0$ (Tchebotarev).
- In fact, $\delta_F \geq 1/D$ where $D = \deg F$.

Main Principles

(A) If p ramifies in $\mathbb{Q}(P)$ for some $P \in t^{-1}(n)$, then $p \mid F(n)$.

(B) For large p, if $p \parallel F(n)$ then p ramifies in $\mathbb{Q}(P)$ for some $P \in t^{-1}(n)$.

(C) For $p \nmid \Delta_F$

$$p^2 \mid F(n) \Rightarrow p \parallel F(n+p).$$

(D) For $p \in \mathcal{P}_F$ there is $n \leq 2p$ such that $p \parallel F(n)$.

(E) When n is large, $F(n)$ has at most D prime divisors $p \geq n/4$.

Primitives

Notation

- $K_n = \mathbb{Q}(t^{-1}(n))$
- p is primitive for n if p ramifies in K_n, but not in $K_1, \ldots, K_{n-1}$.

Consequences of (A–D):

(F) *Every large $p \in \mathcal{P}_F$ is primitive for some $n \leq 2p$.*

(G) *Every large n has at most D primitive $p \geq n/4$.*

In addition to this:

(H) If n **admits a primitive** p then $K_n \not\subset K_1 \cdots K_{n-1}$.

(I) If n admits a primitive p and $t^{-1}(n)$ **is irreducible** then $\mathbb{Q}(P_n) \not\subset \mathbb{Q}(P_1, \ldots, P_{n-1})$.

Proof of the Theorem of Dvornicich & Zannier

Notation

$S_N = \{n \text{ having a primitive } p \in [N/4, N/2]\}$,
$S'_N = \{n \in S_N : t^{-1}(n) \text{ is irreducible}\}$

- (F) $\Rightarrow S_N \subset [1, N]$
- (I) $\Rightarrow [\mathbb{Q}(P_1, \ldots, P_N) : \mathbb{Q}] \geq 2^{|S'_N|}$
- (D) and Tchebotarev $\Rightarrow$ for large N

$$|S_N| \geq \frac{1}{D}\left|\mathcal{P}_F \cap [N/4, N/2]\right| \gg \frac{N}{\log N}.$$

- Hilbert's Irreducibility Theorem $\Rightarrow |S_N \setminus S'_N| \ll N^{1/2}$;
- for large N

$$|S'_N| \gg \frac{N}{\log N}.$$

How to Generalize it?

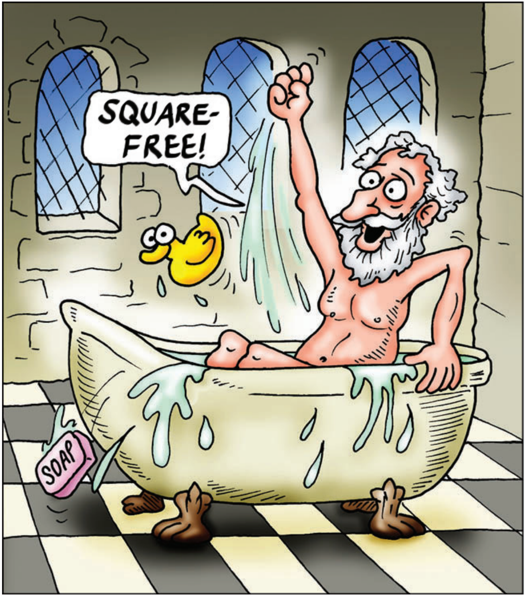
Dvornicich & Zannier: $[\mathbb{Q}(P_1, \dots, P_N) : \mathbb{Q}] \geq e^{cN/\log N}$

Corollary $\left|\{\mathbb{Q}(P_1), \dots, \mathbb{Q}(P_N)\}\right| \geq cN/\log N$

- **Theorem of Dvornicich-Zannier is best possible:** take X as the curve $t = u^2$; then

$$\mathbb{Q}(P_1, \dots, P_N) = \mathbb{Q}(\sqrt{1}, \sqrt{2}, \dots, \sqrt{N}) = \mathbb{Q}(\sqrt{p} : p \leq N),$$
$$[\mathbb{Q}(P_1, \dots, P_N) : \mathbb{Q}] = 2^{\pi(N)}.$$

- **The corollary does not look best possible:** in the same example, if n runs the square-free numbers among $1, \dots, N$ then the fields $\mathbb{Q}(P_n) = \mathbb{Q}(\sqrt{n})$ are pairwise distinct and there are $\approx \zeta(2)^{-1}N$ square-free numbers $n \leq N$.



To improve on the corollary, replace primes by square-free numbers!

Working with Square-Free Numbers

For a separable polynomial $F(T) \in \mathbb{Z}[T]$ we denote:

- Δ_F the discriminant of F;
- $\mathcal{P}_F$ the set of $p \nmid \Delta_F$ for which $F(T)$ has a root $\bmod p$;
- $\mathcal{M}_F$ the set of square-free integers composed of primes from $\mathcal{P}_F$;
- assume m square-free; we say $m \parallel n$ if $m \mid n$ and $\gcd(m, n/m) = 1$.

Working with Square-Free Numbers

For a separable polynomial $F(T) \in \mathbb{Z}[T]$ we denote:

- Δ_F the discriminant of F;
- $\mathcal{P}_F$ the set of $p \nmid \Delta_F$ for which $F(T)$ has a root mod p;
- $\mathcal{M}_F$ the set of square-free integers composed of primes from $\mathcal{P}_F$;
- assume m square-free; we say $m \parallel n$ if $m \mid n$ and $\gcd(m, n/m) = 1$.

Counting:

$$\left|\mathcal{M}_F \cap [0, x]\right| \sim \gamma \frac{x}{(\log x)^{1-\delta}}, \quad \delta = \delta_F, \quad \gamma > 0.$$

Working with Square-Free Numbers

For a separable polynomial $F(T) \in \mathbb{Z}[T]$ we denote:

- Δ_F the discriminant of F;
- $\mathcal{P}_F$ the set of $p \nmid \Delta_F$ for which $F(T)$ has a root $\bmod p$;
- $\mathcal{M}_F$ the set of square-free integers composed of primes from $\mathcal{P}_F$;
- assume m square-free; we say $m \parallel n$ if $m \mid n$ and $\gcd(m, n/m) = 1$.

Counting:

$$\left|\mathcal{M}_F \cap [0, x]\right| \sim \gamma \frac{x}{(\log x)^{1-\delta}}, \quad \delta = \delta_F, \quad \gamma > 0.$$

Need “square-free analogues” of the following of primes:

(D) For $p \in \mathcal{P}_F$ there is $n \le 2p$ such that $p \parallel F(n)$.

(E) When n is large, $F(n)$ has at most D prime divisors $p \ge n/4$.

Analogue of (D)

(D') Assume that every prime divisor of $m \in \mathcal{M}_F$ satisfies $p > \omega(m)$. Then there is $n \le (\omega(m)+1)m$ such that $m \,\|\, F(n)$.

Proof

- There is $n_0 \le m$ such that $m \mid F(n_0)$.
- Then $m \mid F(n_0 + km)$, $k = 0, 1, 2 \ldots$.
- Assume $m \nparallel F(n_0 + km)$ for $k = 0, 1, \ldots, \omega(m)$.

Analogue of (D)

(D') Assume that every prime divisor of $m \in \mathcal{M}_F$ satisfies $p > \omega(m)$. Then there is $n \le (\omega(m)+1)m$ such that $m \,\|\, F(n)$.

Proof

- There is $n_0 \le m$ such that $m \mid F(n_0)$.
- Then $m \mid F(n_0 + km)$, $k = 0, 1, 2 \ldots$.
- Assume $m \nparallel F(n_0 + km)$ for $k = 0, 1, \ldots, \omega(m)$.
- Box principle: there is $p \mid m$ such that

$$p^2 \mid F(n_0 + km), \quad p^2 \mid F(n_0 + \ell m)$$

  and $0 \le k < \ell \le \omega(m)$.
- Then $p \mid (\ell - k)\Delta_F$, contradiction because $p \nmid \Delta_F$ and $\ell - k \le \omega(m)$

Primitives

Call $m \in \mathcal{M}_F$ primitive for n if

- every $p \mid m$ ramifies in $\mathbb{Q}(t^{-1}(n))$;
- for every $p \mid m$ there is $n' < n$ such that p does not ramify in $\mathbb{Q}(t^{-1}(n'))$;

Property (D') from the previous slide implies:

(F') every $m \in \mathcal{M}_F$ with $p_{\min}(m) > \omega(m)$ serves as primitive for some $n = n_m \leq m(\omega(m) + 1)$.

Primitives

Call $m \in \mathcal{M}_F$ primitive for n if

- every $p \mid m$ ramifies in $\mathbb{Q}(t^{-1}(n))$;
- for every $p \mid m$ there is $n' < n$ such that p does not ramify in $\mathbb{Q}(t^{-1}(n'))$;

Property (D') from the previous slide implies:

(F') every $m \in \mathcal{M}_F$ with $p_{\min}(m) > \omega(m)$ serves as primitive for some $n = n_m \leq m(\omega(m) + 1)$.

What we do not have:

(G') a bound $\left|\{n_m\}\right|$ for a given m.

And this is because we do not have

(E') a bound for $\left|\{m \in \mathcal{M}_F : m \mid F(n)\}\right|$ for a given n.

And this is because distinct m are not coprime!

A Special Set of Square-Free Numbers

Fix $\varepsilon > 0$ and define for large x (x will replace N in the sequel):

$$\kappa = \log\log x, \qquad k = \lfloor \varepsilon\delta \log\log x \rfloor + 1,$$

$$\mathcal{M}_F(x) = \left\{ m \in \mathcal{M}_F : \begin{array}{c} \omega(m) = k+1, \\ p_{\min}(m) \geq e^{(\log x)^{1-\varepsilon}}, \\ p_{\max}(m) \geq x^{9/10} \end{array} \right\} \cap \left[\frac{x}{2\kappa}, \frac{x}{\kappa} \right].$$

Counting:

$$\left|\mathcal{M}_F(x)\right| = \frac{x}{(\log x)^{1-\varepsilon\delta+o(1)}} \quad (x \to \infty)$$

A Special Set of Square-Free Numbers

Fix $\varepsilon > 0$ and define for large x (x will replace N in the sequel):

$$\kappa = \log\log x, \qquad k = \lfloor \varepsilon\delta \log\log x \rfloor + 1,$$

$$\mathcal{M}_F(x) = \left\{ m \in \mathcal{M}_F : \begin{array}{c} \omega(m) = k+1, \\ p_{\min}(m) \geq e^{(\log x)^{1-\varepsilon}}, \\ p_{\max}(m) \geq x^{9/10} \end{array} \right\} \cap \left[\frac{x}{2\kappa}, \frac{x}{\kappa} \right].$$

Counting:

$$\left| \mathcal{M}_F(x) \right| = \frac{x}{(\log x)^{1-\varepsilon\delta+o(1)}} \quad (x \to \infty)$$

Distinct $m \in \mathcal{M}_F(x)$ are "almost" co-prime: $\gcd(m, m')$ "much smaller" than $\min\{m, m'\}$.

Using this, one proves:

(E') for "most" $n \leq x$

$$\left| \{ m \in \mathcal{M}_F(x) : m \mid F(n) \} \right| \leq 6D;$$

(G') A consequence: with suitably defined ε, for "most" $m \in \mathcal{M}_F(x)$ we have

$$\left| \{ n_m \} \right| \leq 6D.$$

Using the Primitives

For large x set

$$\mathcal{N}_F(x) = \{n_m : m \in \mathcal{M}_F(x)\},$$
$$\mathcal{N}'_F(x) = \{n \in \mathcal{N}_F(x) : t^{-1}(n) \text{ is irreducble}\}.$$

Then

$$|\mathcal{N}_F(x)| \geq \frac{1}{12D}|\mathcal{M}_F(x)| \geq \frac{x}{(\log x)^{1-\varepsilon\delta+o(1)}}$$

Like before:

$$\begin{aligned} \left|\{\mathbb{Q}(P_n) : n \leq x\}\right| &\geq \left|\mathcal{N}'_F(x)\right| \\ &\geq \left|\mathcal{N}_F(x)\right| - O(N^{1/2}) \\ &\geq \frac{x}{(\log x)^{1-\varepsilon\delta+o(1)}} \end{aligned}$$

as wanted.

Proving (E') and (G')

How one proves (E') and (G')?

(E') for "most" $n \le x$

$$\left|\{m \in \mathcal{M}_F(x) : m \mid F(n)\}\right| \le 6D;$$

(G') with suitably defined ε, for "most" $m \in \mathcal{M}_F(x)$ we have

$$\left|\{n_m\}\right| \le 6D.$$

Proving (E’) and (G’)

How one proves (E’) and (G’)?

(E’) for “most” $n \leq x$

$$\left|\{m \in \mathcal{M}_F(x) : m \mid F(n)\}\right| \leq 6D;$$

(G’) with suitably defined ε, for “most” $m \in \mathcal{M}_F(x)$ we have

$$\left|\{n_m\}\right| \leq 6D.$$

This guy will tell you!