PRIMES! PRIMES! PRIMES!

RUMA talk, 04/08/2025

MERSENNE PRIME

$2^{136,279,841} - 1$, 41 million digits

$2^p - 1$ Mersenne, $2^{11} - 1 = 23 \cdot 89$

FERMAT PRIMES

$F_n = 2^{2^n} + 1$ Fermat conjecture is false

$F_5 = 2^{32} + 1 = 641 \cdot 6700417$ (Euler 1732)

F_0, F_1, F_2, F_3, F_4 only known primes

Conjecture: No more F.P.

F_n is composite if $5 \le n \le 32$.

PROPERTIES

Little Fermat: $a^p \equiv a \pmod p$

Reciprocity Law

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}, \quad \text{if } p, q > 2.$$

$$p \equiv a^2 \pmod q \Leftrightarrow q \equiv b^2 \pmod p, \text{ if } p \equiv 1 \pmod 4$$

$$p = a^2 + b^2 , \quad \text{if } p \equiv 1 \pmod 4$$

$$p \mid (a^2+1) \Rightarrow p \equiv 1 \pmod 4$$

$$p \mid (a^{q-1} + a^{q-2} + \dots + 1) \Rightarrow p \equiv 1 \pmod q$$

$\mathbb{F}_p$ finite field of p elements

$\mathbb{Q}_p$ the field of p-adic numbers.

DISTRIBUTION OF PRIMES

ERATOSTHENES SIEVE (inclusion - exclusion)

EULER PRODUCT

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1} , \text{ if } s > 1,$$

$$\zeta(s) \sim \int_1^{\infty} x^{-s} ds = \frac{1}{s-1} \quad \text{as } s \to 1+$$

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + O(1) = \log \frac{1}{s-1} + O(1)$$

$$\sum_p \frac{1}{p} = \infty.$$

TCHEBYSHEV (1848-52)

$$\theta(x) = \sum_{p \leq x} \log p \asymp x$$

$$\pi(x) = \sum_{p \leq x} 1 \asymp \frac{x}{\log x}$$

PRIME NUMBER THEOREM

$$\pi(x) \sim \frac{x}{\log x}$$

Conjecture by Legendre, Gauss
proved by Hadamard and
de la Vallée Poussin
in 1896

If $\theta(x) \sim \alpha x$, then $\alpha = 1$.
Elementary proof of PNT by Erdős and Selberg.

THE RIEMANN MEMOIR (1859)

$\zeta(s)$ has analytic continuation
with simple pole at $s = 1$

$$(1 - 2^{1-s})\zeta(s) = \sum_{n=1}^{\infty} (-1)^n n^{-s}, \quad \text{if } s = \sigma + it,\ \sigma > 0.$$

$$\zeta(s) \neq 0, \quad \text{if } \sigma > \tfrac{1}{2}$$ the Riemann Hypothesis

$$\theta(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} + O(\log x), \quad \rho = \tfrac{1}{2} + i\gamma \text{ zeros}$$

PRIMES IN ARITHMETIC PROGRESSIONS

$$p \equiv a \pmod{q}, \qquad (a, q) = 1$$

$$\varphi(q) = (\mathbb{Z}/q\mathbb{Z})^* = q \prod_{p \mid q} \left(1 - \frac{1}{p}\right).$$

Dirichlet characters

$$\chi : \mathbb{Z} \to \mathbb{C}$$

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

Dirichlet L-series

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)\, n^{-s} = \prod_{p} (1 - \chi(p) p^{-s})^{-1}$$

$$\sum_{p \equiv a \pmod{q}} \frac{1}{p^s} = \frac{1}{\varphi(q)} \log \frac{1}{s-1} + O(1)$$

Hence primes are equidistributed over the residue classes $a \pmod{q}$ with $(a, q) = 1$.

$$\pi(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1 \sim \frac{1}{\varphi(q)} \frac{x}{\log x}.$$

PRIMES REPRESENTED BY POLYNOMIALS

$$F(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x], \qquad a_n > 0,$$

$F(x)$ irreducible over $\mathbb{Q}$

$F(x)$ has no fixed prime divisors, that is for every p there exists x such that $p \nmid F(x)$.

Example

$$F(x) = x^5 - x + 5 \quad \text{not good.}$$

Then $F(x)$ represents infinitely many primes.

$$|\{n \le X;\ F(n) \text{ is prime}\}| \sim c_F \frac{X}{\log X}.$$

QUADRATIC POLYNOMIALS IN SEVERAL VARIABLES

$$F(x_1, \dots, x_n) = p, \quad \text{if natural conditions hold}$$

$$(x+y)^2 + 1 = p, \quad \text{not covered}$$

SPECIAL POLYNOMIALS

$$m^2 + n^4 = p \qquad \text{(Friedlander + I, 1998)}$$

$$m^3 + 2n^3 = p \qquad \text{(Heath-Brown, 2001)}$$

ZEROS OF $\zeta(s)$

$$\zeta(\rho)=0, \quad \rho=\beta+i\gamma, \quad 0<\beta<1, \quad |\gamma|\leq T.$$

$$\beta < 1-\frac{c}{\log T}, \qquad c>0 \text{ absolute constant}$$

Hence

$$\theta(x) = x + O(x\exp(-c\sqrt{\log x})), \qquad c>0.$$

The RH asserts that $\beta = \frac{1}{2}$. This is equivalent with

$$\theta(x) = x + O(\sqrt{x}(\log x)^2).$$

Hence

$$g_n = p_{n+1} - p_n \ll \sqrt{p_n}\log p_n$$

$$g_n = p_{n+1} - p_n \ll p_n^{0.525} \quad \text{always (Baker+Harman+Pintz)}$$

$$g_n = p_{n+1} - p_n < 600 \quad \text{infinitely often (Maynard)}$$

$$g_n > c\,(\log n)(\log\log n)(\log\log\log\log n)/\log\log\log n$$

$c>0$ by Ford-Green-Konyagin-Maynard-Tao, 2018

c arbitrarily large, \$ 10,000 prize offered by Tao.

$$g_n \ll (\log p_n)^2 \quad \text{always, Cramer's conjecture}$$

SPACING OF ZEROS. Assume the Riemann Hypothesis

$$\rho_n = \frac{1}{2} + i\gamma_n ; \qquad 0 < \gamma_1 \leq \gamma_2 \leq \cdots$$

$$N(T) = |\{ n ;\ 0 < n \leq T \}| \sim \frac{T}{2\pi} \log T$$

$$\gamma_n \sim \frac{2\pi n}{\log n}$$

PAIR CORRELATION OF ZEROS (due to H. Montgomery, 1972)

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

$$\sim c(\alpha, \beta)\, N(T), \quad \text{if } \alpha < \beta, \quad T \to \infty.$$

where

$$c(\alpha, \beta) = \int_\alpha^\beta \left(1 - \left(\frac{\sin \pi x}{\pi x} \right)^2 \right) dx$$

PAIR CORRELATION OF UNITARY MATRIX EIGENVALUES

$U(n)$ unitary $n \times n$ matrix, $U^{-1} = U^* = {}^t\overline{U}$.

$e^{i\theta_1}, \ldots, e^{i\theta_n}$ eigenvalues of $X \in U(n)$

$0 \leq \theta_1 \leq \cdots \leq \theta_n \leq 2\pi$ angles

$f(X) = f(\theta_1, \ldots, \theta_n)$ class function (constant on conjugacy classes) depends only on the angles

Let $f(x)$ be a nice function on $\mathbb{R}$ (vanishes rapidly if $|x| \to \infty$). Put

$$C_n(f) = \frac{1}{n} \int_{U(n)} \sum\sum_{1 \le j < k \le n} f\left(\frac{n}{2\pi}(\theta_j - \theta_k)\right) dX$$

where dX is the Haar measure on $U(n)$. We get by Weyl's integration formula

$$C_n(f) = \frac{1}{2} \int_{-n}^{n} f(x) \left(1 - \left(\frac{\sin \pi x}{n \sin \pi x / n}\right)^2\right) \left(1 - \frac{|x|}{n}\right) dx .$$

Hence the limit as $n \to \infty$ is equal to

$$C(f) = \frac{1}{2} \int_{-\infty}^{\infty} f(x) \left(1 - \left(\frac{\sin \pi x}{\pi x}\right)^2\right) dx$$

This formula was derived by F.J. Dyson in 1962 from

$$\int_{U(n)} |\operatorname{Tr} X^k|^2 \, dX = \min(|k|, n).$$

where

$$\operatorname{Tr} X^k = \lambda_1^k + \cdots + \lambda_n^k = e^{ik\theta_1} + \cdots + e^{ik\theta_n} .$$

Hence

$$|\operatorname{Tr} X^k|^2 = \sum\sum_{1 \le i,j \le n} e\left(\frac{k}{2\pi}(\theta_j - \theta_k)\right) .$$