PRIME NUMBERS AND L-FUNCTIONS

Henryk Iwaniec (Rutgers University)

ICM, Madrid 2006

THEOREM (Bombieri–Vinogradov). We have

$$\sum_{q \le Q} \max_{(a,q)=1} \left| \psi(x;q,a) - \frac{x}{\varphi(q)} \right| \ll x(\log x)^{-A}$$

for any constant $A \ge 1$ with $Q = x^{\frac{1}{2}}(\log x)^{-B}$, $B = B(A) > 0$.

Hence $\psi(x;q,a) \sim x/\varphi(q)$ for almost all $q \le x^{\frac{1}{2}}(\log x)^{-B}$.

Beyond the GRH

CONJECTURE (Elliott–Halberstam). The B-V holds with

$$Q = x^{\theta}, \quad \text{any } \theta < 1.$$

THEOREM (Goldston–Pintz–Yıldırım). If B-V holds with $Q = x^{\theta}$ for some $\frac{1}{2} < \theta < 1$, then the gaps between primes are absolutely bounded infinitely often.

THEOREM (Bombieri–Fouvry–Friedlander–Iwaniec). For any sequence (λ_q) of level $Q = x^{4/7}$ which is "well-factorable"

IN ARITHMETIC PROGRESSIONS

$p \equiv a \pmod{q}$, $p \le x$, $q > \sqrt{x}$

$mn \equiv a \pmod{q}$

m, n – medium size

both irregular

interpretation of the congruence by the equation

$mn = a + qr$

$\det\begin{pmatrix} m & r \\ q & n \end{pmatrix} = a$

By the Hecke operator T_a reduce this to

$\det\begin{pmatrix} m & r \\ q & n \end{pmatrix} = 1$

Spectral theory on congruence groups

Problems with small eigenvalues

$\ell m \equiv a \pmod{q}$

ℓ - large, smooth

m - small, irregular

Fourier analysis in the ℓ-variable (characters)

SPECTRAL ANALYSIS OF PRIMES IN ARITHMETIC PROGRESSIONS

$p \equiv a \pmod{q}$, $p \le x$, $q > \sqrt{x}$

$mn \equiv a \pmod{q}$

m, n – medium size

both irregular

interpretation of the congruence by the equation

$mn = a + qr$

$\det\begin{pmatrix} m & r \\ q & n \end{pmatrix} = a$

By the Hecke operator T_a reduce this to

$\det\begin{pmatrix} m & r \\ q & n \end{pmatrix} = 1$

Spectral theory on congruence groups

Problems with small eigenvalues

$\ell m \equiv a \pmod{q}$

ℓ – large, smooth

m – small, irregular

Fourier analysis in the ℓ-variable (characters)

EXPLICIT FORMULA

$$\psi(x;q,a) - \frac{x}{\varphi(q)} = -\frac{1}{\varphi(q)} \sum_{\chi \,(\mathrm{mod}\, q)} \bar{\chi}(a) \sum_{\rho} \frac{x^{\rho}}{\rho} + \dots$$

$L(\rho, \chi) = 0$

$\rho = \frac{1}{2} + i\gamma$ the Grand Riemann Hypothesis

TCHEBYSHEV'S BIAS

Observe more primes $p \equiv 3 \pmod 4$ than $p \equiv 1 \pmod 4$!

Comparative Prime Number Theory (Knapowski + Turan)

The bias of multi classes (Rubinstein + Sarnak)

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_m \frac{\mu(m)}{m^s}, \qquad \sigma > \frac{1}{2}.$$

$\mu(m) = (-1)^r$ if $m = p_1 \dots p_r$ distinct prime factors

$\mu(m) = 0$ if $p^2 \mid m$

The Möbius function $\mu(m)$ changes sign in the unbiased fashion towards any natural sequence c_m producing a considerable cancellation in the twisted sums

$$\sum_{m \leq x} \mu(m) c_m .$$

This principle is very useful for testing sums over primes

$$\sum_{n \leq x} a_n \Lambda(n)$$

where $\mathcal{A} = (a_n)$ is quite general sequence of real, non-negative numbers. Indeed, we have

Assuming

$$\sum_{\substack{n \le x \\ n \equiv 0 \pmod{m}}} a_n \sim g(m)X$$

where g is a suitable multiplicative function one is led by the randomness principle to the ASYMPTOTIC FORMULA FOR SUMS OVER PRIMES

$$\sum_{n \le x} a_n \Lambda(n) \sim HX$$

where H is a positive constant given by the infinite product

$$H = \prod_p (1 - g(p))\left(1 - \frac{1}{p}\right)^{-1}.$$

Sieve for Primes

Fix $\delta > 0$. Suppose

$$\sum_{m \le x^{1-\delta}} \Big| \sum_{\substack{n \le x \\ n \equiv 0 \pmod{m}}} a_n - g(m)X \Big| \ll X(\log x)^{-2}$$

and

$$\sum_{\ell} \Big| \sum_{\substack{\ell m \le x \\ x^{\delta} < m < x^{2\delta}}} \mu(m) a_{\ell m} \Big| \ll X(\log x)^{-2}$$

Then we have the asymptotic formula

Sieve for Primes

Fix $\delta > 0$. Suppose

$$\sum_{m \le x^{1-\delta}} \Big| \sum_{\substack{n \le x \\ n \equiv 0 \, (\mathrm{mod}\, m)}} a_n - g(m) X \Big| \ll X (\log x)^{-2}$$

and

$$\sum_{\ell} \Big| \sum_{\substack{\ell m \le x \\ x^{\delta} < m < x^{2\delta}}} \mu(m) a_{\ell m} \Big| \ll X (\log x)^{-2}$$

Then we have the asymptotic formula

$$\sum_{n \le x} a_n \Lambda(n) \sim HX$$

THEOREM (Fouvry – Iwaniec)

$$\sum_{\ell^2+m^2\le x} \Lambda(\ell)\Lambda(\ell^2+m^2) \sim HX, \quad \text{with } X = x.$$

Hence there are infinitely many primes of type $p = \ell^2+m^2$ where ℓ is also prime.

THEOREM (Friedlander – Iwaniec)

$$\sum_{a^2+b^4\le x} \Lambda(a^2+b^4) \sim HX.$$

Hence there are infinitely many $p =$

THEOREM (Heath – Brown)

$$\sum \Lambda(a^3+2b^3) \sim HX,$$

THEOREM (Fouvry + Iwaniec)

$$\sum_{\ell^2+m^2\le x} \Lambda(\ell)\Lambda(\ell^2+m^2) \sim HX, \quad \text{with } X \asymp x.$$

Hence there are infinitely many primes of type $p=\ell^2+m^2$ where ℓ is also prime.

THEOREM (Friedlander + Iwaniec)

$$\sum_{a^2+b^4\le x} \Lambda(a^2+b^4) \sim HX, \quad \text{with } X \asymp x^{\frac{3}{4}}.$$

Hence there are infinitely many primes of type $p=a^2+b^4$.

THEOREM (Heath-Brown)

$$\sum \Lambda(a^3+2b^3) \sim HX, \quad \text{with } X \asymp x^{\frac{2}{3}}$$

1. WHAT ARE THE PRIME NUMBERS GOOD FOR ?

$\mathcal{P} = \{ p = 2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots \}$

elementary particles of arithmetic

Fundamental Areas and Principles:

$\mathbb{F}_p$ – finite fields
$\mathbb{Q}_p$ – p-adic fields
local-global principles
prime ideals in number fields

Entertaining Problems

– The largest known prime number
(produced by C. Cooper & S. Boone in 12/15/2005)

$p = 2^{30402457} - 1$ over nine million digits

– The Twin Primes Conjecture

The Spin of Gaussian Primes

$p \equiv 1 \pmod 4$, $p = \pi\bar{\pi}$,

$\pi = r + is$, $p = r^2 + s^2$, $r, s > 0$, r odd

$s_p = \left(\frac{s}{r}\right) = \pm 1$ the Legendre symbol

We have (Friedlander + Iwaniec)

$$\sum_{p \le x} s_p \ll x^{76/77}.$$

Surprising Conspiracy (set up by Iwaniec + Luo + Sarnak)

$\lambda(p)$ – the eigenvalues of the Hecke operators T_p acting on the cusp forms on the full modular group $\Gamma = SL_2(\mathbb{Z})$

$|\lambda(p)| \le 2$ the Ramanujan

The Spin of Gaussian Primes

$p \equiv 1 \pmod 4$, $p = \pi\bar{\pi}$,

$\pi = r + is$, $p = r^2 + s^2$, $r, s > 0$, r odd

$s_p = \left(\frac{s}{r}\right) = \pm 1$ the Legendre symbol

We have (Friedlander + Iwaniec)

$$\sum_{p \le x} s_p \ll x^{76/77}.$$

Surprising Conspiracy (set up by Iwaniec + Luo + Sarnak)

$\lambda(p)$ – the eigenvalues of the Hecke operator T_p acting on a cusp form on the full modular group $\Gamma = SL_2(\mathbb{Z})$

$|\lambda(p)| \le 2$ the Ramanujan Conjecture (proved by P. Deligne)

By the GRH we get

$$\sum \lambda(p) \ll x^{\frac{1}{2}+\varepsilon} \qquad \sum e^{2\pi i\sqrt{p}} \ll x^{\frac{1}{2}+\varepsilon}$$

$\mathfrak{p} = r + is$, $p = r^2 + s^2$, $r, s > 0$, r odd

$\delta_p = \left(\frac{s}{r}\right) = \pm 1$ the Legendre symbol

We have (Friedlander + Iwaniec)

$$\sum_{p \le x} \delta_p \ll x^{76/77}.$$

Surprising Conspiracy (set up by Iwaniec + Luo + Sarnak)

$\lambda(p)$ – the eigenvalues of the Hecke operators T_p acting on a cusp form on the full modular group $\Gamma = SL_2(\mathbb{Z})$

$|\lambda(p)| \le 2$ the Ramanujan Conjecture (proved by P. Deligne)

By the GRH we get

$$\sum_{p \le x} \lambda(p) \ll x^{\frac{1}{2}+\epsilon}, \qquad \sum_{p \le x} e^{4\pi i \sqrt{p}} \ll x^{\frac{1}{2}+\epsilon}$$

By the randomness principle of the Möbius function we derive

$$\sum \lambda(p) e^{4\pi i \sqrt{p}} \sim c\, x^{\frac{3}{4}} \; ?$$

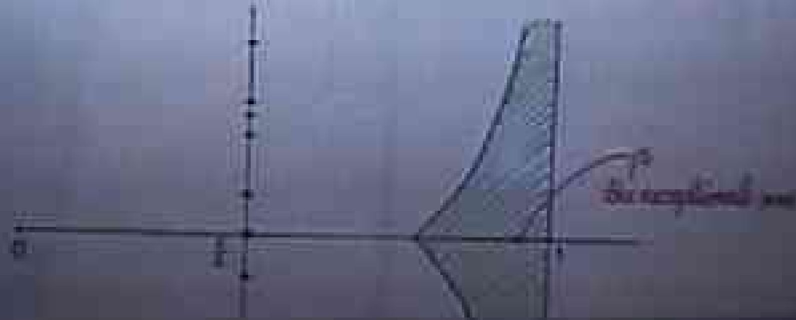
THE EXCEPTIONAL CHARACTER

THEOREM (Landau). Let $D > 4$. There exists at most one character $\chi = \chi_D$ of conductor D such that $L(s, \chi_D)$ has a zero in the region

$$s = \sigma + it, \quad \sigma \geq 1 - \frac{c}{\log D(|t|+1)}$$

where $c > 0$ is a small absolute constant.
The exceptional character is real and the exceptional zero, say β, is also real and simple

$$1 - \frac{c}{\log D} < \beta < 1.$$



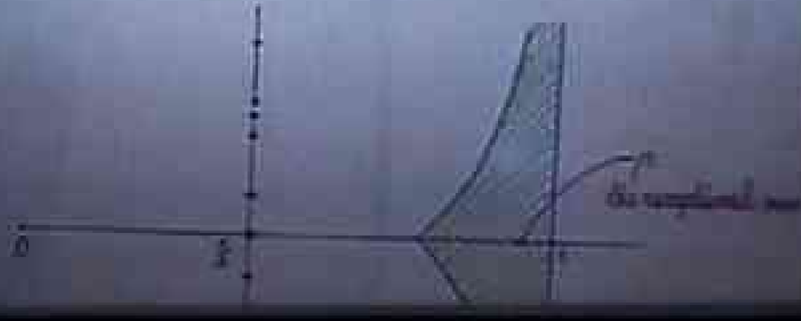
1. THE EXCEPTIONAL CHARACTER

THEOREM (Landau). Let $D > 4$. There exists at most one character $\chi = \chi_D$ of conductor D such that $L(s, \chi_D)$ has a zero in the region

$$s = \sigma + it, \quad \sigma \geq 1 - \frac{c}{\log D(|t|+1)}$$

where $c > 0$ is a small absolute constant.
The exceptional character is real and the exceptional zero, say β, is also real and simple

$$1 - \frac{c}{\log D} \leq \beta < 1.$$

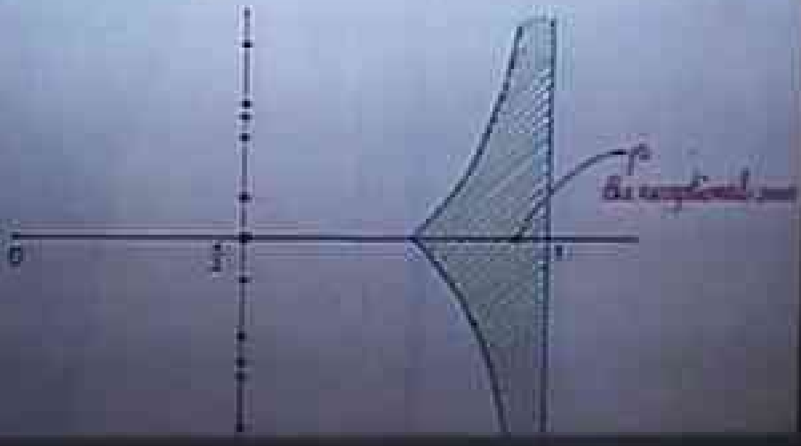


at most one character $\chi = \chi_D$ of conductor D such that $L(s, \chi_D)$ has a zero in the region

$$s = \sigma + it, \quad \sigma > 1 - \frac{c}{\log D(|t|+1)}$$

where $c > 0$ is a small absolute constant.
The exceptional character is real and the exceptional zero, say β, is also real and simple.

$$1 - \frac{c}{\log D} < \beta < 1.$$



$$\chi_D(n) = \left(\frac{-D}{n}\right)$$

is the Kronecker symbol associated with the imaginary quadratic field

$$K = \mathbb{Q}(\sqrt{-D}).$$

The Dirichlet Class Number Formula

$$h(-D) = \pi^{-1}\sqrt{D}\,L(1,\chi_D) \geq 1.$$

REPELLING PROPERTY. If the exceptional zero of $L(s,\chi_D)$ is close to the point $s=1$, then the other zeros, real or complex, of any natural L-function stay further from $s=1$.

The exceptional character pretends to be the Möbius function!

Hence the exceptional character opens the way for estimating sums over primes by applying harmonic analysis!

repelling property. [illegible] rapidly as β approaches the central point $s = \frac{1}{2}$. Yet, if the central point is a multiple zero then its repelling power is not gone entirely.

If the repelling is very strong one can obtain results about prime numbers which cannot be derived by the GRH alone. Therefore the exceptional character is welcome. Of course, its existence would contradict the Grand Riemann Hypothesis, so we better call the primes obtained by means of the exceptional character the "illusory primes".

EXAMPLE (Heath-Brown). There are infinitely many twin primes.

EXAMPLE (Friedlander + Iwaniec). There are infinitely many primes of type $p = 3a^2 + 2b^6$ ([illegible] elliptic curves with only one place of bad reduction).

OBSERVATION (Friedlander). Any real zero $\beta > \frac{1}{2}$ is exceptional in the sense of having the repelling property. The power of repelling diminishes rapidly as β approaches the central point $s = \frac{1}{2}$. Yet, if the central point is a multiple zero then its repelling power is not gone entirely.

If the repelling is very strong one can obtain results about prime numbers which cannot be derived by the GRH alone. Therefore the exceptional character is welcome. Of course, its existence would contradict the Grand Riemann Hypothesis, so we better call the primes obtained by means of the exceptional character the "illusory primes".

EXAMPLE (Heath-Brown). There are infinitely many twin primes.

EXAMPLE (Friedlander + Iwaniec). There are infinitely many primes of type $p = x^2 + y^6$

$\frac{1}{2} < \beta < 1$ the exceptional zero

$$h(-D) \gg D^{\beta-\frac{1}{2}}(\log D)^{-2}$$

If $\beta = \frac{1}{2}$ is a triple zero of the Hasse-Weil L-function of an elliptic curve (of rank ≥ 3) then

$$h(-D) \gg \log D \qquad \text{(D. Goldfeld)}$$

2. THE PRIME NUMBER THEOREM

$$\pi(x) = |\{p \le x;\ p \text{ prime}\}| \sim \frac{x}{\log x}$$

$$\pi_2(x) = |\{p \le x;\ p, p+2 \text{ primes}\}| \sim \frac{cx}{(\log x)^2}$$

$c = 0.66\ldots$ constant

Better counting with

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^\alpha;\ \alpha > 0 \\ 0, & \text{otherwise} \end{cases}$$

$$\psi(x) = \sum_{n \le x} \Lambda(n) \sim x \quad \text{(Hadamard, de la Vallée Poussin)}$$

$$\psi_2(x) = \sum_{n \le x} \Lambda(n)\Lambda(n+2) \sim x \quad \text{(conjecture)}$$

OBSERVATION (Friedlander). Any real zero $\beta > \frac{1}{2}$ is exceptional in the sense of having the repelling property. The power of repelling diminishes rapidly as β approaches the central point $s = \frac{1}{2}$. Yet, if the central point is a multiple zero then its repelling power is not gone entirely.

If the repelling is very strong one can obtain results about prime numbers which cannot be derived by the GRH alone. Therefore the exceptional character is welcome. Of course, its existence would contradict the Grand Riemann Hypothesis, so we better call the primes obtained by means of the exceptional character the "illusory primes".

EXAMPLE (Heath-Brown). There are infinitely many twin primes.

EXAMPLE (Fri

WARNING (Sarnak + Zaharescu). The existence of exceptional character would mean the Grand Riemann Hypothesis may badly fail. The L-functions of certain cusp forms would have complex zeros off the critical line!

How do you believe in the real exceptional character?

Eliminating the exceptional character is one of the most important problem in Analytic Number Theory.

THEOREM (Conrey + Iwaniec). Suppose $\zeta(s)$ has a positive proportion of pairs of zeros on the critical line with gaps smaller than the half of the normal (average) gap. Then the exceptional character does not exist!

The Random Matrix Theory predicts that very small gaps between zeros occur often.

PAIR CORRELATION CONJECTURE (Montgomery)

$$\left\| \left\{ m \neq n ;\ 0 < \gamma_m, \gamma_n < T,\ \frac{2\pi\alpha}{\log T} < \gamma_m - \gamma_n < \frac{2\pi\beta}{\log T} \right\} \right\|$$

[illegible]

WARNING (Sarnak + Zaharescu). The existence of exceptional character would ruin the General Riemann Hypothesis very badly. The L-functions of certain cusp forms would have complex zeros off the critical line!

How do you believe in the real exceptional character?

Eliminating the exceptional character is one of the most important problem in Analytic Number Theory.

THEOREM (Conrey + Iwaniec). Suppose $\zeta(s)$ has a positive proportion of pairs of zeros on the critical line with gaps smaller than the half of the normal (average) gaps. Then the exceptional character does not exist!

The Random Matrix Theory predicts that very small gaps between zeros occur often.

PAIR CORRELATION CONJECTURE (Montgomery).

$$\left|\left\{m \neq n,\ 0 < \gamma_m, \gamma_n \leq T,\ \frac{2\pi\alpha}{\log T} < \gamma_m - \gamma_n < \frac{2\pi\beta}{\log T}\right\}\right|$$

$$\sim T(\log T) \int_\alpha^\beta \left(1 - \left(\frac{\sin \pi u}{\pi u}\right)^2\right) du.$$

WARNING (Sarnak + Zaharescu) The existence of exceptional character would ruin the Grand Riemann Hypothesis very badly. The L-functions of certain cusp forms would have complex zeros off the critical line!

How do you believe in the real exceptional character?

Eliminating the exceptional character is one of the most important problem in Analytic Number Theory.

THEOREM (Conrey + Iwaniec). Suppose $\zeta(s)$ has a positive proportion of pairs of zeros on the critical line with gaps smaller than the half of the normal (average) gap. Then the exceptional character does not exist!

The Random Matrix Theory predicts that very small gaps between zeros occur often

PAIR CORRELATION CONJECTURE (Montgomery).

$$\left|\left\{ m \neq n \,;\, 0 < \gamma_m, \gamma_n \leq T,\ \frac{2\pi\alpha}{\log T} < \gamma_m - \gamma_n < \frac{2\pi\beta}{\log T} \right\}\right|$$

$$\sim \frac{T}{2\pi}(\log T) \int_\alpha^\beta \left(1 - \left(\frac{\sin \pi u}{\pi u}\right)^2\right) du$$

ANALYTIC NUMBER THEORY

FLOURISHES WITH OR WITHOUT

THE RIEMANN HYPOTHESIS

PRIMES VERSUS ZEROS

The additive group aspects of integers are quite well understood by means of harmonic analysis:

$$\sum_{m\in\mathbb{Z}^n} f(m) = \sum_{n\in\mathbb{Z}^n} \hat{f}(n) \qquad \text{Poisson's formula}$$

The zeta function

$$\zeta(s) = \sum_n n^{-s} = \prod_p \left(1-\frac{1}{p^s}\right)^{-1}, \quad s=\sigma+it, \quad \sigma>1$$

$$s(1-s)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = e^{-bs}\prod_\rho \left(1-\frac{s}{\rho}\right)e^{s/\rho}, \quad \rho = \beta + i\gamma, \quad 0<\beta<1$$

The zeros are "dual" companions to primes

$$\sum_n \Lambda(n) f(n) = -\sum_\rho F(\rho) + \int_1^\infty \left(1-\frac{1}{(x-1)x(x+1)}\right) f(x)\,dx$$

$f(x)$ – a test function, $F(s)$ – the Mellin transform

THE RIEMANN HYPOTHESIS

$\rho = \frac{1}{2} + i\gamma$

3. PRIMES VERSUS ZEROS

The additive group aspects of integers are quite well understood by means of harmonic analysis

$$\sum_{m\in\mathbb{Z}^n} f(m) = \sum_{n\in\mathbb{Z}^n} \hat{f}(n) \qquad \text{Poisson's formula}$$

The zeta function

$$\zeta(s) = \sum_n n^{-s} = \prod_p \left(1-\frac{1}{p^s}\right)^{-1}, \quad s=\sigma+it, \quad \sigma>1$$

$$s(1-s)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = e^{-bs}\prod_\rho \left(1-\frac{s}{\rho}\right)e^{s/\rho}, \quad \begin{matrix}\rho=\beta+i\gamma \\ 0<\beta<1\end{matrix}$$

The zeros are "dual" companions to primes

$$\sum_n \Lambda(n) f(n) = -\sum_\rho F(\rho) + \int_1^\infty \left(1-\frac{1}{(x-1)x(x+1)}\right) f(x)\,dx$$

$f(x)$ – a test function, $F(s)$ – the Mellin transform

THE RIEMANN HYPOTHESIS

Total number of zeros

$$|\{\rho=\beta+i\gamma,\ 0<\gamma\le T\}| = \frac{T}{2\pi}\log T + O(T)$$

Density estimate

$$|\{\rho=\beta+i\gamma,\ 0<\gamma\le T,\ \beta\ge\alpha\}| \ll T^{c(1-\alpha)}\log T$$

$c=\frac{12}{5}$ (Huxley)

$c=2$ Density Conjecture

Zero Detectors

Theory of large values of Dirichlet Polynomials

Consecutive zeros

$$0<\gamma_1\le\gamma_2\le\cdots, \qquad \gamma_n\sim\frac{2\pi n}{\log n}$$

Average spacing

4. GAPS BETWEEN PRIMES

p_n – the n-th prime number

$p_n \sim n \log n$

$d_n = p_{n+1} - p_n \sim \log n$ on average

$d_n \ll (\log n)^2$ Cramér's Conjecture

$d_n \ll n^{\frac{1}{2}} (\log n)^2$ by the Riemann hypothesis

$d_n \ll n^{0.525}$ the world record due to Baker + Harman + Pintz

$d_n = 2$ infinitely often (the Twin Primes Conjecture)

$\liminf_{n} \frac{p_{n+1} - p_n}{\log n} = 0$ (Goldston – Pintz + Yildirim, 2005)

$(\log n)^{\frac{1}{2}} (\log \log n)^2$

$q \geq 1, \quad (a,q)=1$

$p \equiv a \pmod{q}$

$\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ Dirichlet characters
$\varphi(q)$ of these

$$L(s,\chi) = \sum_n \chi(n) n^{-s}$$
$$= \prod_p \left(1 - \chi(p) p^{-s}\right)^{-1} \qquad \text{L-functions}$$

The Riemann memoir extends to all L-functions

Assuming the Grand Riemann Hypothesis we have

$$\psi(x;q,a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n) = \frac{x}{\varphi(q)} + O\left(\sqrt{x}(\log x)^2\right)$$

if $q < \sqrt{x}(\log x)^{-2}$.

$\psi(x;q,a) \sim \dfrac{x}{\varphi(q)}$ for every $q \leq x^{1-\varepsilon}$
(Montgomery's Conjecture)

5. PRIMES IN ARITHMETIC PROGRESSIONS

$q \geq 1, \quad (a,q)=1$

$p \equiv a \pmod{q}$

$\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ Dirichlet characters

$\varphi(q)$ of these

$$L(s,\chi) = \sum_n \chi(n) n^{-s}$$

$$= \prod_p (1-\chi(p)p^{-s})^{-1} \qquad L\text{-functions}$$

The Riemann measure extends to all L-functions

Assuming the Grand Riemann Hypothesis we have

$$\psi(x;q,a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n) = \frac{x}{\varphi(q)} + O(\sqrt{x}(\log x)^2)$$

if $q < \sqrt{x}(\log x)^{-2}$.

$\psi(x;q,a) \sim \frac{x}{\varphi(q)}$ for every $q \leq x^{1-\varepsilon}$