Friable values of polynomials

Greg Martin
University of British Columbia

Second Canada-France Congress
Université du Québec à Montréal
June 4, 2008

Outline

1. Introduction
2. Bounds for friable values of polynomials
   - Very friable values of special polynomials
   - Somewhat friable values of general polynomials
   - Positive proportion of friable values
3. Conjecture for friable values of polynomials
   - Conjecture for prime values of polynomials
   - Implication for friable values of polynomials

Friable

Définition

- **friable**, *adjectif*

  sens: qui se réduit facilement en morceaux, en poudre

Friable

Définition

- **friable**, *adjectif*

  sens: qui se réduit facilement en morceaux, en poudre

Definition

- **friable**, *adjective*

  meaning: easily broken into small fragments or reduced to powder

Friable integers

Definition

$\Psi(x,y) = \#\{n \le x : p \mid n \implies p \le y\}$ is the number of integers up to x whose prime factors are all at most y.

Theorem

For a large range of x and y, $\Psi(x,y) \sim x\rho\big(\frac{\log x}{\log y}\big)$, where $\rho(u)$ is the "Dickman–de Bruijn rho-function".

Heuristic interpretation

A "randomly chosen" integer of size x has probability $\rho(u)$ of being $x^{1/u}$-friable.

- In this talk, think of $u = \log x/\log y$ as being bounded above, that is, $y \ge x^{\varepsilon}$ for some $\varepsilon > 0$.

Friable integers

Definition

$\Psi(x,y) = \#\{n \le x : p \mid n \implies p \le y\}$ is the number of integers up to x whose prime factors are all at most y.

Theorem

For a large range of x and y, $\Psi(x,y) \sim x\rho\big(\frac{\log x}{\log y}\big)$, where $\rho(u)$ is the "Dickman–de Bruijn rho-function".

Heuristic interpretation

A "randomly chosen" integer of size x has probability $\rho(u)$ of being $x^{1/u}$-friable.

- In this talk, think of $u = \log x/\log y$ as being bounded above, that is, $y \ge x^{\varepsilon}$ for some $\varepsilon > 0$.

Friable integers

Definition

$\Psi(x,y) = \#\{n \le x : p \mid n \implies p \le y\}$ is the number of integers up to x whose prime factors are all at most y.

Theorem

For a large range of x and y, $\Psi(x,y) \sim x\rho\left(\frac{\log x}{\log y}\right)$, where $\rho(u)$ is the "Dickman–de Bruijn rho-function".

Heuristic interpretation

A "randomly chosen" integer of size x has probability $\rho(u)$ of being $x^{1/u}$-friable.

- In this talk, think of $u = \log x / \log y$ as being bounded above, that is, $y \ge x^{\varepsilon}$ for some $\varepsilon > 0$.

Friable integers

Definition

$\Psi(x,y) = \#\{n \le x : p \mid n \implies p \le y\}$ is the number of integers up to x whose prime factors are all at most y.

Theorem

For a large range of x and y, $\Psi(x,y) \sim x\rho\big(\frac{\log x}{\log y}\big)$, where $\rho(u)$ is the "Dickman–de Bruijn rho-function".

Heuristic interpretation

A "randomly chosen" integer of size x has probability $\rho(u)$ of being $x^{1/u}$-friable.

- In this talk, think of $u = \log x/\log y$ as being bounded above, that is, $y \ge x^{\varepsilon}$ for some $\varepsilon > 0$.

The Dickman–de Bruijn ρ-function

Definition

$\rho(u)$ is the continuous solution of the differential-difference equation $u\rho'(u) = -\rho(u-1)$ for $u \geq 1$ that satisfies the initial condition $\rho(u) = 1$ for $0 \leq u \leq 1$.

Example

For $1 \leq u \leq 2$,

$$\rho'(u) = -\frac{\rho(u-1)}{u} = -\frac{1}{u} \implies \rho(u) = C - \log u.$$

Since $\rho(u) = 1$, we have $\rho(u) = 1 - \log u$ for $1 \leq u \leq 2$.

- Note that $\rho(u) = \frac{1}{2}$ when $u = \sqrt{e}$. Therefore the "median size" of the largest prime factor of n is $n^{1/\sqrt{e}}$.

The Dickman–de Bruijn ρ-function

Definition

$\rho(u)$ is the continuous solution of the differential-difference equation $u\rho'(u) = -\rho(u-1)$ for $u \geq 1$ that satisfies the initial condition $\rho(u) = 1$ for $0 \leq u \leq 1$.

Example

For $1 \leq u \leq 2$,

$$\rho'(u) = -\frac{\rho(u-1)}{u} = -\frac{1}{u} \implies \rho(u) = C - \log u.$$

Since $\rho(u) = 1$, we have $\rho(u) = 1 - \log u$ for $1 \leq u \leq 2$.

- Note that $\rho(u) = \frac{1}{2}$ when $u = \sqrt{e}$. Therefore the "median size" of the largest prime factor of n is $n^{1/\sqrt{e}}$.

The Dickman–de Bruijn ρ-function

Definition

$\rho(u)$ is the continuous solution of the differential-difference equation $u\rho'(u) = -\rho(u-1)$ for $u \geq 1$ that satisfies the initial condition $\rho(u) = 1$ for $0 \leq u \leq 1$.

Example

For $1 \leq u \leq 2$,

$$\rho'(u) = -\frac{\rho(u-1)}{u} = -\frac{1}{u} \implies \rho(u) = C - \log u.$$

Since $\rho(u) = 1$, we have $\rho(u) = 1 - \log u$ for $1 \leq u \leq 2$.

- Note that $\rho(u) = \frac{1}{2}$ when $u = \sqrt{e}$. Therefore the "median size" of the largest prime factor of n is $n^{1/\sqrt{e}}$.

Friable numbers among values of polynomials

Definition

$\Psi(F;x,y) = \#\{1 \le n \le x : p \mid F(n) \implies p \le y\}$ is the number of integers n up to x such that all the prime factors of $F(n)$ are all at most y.

- When $F(x)$ is a linear polynomial (friable numbers in arithmetic progressions), we have the same asymptotic formula $\Psi(F;x,y) \sim x\rho\left(\frac{\log x}{\log y}\right)$.
- Knowing the size of $\Psi(F;x,y)$ has applications to analyzing the running time of modern factoring algorithms (quadratic sieve, number field sieve).

Fundamental question

Are two arithmetic properties (in this case, friability and being the value of a polynomial) independent?

Friable numbers among values of polynomials

Definition

$\Psi(F;x,y) = \#\{1 \le n \le x : p \mid F(n) \implies p \le y\}$ is the number of integers n up to x such that all the prime factors of $F(n)$ are all at most y.

- When $F(x)$ is a linear polynomial (friable numbers in arithmetic progressions), we have the same asymptotic formula $\Psi(F;x,y) \sim x\rho\left(\frac{\log x}{\log y}\right)$.
- Knowing the size of $\Psi(F;x,y)$ has applications to analyzing the running time of modern factoring algorithms (quadratic sieve, number field sieve).

Fundamental question

Are two arithmetic properties (in this case, friability and being the value of a polynomial) independent?

Friable numbers among values of polynomials

Definition

$\Psi(F;x,y) = \#\{1 \le n \le x : p \mid F(n) \implies p \le y\}$ is the number of integers n up to x such that all the prime factors of $F(n)$ are all at most y.

- When $F(x)$ is a linear polynomial (friable numbers in arithmetic progressions), we have the same asymptotic formula $\Psi(F;x,y) \sim x\rho\left(\frac{\log x}{\log y}\right)$.
- Knowing the size of $\Psi(F;x,y)$ has applications to analyzing the running time of modern factoring algorithms (quadratic sieve, number field sieve).

Fundamental question

Are two arithmetic properties (in this case, friability and being the value of a polynomial) independent?

Friable numbers among values of polynomials

Definition

$\Psi(F;x,y) = \#\{1 \le n \le x : p \mid F(n) \implies p \le y\}$ is the number of integers n up to x such that all the prime factors of $F(n)$ are all at most y.

- When $F(x)$ is a linear polynomial (friable numbers in arithmetic progressions), we have the same asymptotic formula $\Psi(F;x,y) \sim x\rho\left(\frac{\log x}{\log y}\right)$.
- Knowing the size of $\Psi(F;x,y)$ has applications to analyzing the running time of modern factoring algorithms (quadratic sieve, number field sieve).

Fundamental question

Are two arithmetic properties (in this case, friability and being the value of a polynomial) independent?

How friable can values of special polynomials be?

- For binomials, there's a nice trick which yields:

Theorem (Schinzel, 1967)

For any nonzero integers A and B, any positive integer d, and any $\varepsilon > 0$, there are infinitely many numbers n for which $An^d + B$ is n^ε-friable.

- Balog and Wooley (1998), building on an idea of Eggleton and Selfridge, extended this result to products of binomials

$$\prod_{j=1}^{L} (A_j n^{d_j} + B_j),$$

which includes products of linear polynomials.

How friable can values of special polynomials be?

- For binomials, there's a nice trick which yields:

Theorem (Schinzel, 1967)

For any nonzero integers A and B, any positive integer d, and any $\varepsilon > 0$, there are infinitely many numbers n for which $An^d + B$ is n^ε-friable.

- Balog and Wooley (1998), building on an idea of Eggleton and Selfridge, extended this result to products of binomials

$$\prod_{j=1}^{L} (A_j n^{d_j} + B_j),$$

which includes products of linear polynomials.

Proof for an explicit binomial

Example

Let's show that for any $\varepsilon > 0$, there are infinitely many numbers n for which $F(n) = 3n^5 + 7$ is n^ε-friable.

Define $n_k = 3^{8k-1}7^{2k}$. Then

$$F(n_k) = 3^{5(8k-1)+1}7^{5(2k)} + 7 = -7\big((-3^4 7)^{10k-1} - 1\big)$$

factors into values of cyclotomic polynomials:

$$F(n_k) = -7 \prod_{m \mid (10k-1)} \Phi_m(-3^4 7).$$

- $\Phi_m(x) = \prod_{\substack{1 \le r \le m \\ (r,m)=1}} \big(x - e^{2\pi i r/m}\big)$
- Φ_m has integer coefficients and degree $\phi(m)$

Proof for an explicit binomial

Example

Let's show that for any $\varepsilon > 0$, there are infinitely many numbers n for which $F(n) = 3n^5 + 7$ is n^ε-friable.

Define $n_k = 3^{8k-1}7^{2k}$. Then

$$F(n_k) = 3^{5(8k-1)+1}7^{5(2k)} + 7 = -7\big((-3^4 7)^{10k-1} - 1\big)$$

factors into values of cyclotomic polynomials:

$$F(n_k) = -7 \prod_{m \mid (10k-1)} \Phi_m(-3^4 7).$$

- $\Phi_m(x) = \prod_{\substack{1 \le r \le m \\ (r,m)=1}} \big(x - e^{2\pi i r/m}\big)$
- Φ_m has integer coefficients and degree $\phi(m)$

Proof for an explicit binomial

Example

Let's show that for any $\varepsilon > 0$, there are infinitely many numbers n for which $F(n) = 3n^5 + 7$ is n^ε-friable.

Define $n_k = 3^{8k-1}7^{2k}$. Then

$$F(n_k) = 3^{5(8k-1)+1}7^{5(2k)} + 7 = -7\big((-3^4 7)^{10k-1} - 1\big)$$

factors into values of cyclotomic polynomials:

$$F(n_k) = -7 \prod_{m \mid (10k-1)} \Phi_m(-3^4 7).$$

- $\Phi_m(x) = \prod_{\substack{1 \le r \le m \\ (r,m)=1}} \big(x - e^{2\pi i r/m}\big)$
- Φ_m has integer coefficients and degree $\phi(m)$

Proof for an explicit binomial

Example

Let's show that for any $\varepsilon > 0$, there are infinitely many numbers n for which $F(n) = 3n^5 + 7$ is n^ε-friable.

Define $n_k = 3^{8k-1}7^{2k}$. Then

$$F(n_k) = 3^{5(8k-1)+1}7^{5(2k)} + 7 = -7\big((-3^4 7)^{10k-1} - 1\big)$$

factors into values of cyclotomic polynomials:

$$F(n_k) = -7 \prod_{m \mid (10k-1)} \Phi_m(-3^4 7).$$

- $\Phi_m(x) = \prod_{\substack{1 \le r \le m \\ (r,m)=1}} \big(x - e^{2\pi i r/m}\big)$
- Φ_m has integer coefficients and degree $\phi(m)$

Proof for an explicit binomial

Example

Let's show that for any $\varepsilon > 0$, there are infinitely many numbers n for which $F(n) = 3n^5 + 7$ is n^ε-friable.

Define $n_k = 3^{8k-1}7^{2k}$. Then

$$F(n_k) = 3^{5(8k-1)+1}7^{5(2k)} + 7 = -7\big((-3^4 7)^{10k-1} - 1\big)$$

factors into values of cyclotomic polynomials:

$$F(n_k) = -7 \prod_{m \mid (10k-1)} \Phi_m(-3^4 7).$$

- $\Phi_m(x) = \prod_{\substack{1 \le r \le m \\ (r,m)=1}} \big(x - e^{2\pi i r/m}\big)$
- Φ_m has integer coefficients and degree $\phi(m)$

From the last slide

- $F(n) = 3n^5 + 7$
- $n_k = 3^{8k-1}7^{2k}$
- $F(n_k) = -7 \prod_{m|(10k-1)} \Phi_m(-3^4 7)$

- the primes dividing $F(n_k)$ are at most $\max_{m|(10k-1)} \left|\Phi_m(-3^4 7)\right|$
- each $\Phi_m(x)$ is roughly $|x|^{\phi(m)} \le |x|^{\phi(10k-1)}$
- n_k is roughly $(3^4 7)^{4k}$, but the largest prime factor of $F(n_k)$ is bounded by roughly $(3^4 7)^{\phi(10k-1)}$
- there are infinitely many k with $\phi(10k-1)/4k < \varepsilon$

Drawbacks

- Only works for special polynomials.
- Among the inputs $n \le x$, this construction yields only $O(\log x)$ values $F(n)$ that are n^{ε}-friable.

From the last slide

- $F(n) = 3n^5 + 7$
- $n_k = 3^{8k-1}7^{2k}$
- $F(n_k) = -7 \prod_{m|(10k-1)} \Phi_m(-3^4 7)$

- the primes dividing $F(n_k)$ are at most $\max_{m|(10k-1)} \left|\Phi_m(-3^4 7)\right|$
- each $\Phi_m(x)$ is roughly $|x|^{\phi(m)} \le |x|^{\phi(10k-1)}$
- n_k is roughly $(3^4 7)^{4k}$, but the largest prime factor of $F(n_k)$ is bounded by roughly $(3^4 7)^{\phi(10k-1)}$
- there are infinitely many k with $\phi(10k-1)/4k < \varepsilon$

Drawbacks

- Only works for special polynomials.
- Among the inputs $n \le x$, this construction yields only $O(\log x)$ values $F(n)$ that are n^{ε}-friable.

From the last slide

- $F(n) = 3n^5 + 7$
- $n_k = 3^{8k-1}7^{2k}$
- $F(n_k) = -7 \prod_{m|(10k-1)} \Phi_m(-3^4 7)$

- the primes dividing $F(n_k)$ are at most $\max_{m|(10k-1)} \left|\Phi_m(-3^4 7)\right|$
- each $\Phi_m(x)$ is roughly $|x|^{\phi(m)} \le |x|^{\phi(10k-1)}$
- n_k is roughly $(3^4 7)^{4k}$, but the largest prime factor of $F(n_k)$ is bounded by roughly $(3^4 7)^{\phi(10k-1)}$
- there are infinitely many k with $\phi(10k-1)/4k < \varepsilon$

Drawbacks

- Only works for special polynomials.
- Among the inputs $n \le x$, this construction yields only $O(\log x)$ values $F(n)$ that are n^{ε}-friable.

From the last slide

- $F(n) = 3n^5 + 7$
- $n_k = 3^{8k-1}7^{2k}$
- $F(n_k) = -7 \prod_{m|(10k-1)} \Phi_m(-3^4 7)$

- the primes dividing $F(n_k)$ are at most $\max_{m|(10k-1)} \left|\Phi_m(-3^4 7)\right|$
- each $\Phi_m(x)$ is roughly $|x|^{\phi(m)} \le |x|^{\phi(10k-1)}$
- n_k is roughly $(3^4 7)^{4k}$, but the largest prime factor of $F(n_k)$ is bounded by roughly $(3^4 7)^{\phi(10k-1)}$
- there are infinitely many k with $\phi(10k-1)/4k < \varepsilon$

Drawbacks

- Only works for special polynomials.
- Among the inputs $n \le x$, this construction yields only $O(\log x)$ values $F(n)$ that are n^{ε}-friable.

From the last slide

- $F(n) = 3n^5 + 7$
- $n_k = 3^{8k-1}7^{2k}$
- $F(n_k) = -7 \prod_{m|(10k-1)} \Phi_m(-3^4 7)$

- the primes dividing $F(n_k)$ are at most $\max_{m|(10k-1)} \left|\Phi_m(-3^4 7)\right|$
- each $\Phi_m(x)$ is roughly $|x|^{\phi(m)} \le |x|^{\phi(10k-1)}$
- n_k is roughly $(3^4 7)^{4k}$, but the largest prime factor of $F(n_k)$ is bounded by roughly $(3^4 7)^{\phi(10k-1)}$
- there are infinitely many k with $\phi(10k-1)/4k < \varepsilon$

Drawbacks

- Only works for special polynomials.
- Among the inputs $n \le x$, this construction yields only $O(\log x)$ values $F(n)$ that are n^ε-friable.

Polynomial factorizations

Example

The polynomial $F(x+F(x))$ is always divisible by $F(x)$. In particular, if $\deg F = d$, then $F(x+F(x))$ is roughly x^{d^2} yet is automatically roughly x^{d^2-d}-friable.

Mnemonic

$$F\big(x+F(x)\big) \equiv F(x) \equiv 0 \pmod{F(x)}$$

Cool special case

- If $F(x)$ is quadratic with leading coefficient a, then

$$F(x+F(x)) = F(x)\cdot aF\big(x+\tfrac{1}{a}\big).$$

- So if $F(x) = x^2+bx+c$, then $F(x+F(x)) = F(x)F(x+1)$.

Polynomial factorizations

Example

The polynomial $F(x+F(x))$ is always divisible by $F(x)$. In particular, if $\deg F = d$, then $F(x+F(x))$ is roughly x^{d^2} yet is automatically roughly x^{d^2-d}-friable.

Mnemonic

$$F\big(x+F(x)\big) \equiv F(x) \equiv 0 \pmod{F(x)}$$

Cool special case

- If $F(x)$ is quadratic with leading coefficient a, then

$$F(x+F(x)) = F(x)\cdot aF\big(x+\tfrac{1}{a}\big).$$

- So if $F(x) = x^2+bx+c$, then $F(x+F(x)) = F(x)F(x+1)$.

Polynomial factorizations

Example

The polynomial $F(x+F(x))$ is always divisible by $F(x)$. In particular, if $\deg F = d$, then $F(x+F(x))$ is roughly x^{d^2} yet is automatically roughly x^{d^2-d}-friable.

Mnemonic

$$F\big(x+F(x)\big) \equiv F(x) \equiv 0 \pmod{F(x)}$$

Cool special case

- If $F(x)$ is quadratic with leading coefficient a, then

$$F(x+F(x)) = F(x)\cdot aF\big(x+\tfrac{1}{a}\big).$$

- So if $F(x) = x^2+bx+c$, then $F(x+F(x)) = F(x)F(x+1)$.

A refinement of Schinzel

- Idea: use the reciprocal polynomial $x^d F(1/x)$.

Proposition

Let $h(x)$ be a polynomial such that $xh(x) - 1$ is divisible by $x^d F(1/x)$. Then $F(h(x))$ is divisible by $x^d F(1/x)$. In particular, we can take $\deg h = d - 1$, in which case $F(h(x))$ is roughly x^{d^2-d} yet is automatically roughly x^{d^2-2d}-friable.

Note: The proposition isn't true for $d = 2$, since the leftover "factor" of degree $2^2 - 2 \cdot 2 = 0$ is a constant.

Mnemonic

$$F(h(x)) \equiv F(1/x) \equiv 0 \pmod{F(1/x)}$$

A refinement of Schinzel

- Idea: use the reciprocal polynomial $x^d F(1/x)$.

Proposition

Let $h(x)$ be a polynomial such that $xh(x) - 1$ is divisible by $x^d F(1/x)$. Then $F(h(x))$ is divisible by $x^d F(1/x)$. In particular, we can take $\deg h = d - 1$, in which case $F(h(x))$ is roughly x^{d^2-d} yet is automatically roughly x^{d^2-2d}-friable.

Note: The proposition isn't true for $d = 2$, since the leftover "factor" of degree $2^2 - 2 \cdot 2 = 0$ is a constant.

Mnemonic

$$F(h(x)) \equiv F(1/x) \equiv 0 \pmod{F(1/x)}$$

A refinement of Schinzel

- Idea: use the reciprocal polynomial $x^d F(1/x)$.

Proposition

Let $h(x)$ be a polynomial such that $xh(x) - 1$ is divisible by $x^d F(1/x)$. Then $F(h(x))$ is divisible by $x^d F(1/x)$. In particular, we can take $\deg h = d - 1$, in which case $F(h(x))$ is roughly x^{d^2-d} yet is automatically roughly x^{d^2-2d}-friable.

Note: The proposition isn't true for $d = 2$, since the leftover "factor" of degree $2^2 - 2 \cdot 2 = 0$ is a constant.

Mnemonic

$$F(h(x)) \equiv F(1/x) \equiv 0 \pmod{F(1/x)}$$

A refinement of Schinzel

- Idea: use the reciprocal polynomial $x^d F(1/x)$.

Proposition

Let $h(x)$ be a polynomial such that $xh(x) - 1$ is divisible by $x^d F(1/x)$. Then $F(h(x))$ is divisible by $x^d F(1/x)$. In particular, we can take $\deg h = d - 1$, in which case $F(h(x))$ is roughly x^{d^2-d} yet is automatically roughly x^{d^2-2d}-friable.

Note: The proposition isn't true for $d = 2$, since the leftover "factor" of degree $2^2 - 2 \cdot 2 = 0$ is a constant.

Mnemonic

$$F(h(x)) \equiv F(1/x) \equiv 0 \pmod{F(1/x)}$$

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(D_3(D_7)) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\big(x + F(x) + F\big(x + F(x)\big)\big) = F(x) \cdot aF\Big(x + \tfrac{1}{a}\Big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(D_3(D_7)) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\big(x + F(x) + F\big(x + F(x)\big)\big) = F(x) \cdot aF\Big(x + \tfrac{1}{a}\Big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(\,D_3(D_7)\,) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\big(x + F(x) + F\big(x + F(x)\big)\big) = F(x) \cdot aF\big(x + \tfrac{1}{a}\big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(\,D_3(D_7)\,) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\big(x + F(x) + F\big(x + F(x)\big)\big) = F(x) \cdot aF\big(x + \tfrac{1}{a}\big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(\quad D_{21} \quad) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\big(x + F(x) + F\big(x + F(x)\big)\big) = F(x) \cdot aF\big(x + \tfrac{1}{a}\big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(\quad D_{21} \quad) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\big(x + F(x) + F\big(x + F(x)\big)\big) = F(x) \cdot aF\big(x + \tfrac{1}{a}\big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(\quad D_{21} \quad) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\big(x + F(x) + F\big(x + F(x)\big)\big) = F(x) \cdot aF\Big(x + \tfrac{1}{a}\Big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(\quad D_{21} \quad) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\Big(x + F(x) + F\Big(x + F(x)\Big)\Big) = F(x) \cdot aF\Big(x + \tfrac{1}{a}\Big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

Recursively use Schinzel's construction

- Let D_m denote an unspecified polynomial of degree m.
- Schinzel's construction: if $\deg F = d$, we can find D_{d-1} such that $F(D_{d-1}) = D_d D_{d(d-2)}$.

Example: $\deg F(x) = 4$

Use Schinzel's construction repeatedly:

$D_{12} = F(D_3) = D_4 D_8$ "score" = 8/3

$D_{84} = F(\quad D_{21} \quad) = D_{28} D_8 D_{48}$ "score" = 48/21

$D_{3984} = F(D_{987}) = D_{1316} D_{376} D_{48} D_{2208}$ "score" = 2208/987

- For $\deg F = 2$, begin with $F(D_4) = D_2 D_2 D_4$. Specifically,

$$F\Big(x + F(x) + F\Big(x + F(x)\Big)\Big) = F(x) \cdot aF\Big(x + \tfrac{1}{a}\Big) \cdot D_4.$$

- For $\deg F = 3$, begin with $F(D_4) = D_3 D_3 D_6$.

How friable can values of general polynomials be?

- For $d \ge 4$, define $s(d) = d \prod_{j=1}^{\infty} \left(1 - \frac{1}{u_j(d)}\right)$, where $u_1(d) = d - 1$ and $u_{j+1}(d) = u_j(d)^2 - 2$
- Define $s(2) = s(4)/4$ and $s(3) = s(6)/4$

Theorem (Schinzel, 1967)

Given a polynomial $F(x)$ of degree $d \ge 2$, there are infinitely many numbers n for which $F(n)$ is $n^{s(d)}$-friable.

$F(n)$	$s(d)$	$F(n)$	$s(d)$
degree 1	ε	degree 5	3.46410
degree 2	0.55902	degree 6	4.58258
degree 3	1.14564	degree 7	5.65685
degree 4	2.23607	degree d	$\approx d - 1 - 2/d$

How friable can values of general polynomials be?

- For $d \ge 4$, define $s(d) = d \prod_{j=1}^{\infty} \left(1 - \frac{1}{u_j(d)}\right)$, where $u_1(d) = d - 1$ and $u_{j+1}(d) = u_j(d)^2 - 2$
- Define $s(2) = s(4)/4$ and $s(3) = s(6)/4$

Theorem (Schinzel, 1967)

Given a polynomial $F(x)$ of degree $d \ge 2$, there are infinitely many numbers n for which $F(n)$ is $n^{s(d)}$-friable.

$F(n)$	$s(d)$	$F(n)$	$s(d)$
degree 1	ε	degree 5	3.46410
degree 2	0.55902	degree 6	4.58258
degree 3	1.14564	degree 7	5.65685
degree 4	2.23607	degree d	$\approx d - 1 - 2/d$

How friable can values of general polynomials be?

- For $d \ge 4$, define $s(d) = d \prod_{j=1}^{\infty} \left(1 - \frac{1}{u_j(d)}\right)$, where $u_1(d) = d - 1$ and $u_{j+1}(d) = u_j(d)^2 - 2$
- Define $s(2) = s(4)/4$ and $s(3) = s(6)/4$

Theorem (Schinzel, 1967)

Given a polynomial $F(x)$ of degree $d \ge 2$, there are infinitely many numbers n for which $F(n)$ is $n^{s(d)}$-friable.

$F(n)$	$s(d)$	$F(n)$	$s(d)$
degree 1	ε	degree 5	3.46410
degree 2	0.55902	degree 6	4.58258
degree 3	1.14564	degree 7	5.65685
degree 4	2.23607	degree d	$\approx d - 1 - 2/d$

How friable can values of general polynomials be?

- For $d \ge 4$, define $s(d) = d \prod_{j=1}^{\infty} \left(1 - \frac{1}{u_j(d)}\right)$, where $u_1(d) = d - 1$ and $u_{j+1}(d) = u_j(d)^2 - 2$
- Define $s(2) = s(4)/4$ and $s(3) = s(6)/4$

Theorem (Schinzel, 1967)

Given a polynomial $F(x)$ of degree $d \ge 2$, there are infinitely many numbers n for which $F(n)$ is $n^{s(d)}$-friable.

$F(n)$	$s(d)$	$F(n)$	$s(d)$
degree 1	ε	degree 5	3.46410
degree 2	0.55902	degree 6	4.58258
degree 3	1.14564	degree 7	5.65685
degree 4	2.23607	degree d	$\approx d - 1 - 2/d$

Polynomial substitution yields few friable values

Special case

Given a quadratic polynomial $F(x)$, there are infinitely many numbers n for which $F(n)$ is $n^{0.55902}$-friable.

Example

To obtain n for which $F(n)$ is $n^{0.56}$-friable:

$$D_{168} = F(D_{84}) = D_{42}D_{42}D_{28}D_8D_{48} \qquad \text{“score”} = 48/84 > 0.56$$
$$D_{7896} = F(D_{3948}) \qquad \text{“score”} = 2208/3948$$
$$= D_{1974}D_{1974}D_{1316}D_{376}D_{48}D_{2208} \qquad < 0.56$$

The counting function of such n is about $x^{1/3948}$.

“Improvement” Balog, M., Wooley can obtain $x^{2/3948}$ and an analogous improvement for $\deg F = 3$.

Polynomial substitution yields few friable values

Special case

Given a quadratic polynomial $F(x)$, there are infinitely many numbers n for which $F(n)$ is $n^{0.55902}$-friable.

Example

To obtain n for which $F(n)$ is $n^{0.56}$-friable:

$D_{168} = F(D_{84}) = D_{42}D_{42}D_{28}D_8D_{48}$ "score" $= 48/84 > 0.56$

$D_{7896} = F(D_{3948})$ "score" $= 2208/3948$

$= D_{1974}D_{1974}D_{1316}D_{376}D_{48}D_{2208}$ < 0.56

The counting function of such n is about $x^{1/3948}$.

"Improvement" Balog, M., Wooley can obtain $x^{2/3948}$ and an analogous improvement for $\deg F = 3$.

Polynomial substitution yields few friable values

Special case

Given a quadratic polynomial $F(x)$, there are infinitely many numbers n for which $F(n)$ is $n^{0.55902}$-friable.

Example

To obtain n for which $F(n)$ is $n^{0.56}$-friable:

$$D_{168} = F(D_{84}) = D_{42}D_{42}D_{28}D_{8}D_{48} \qquad \text{“score”} = 48/84 > 0.56$$
$$D_{7896} = F(D_{3948}) \qquad \text{“score”} = 2208/3948$$
$$= D_{1974}D_{1974}D_{1316}D_{376}D_{48}D_{2208} \qquad < 0.56$$

The counting function of such n is about $x^{1/3948}$.

“Improvement” Balog, M., Wooley can obtain $x^{2/3948}$ and an analogous improvement for $\deg F = 3$.

Polynomial substitution yields few friable values

Special case

Given a quadratic polynomial $F(x)$, there are infinitely many numbers n for which $F(n)$ is $n^{0.55902}$-friable.

Example

To obtain n for which $F(n)$ is $n^{0.56}$-friable:

$$D_{168} = F(D_{84}) = D_{42}D_{42}D_{28}D_8D_{48} \qquad \text{“score”} = 48/84 > 0.56$$
$$D_{7896} = F(D_{3948}) \qquad \text{“score”} = 2208/3948$$
$$= D_{1974}D_{1974}D_{1316}D_{376}D_{48}D_{2208} \qquad < 0.56$$

The counting function of such n is about $x^{1/3948}$.

“Improvement” Balog, M., Wooley can obtain $x^{2/3948}$ and an analogous improvement for $\deg F = 3$.

Polynomial substitution yields few friable values

Special case

Given a quadratic polynomial $F(x)$, there are infinitely many numbers n for which $F(n)$ is $n^{0.55902}$-friable.

Example

To obtain n for which $F(n)$ is $n^{0.56}$-friable:

$$D_{168} = F(D_{84}) = D_{42}D_{42}D_{28}D_8D_{48} \qquad \text{“score”} = 48/84 > 0.56$$
$$D_{7896} = F(D_{3948}) \qquad \text{“score”} = 2208/3948$$
$$= D_{1974}D_{1974}D_{1316}D_{376}D_{48}D_{2208} \qquad < 0.56$$

The counting function of such n is about $x^{1/3948}$.

“Improvement” Balog, M., Wooley can obtain $x^{2/3948}$ and an analogous improvement for $\deg F = 3$.

Can we have lots of friable values?

Our expectation

For any $\varepsilon > 0$, a positive proportion of values $F(n)$ are n^ε-friable.

At the turn of the millenium, we knew this for:

- linear polynomials (arithmetic progressions)
- Hildebrand (1985), then Balog and Ruzsa (1995): $F(n) = n(an + b)$
- Hildebrand (1989): $F(n) = (n+1)\cdots(n+L)$, positive proportion of values n^β-friable for $\beta > e^{-1/(L-1)}$

  Note: $\rho(e^{-1/L}) = 1 - \frac{1}{L}$, so $\beta \le e^{-1/L}$ is nontrivial
- Dartyge (1996): $F(n) = n^2 + 1$, positive proportion of values n^β-friable for $\beta > 149/179$

Can we have lots of friable values?

Our expectation

For any $\varepsilon > 0$, a positive proportion of values $F(n)$ are n^ε-friable.

At the turn of the millenium, we knew this for:

- linear polynomials (arithmetic progressions)
- Hildebrand (1985), then Balog and Ruzsa (1995): $F(n) = n(an+b)$
- Hildebrand (1989): $F(n) = (n+1)\cdots(n+L)$, positive proportion of values n^β-friable for $\beta > e^{-1/(L-1)}$

  Note: $\rho(e^{-1/L}) = 1 - \frac{1}{L}$, so $\beta \le e^{-1/L}$ is nontrivial
- Dartyge (1996): $F(n) = n^2 + 1$, positive proportion of values n^β-friable for $\beta > 149/179$

Can we have lots of friable values?

Our expectation

For any $\varepsilon > 0$, a positive proportion of values $F(n)$ are n^ε-friable.

At the turn of the millenium, we knew this for:

- linear polynomials (arithmetic progressions)
- Hildebrand (1985), then Balog and Ruzsa (1995): $F(n) = n(an+b)$
- Hildebrand (1989): $F(n) = (n+1)\cdots(n+L)$, positive proportion of values n^β-friable for $\beta > e^{-1/(L-1)}$

  Note: $\rho(e^{-1/L}) = 1 - \frac{1}{L}$, so $\beta \le e^{-1/L}$ is nontrivial
- Dartyge (1996): $F(n) = n^2 + 1$, positive proportion of values n^β-friable for $\beta > 149/179$

Can we have lots of friable values?

Our expectation

For any $\varepsilon > 0$, a positive proportion of values $F(n)$ are n^ε-friable.

At the turn of the millenium, we knew this for:

- linear polynomials (arithmetic progressions)
- Hildebrand (1985), then Balog and Ruzsa (1995): $F(n) = n(an + b)$
- Hildebrand (1989): $F(n) = (n+1)\cdots(n+L)$, positive proportion of values n^β-friable for $\beta > e^{-1/(L-1)}$

  Note: $\rho(e^{-1/L}) = 1 - \frac{1}{L}$, so $\beta \le e^{-1/L}$ is nontrivial
- Dartyge (1996): $F(n) = n^2 + 1$, positive proportion of values n^β-friable for $\beta > 149/179$

Can we have lots of friable values?

Our expectation

For any $\varepsilon > 0$, a positive proportion of values $F(n)$ are n^ε-friable.

At the turn of the millenium, we knew this for:

- linear polynomials (arithmetic progressions)
- Hildebrand (1985), then Balog and Ruzsa (1995): $F(n) = n(an + b)$
- Hildebrand (1989): $F(n) = (n+1)\cdots(n+L)$, positive proportion of values n^β-friable for $\beta > e^{-1/(L-1)}$

  Note: $\rho(e^{-1/L}) = 1 - \frac{1}{L}$, so $\beta \le e^{-1/L}$ is nontrivial
- Dartyge (1996): $F(n) = n^2 + 1$, positive proportion of values n^β-friable for $\beta > 149/179$

Theorem (Dartyge, M., Tenenbaum, 2001)

Let $F(x)$ be the product of K distinct irreducible polynomials of degree d. Then for any $\varepsilon > 0$, a positive proportion of values $F(n)$ are $n^{d-1/K+\varepsilon}$-friable.

- Anything better than n^d-friable is nontrivial.

No loss of generality

When the friability level exceeds n^{d-1}, only irreducible factors of degree at least d matter. Therefore the theorem also holds if $F(x)$ has K distinct irreducible factors of degree d and any number of irreducible factors of degree less than d.

Theorem (Dartyge, M., Tenenbaum, 2001)

Let $F(x)$ be the product of K distinct irreducible polynomials of degree d. Then for any $\varepsilon > 0$, a positive proportion of values $F(n)$ are $n^{d-1/K+\varepsilon}$-friable.

- Anything better than n^d-friable is nontrivial.

No loss of generality

When the friability level exceeds n^{d-1}, only irreducible factors of degree at least d matter. Therefore the theorem also holds if $F(x)$ has K distinct irreducible factors of degree d and any number of irreducible factors of degree less than d.

Theorem (Dartyge, M., Tenenbaum, 2001)

Let $F(x)$ be the product of K distinct irreducible polynomials of degree d. Then for any $\varepsilon > 0$, a positive proportion of values $F(n)$ are $n^{d-1/K+\varepsilon}$-friable.

- Anything better than n^d-friable is nontrivial.

No loss of generality

When the friability level exceeds n^{d-1}, only irreducible factors of degree at least d matter. Therefore the theorem also holds if $F(x)$ has K distinct irreducible factors of degree d and any number of irreducible factors of degree less than d.

Schinzel's "Hypothesis H" (Bateman–Horn conjecture)

Definition

$\pi(F;x) = \#\{n \le x :$
$f(n)$ is prime for each irreducible factor f of $F\}$

Conjecture: $\pi(F;x)$ is asymptotic to $H(F)\,\mathrm{li}(F;x)$, where:

- $\mathrm{li}(F;x) = \displaystyle\int_{0<t<x} \left(\prod_{\substack{f \mid F \\ f \text{ irreducible}}} \frac{1}{\log|f(t)|} \right) dt$
- $H(F) = \displaystyle\prod_p \left(1-\frac{1}{p}\right)^{-L} \left(1-\frac{\sigma(F;p)}{p}\right)$

L: the number of distinct irreducible factors of F

$\sigma(F;n)$: the number of solutions of $F(a) \equiv 0 \pmod{n}$

Schinzel's "Hypothesis H" (Bateman–Horn conjecture)

Definition

$\pi(F;x) = \#\{n \le x :$
$f(n)$ is prime for each irreducible factor f of $F\}$

Conjecture: $\pi(F;x)$ is asymptotic to $H(F)\,\mathrm{li}(F;x)$, where:

- $\mathrm{li}(F;x) = \displaystyle\int_{0<t<x} \left(\prod_{\substack{f \mid F \\ f \text{ irreducible}}} \frac{1}{\log|f(t)|} \right) dt$
- $H(F) = \displaystyle\prod_p \left(1-\frac{1}{p}\right)^{-L} \left(1-\frac{\sigma(F;p)}{p}\right)$

L: the number of distinct irreducible factors of F

$\sigma(F;n)$: the number of solutions of $F(a) \equiv 0 \pmod{n}$

Schinzel's "Hypothesis H" (Bateman–Horn conjecture)

Definition

$\pi(F;x) = \#\{n \le x :$
$f(n)$ is prime for each irreducible factor f of $F\}$

Conjecture: $\pi(F;x)$ is asymptotic to $H(F)\,\mathrm{li}(F;x)$, where:

- $\displaystyle \mathrm{li}(F;x) = \int_{0<t<x} \left(\prod_{\substack{f \mid F \\ f \text{ irreducible}}} \frac{1}{\log|f(t)|} \right) dt$
- $\displaystyle H(F) = \prod_p \left(1-\frac{1}{p}\right)^{-L} \left(1-\frac{\sigma(F;p)}{p}\right)$

L: the number of distinct irreducible factors of F

$\sigma(F;n)$: the number of solutions of $F(a) \equiv 0 \pmod n$

Schinzel's "Hypothesis H" (Bateman–Horn conjecture)

Definition

$\pi(F;x) = \#\{n \le x :$
$f(n)$ is prime for each irreducible factor f of $F\}$

Conjecture: $\pi(F;x)$ is asymptotic to $H(F)\,\mathrm{li}(F;x)$, where:

- $\displaystyle \mathrm{li}(F;x) = \int_{0<t<x} \left(\prod_{\substack{f \mid F \\ f \text{ irreducible}}} \frac{1}{\log |f(t)|} \right) dt$
- $\displaystyle H(F) = \prod_p \left(1 - \frac{1}{p}\right)^{-L} \left(1 - \frac{\sigma(F;p)}{p}\right)$

L: the number of distinct irreducible factors of F

$\sigma(F;n)$: the number of solutions of $F(a) \equiv 0 \pmod{n}$

Schinzel's "Hypothesis H" (Bateman–Horn conjecture)

Definition

$\pi(F;x) = \#\{n \le x :$
$f(n)$ is prime for each irreducible factor f of $F\}$

Conjecture: $\pi(F;x)$ is asymptotic to $H(F)\,\mathrm{li}(F;x)$, where:

- $\displaystyle \mathrm{li}(F;x) = \int_{0<t<x} \left(\prod_{\substack{f \mid F \\ f \text{ irreducible}}} \frac{1}{\log |f(t)|} \right) dt$
- $\displaystyle H(F) = \prod_p \left(1 - \frac{1}{p}\right)^{-L} \left(1 - \frac{\sigma(F;p)}{p}\right)$

L: the number of distinct irreducible factors of F

$\sigma(F;n)$: the number of solutions of $F(a) \equiv 0 \pmod{n}$

A uniform version of Hypothesis H

Hypothesis UH

$$\pi(F;x) - H(F)\,\mathrm{li}(F;x) \ll_{d,B} 1 + \frac{H(F)x}{(\log x)^{L+1}}$$

uniformly for all polynomials F of degree d with L distinct irreducible factors, each of which has coefficients bounded by x^B in absolute value.

- $\mathrm{li}(F;x)$ is asymptotic to $\dfrac{x}{(\log x)^L}$ for fixed F

The uniformity is reasonable

For $d = L = 1$, Hypothesis UH is equivalent to the conjectured number of primes, in an interval of length $y = T^\varepsilon$ near T, in an arithmetic progression to a modulus $q \le y^{1-\varepsilon}$.

A uniform version of Hypothesis H

Hypothesis UH

$$\pi(F;x) - H(F)\,\mathrm{li}(F;x) \ll_{d,B} 1 + \frac{H(F)x}{(\log x)^{L+1}}$$

uniformly for all polynomials F of degree d with L distinct irreducible factors, each of which has coefficients bounded by x^B in absolute value.

- $\mathrm{li}(F;x)$ is asymptotic to $\dfrac{x}{(\log x)^L}$ for fixed F

The uniformity is reasonable

For $d = L = 1$, Hypothesis UH is equivalent to the conjectured number of primes, in an interval of length $y = T^\varepsilon$ near T, in an arithmetic progression to a modulus $q \le y^{1-\varepsilon}$.

A uniform version of Hypothesis H

Hypothesis UH

$$\pi(F;x) - H(F)\,\mathrm{li}(F;x) \ll_{d,B} 1 + \frac{H(F)x}{(\log x)^{L+1}}$$

uniformly for all polynomials F of degree d with L distinct irreducible factors, each of which has coefficients bounded by x^B in absolute value.

- $\mathrm{li}(F;x)$ is asymptotic to $\dfrac{x}{(\log x)^L}$ for fixed F

The uniformity is reasonable

For $d = L = 1$, Hypothesis UH is equivalent to the conjectured number of primes, in an interval of length $y = T^\varepsilon$ near T, in an arithmetic progression to a modulus $q \le y^{1-\varepsilon}$.

What's the connection?

Why are we talking about prime values of polynomials in a lecture about friable values of polynomials?

Heuristic

The process of "guessing" the right answer for $\pi(F;x)$ puts us in the right state of mind for trying to guess the right answer for $\Psi(F;x,y)$.

Implication

By assuming the expected formula for $\pi(F;x)$ with some uniformity (Hypothesis UH), we can derive a formula for $\Psi(F;x,y)$ in a limited range.

- This implication informs our beliefs about the expected formula for $\Psi(F;x,y)$.

What's the connection?

Why are we talking about prime values of polynomials in a lecture about friable values of polynomials?

Heuristic

The process of "guessing" the right answer for $\pi(F;x)$ puts us in the right state of mind for trying to guess the right answer for $\Psi(F;x,y)$.

Implication

By assuming the expected formula for $\pi(F;x)$ with some uniformity (Hypothesis UH), we can derive a formula for $\Psi(F;x,y)$ in a limited range.

- This implication informs our beliefs about the expected formula for $\Psi(F;x,y)$.

What's the connection?

Why are we talking about prime values of polynomials in a lecture about friable values of polynomials?

Heuristic

The process of "guessing" the right answer for $\pi(F;x)$ puts us in the right state of mind for trying to guess the right answer for $\Psi(F;x,y)$.

Implication

By assuming the expected formula for $\pi(F;x)$ with some uniformity (Hypothesis UH), we can derive a formula for $\Psi(F;x,y)$ in a limited range.

- This implication informs our beliefs about the expected formula for $\Psi(F;x,y)$.

What's the connection?

Why are we talking about prime values of polynomials in a lecture about friable values of polynomials?

Heuristic

The process of "guessing" the right answer for $\pi(F;x)$ puts us in the right state of mind for trying to guess the right answer for $\Psi(F;x,y)$.

Implication

By assuming the expected formula for $\pi(F;x)$ with some uniformity (Hypothesis UH), we can derive a formula for $\Psi(F;x,y)$ in a limited range.

- This implication informs our beliefs about the expected formula for $\Psi(F;x,y)$.

What would we expect on probablistic grounds?

Let $F(x) = f_1(x) \cdots f_L(x)$, where $\deg f_j(x) = d_j$. Let $u > 0$.

- $f_j(n)$ is roughly n^{d_j}, and integers of that size are $n^{1/u}$-friable with probability $\rho(d_j u)$.
- Are the friabilities of the various factors $f_j(n)$ independent? This would lead to a prediction involving

$$x \prod_{j=1}^{L} \rho(d_j u).$$

- What about local densities depending on the arithmetic of F (as in Hypothesis H)?

What would we expect on probablistic grounds?

Let $F(x) = f_1(x) \cdots f_L(x)$, where $\deg f_j(x) = d_j$. Let $u > 0$.

- $f_j(n)$ is roughly n^{d_j}, and integers of that size are $n^{1/u}$-friable with probability $\rho(d_j u)$.
- Are the friabilities of the various factors $f_j(n)$ independent? This would lead to a prediction involving

$$x \prod_{j=1}^{L} \rho(d_j u).$$

- What about local densities depending on the arithmetic of F (as in Hypothesis H)?

What would we expect on probablistic grounds?

Let $F(x) = f_1(x) \cdots f_L(x)$, where $\deg f_j(x) = d_j$. Let $u > 0$.

- $f_j(n)$ is roughly n^{d_j}, and integers of that size are $n^{1/u}$-friable with probability $\rho(d_j u)$.
- Are the friabilities of the various factors $f_j(n)$ independent? This would lead to a prediction involving

$$x \prod_{j=1}^{L} \rho(d_j u).$$

- What about local densities depending on the arithmetic of F (as in Hypothesis H)?

What would we expect on probablistic grounds?

Let $F(x) = f_1(x) \cdots f_L(x)$, where $\deg f_j(x) = d_j$. Let $u > 0$.

- $f_j(n)$ is roughly n^{d_j}, and integers of that size are $n^{1/u}$-friable with probability $\rho(d_j u)$.
- Are the friabilities of the various factors $f_j(n)$ independent? This would lead to a prediction involving

$$x \prod_{j=1}^{L} \rho(d_j u).$$

- What about local densities depending on the arithmetic of F (as in Hypothesis H)?

Conjecture for friable values of polynomials

Conjecture

Let $F(x)$ be any polynomial, let $f_1, \dots, f_L$ be its distinct irreducible factors, and let $d_1, \dots, d_L$ be their degrees. Then

$$\Psi(F; x, x^{1/u}) = x \prod_{j=1}^{L} \rho(d_j u) + O\left(\frac{x}{\log x}\right)$$

for all $0 < u$.

If F irreducible: $\Psi(F; x, x^{1/u}) = x\rho(du) + O(x/\log x)$ for $0 < u$.

Remark: Not as universally accepted as Hypothesis H; lack of local factors is controversial.

Conjecture for friable values of polynomials

Conjecture

Let $F(x)$ be any polynomial, let $f_1, \dots, f_L$ be its distinct irreducible factors, and let $d_1, \dots, d_L$ be their degrees. Then

$$\Psi(F; x, x^{1/u}) = x \prod_{j=1}^{L} \rho(d_j u) + O\left(\frac{x}{\log x}\right)$$

for all $0 < u$.

If F irreducible: $\Psi(F; x, x^{1/u}) = x\rho(du) + O(x/\log x)$ for $0 < u$.

Remark: Not as universally accepted as Hypothesis H; lack of local factors is controversial.

Conjecture for friable values of polynomials

Conjecture

Let $F(x)$ be any polynomial, let $f_1, \dots, f_L$ be its distinct irreducible factors, and let $d_1, \dots, d_L$ be their degrees. Then

$$\Psi(F; x, x^{1/u}) = x \prod_{j=1}^{L} \rho(d_j u) + O\left(\frac{x}{\log x}\right)$$

for all $0 < u$.

If F irreducible: $\Psi(F; x, x^{1/u}) = x\rho(du) + O(x/\log x)$ for $0 < u$.

Remark: Not as universally accepted as Hypothesis H; lack of local factors is controversial.

Conjecture for friable values of polynomials

Theorem (M., 2002)

Assume Hypothesis UH. Let $F(x)$ be any polynomial, let $f_1, \dots, f_L$ be its distinct irreducible factors, and let $d_1, \dots, d_L$ be their degrees. Let $d = \max\{d_1, \dots, d_L\}$, and let F have exactly K distinct irreducible factors of degree d. Then

$$\Psi(F; x, x^{1/u}) = x \prod_{j=1}^{L} \rho(d_j u) + O\left(\frac{x}{\log x}\right)$$

for all $0 < u < 1/(d - 1/K)$.

If F irreducible: $\Psi(F; x, x^{1/u}) = x\rho(du) + O(x/\log x)$ for $0 < u < 1/(d-1)$.

Trivial: $0 < u < 1/d$.

Shifted primes

Theorem (M., 2002)

Assume Hypothesis UH. For any nonzero integer a, the number of primes p such that $p - a$ is $x^{1/u}$-friable is

$$\pi(x)\rho(u) + O\left(\frac{\pi(x)}{\log x}\right)$$

for all $0 < u < 3$.

- In the range $1 \le u \le 2$, we have the elementary formula $\rho(u) = 1 - \log u$, but $\rho(u)$ is less elementary in the range $u > 2$. So the appearance of $\rho(u)$ in the range $2 < u < 3$ is portentous.
- There is no Buchstab formula for shifted primes, so the combinatorics has to be done by hand. In principle, the theorem could be extended to cover all $u > 0$.

Shifted primes

Theorem (M., 2002)

Assume Hypothesis UH. For any nonzero integer a, the number of primes p such that $p - a$ is $x^{1/u}$-friable is

$$\pi(x)\rho(u) + O\left(\frac{\pi(x)}{\log x}\right)$$

for all $0 < u < 3$.

- In the range $1 \le u \le 2$, we have the elementary formula $\rho(u) = 1 - \log u$, but $\rho(u)$ is less elementary in the range $u > 2$. So the appearance of $\rho(u)$ in the range $2 < u < 3$ is portentous.
- There is no Buchstab formula for shifted primes, so the combinatorics has to be done by hand. In principle, the theorem could be extended to cover all $u > 0$.

Shifted primes

Theorem (M., 2002)

Assume Hypothesis UH. For any nonzero integer a, the number of primes p such that $p - a$ is $x^{1/u}$-friable is

$$\pi(x)\rho(u) + O\left(\frac{\pi(x)}{\log x}\right)$$

for all $0 < u < 3$.

- In the range $1 \le u \le 2$, we have the elementary formula $\rho(u) = 1 - \log u$, but $\rho(u)$ is less elementary in the range $u > 2$. So the appearance of $\rho(u)$ in the range $2 < u < 3$ is portentous.
- There is no Buchstab formula for shifted primes, so the combinatorics has to be done by hand. In principle, the theorem could be extended to cover all $u > 0$.

The end

The papers *Polynomial values free of large prime factors* (with Dartyge and Tenenbaum) and *An asymptotic formula for the number of smooth values of a polynomial*, as well as these slides, are available for downloading:

My papers

www.math.ubc.ca/~gerg/index.shtml?research

My talk slides

www.math.ubc.ca/~gerg/index.shtml?slides