2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

More Fun with Prime Numbers

Week 2

Sums of Two Squares

Tetsushi Ito

Department of Mathematics
Kyoto University

Fermat and his Theorems (1)

- **Prime Numbers**

  2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499…… (**infinitely many**)

- **Prime Number Thm** is a distribution law.
- Today, it is known that each individual prime number also obeys beautiful laws called **Reciprocity Laws**.

Fermat and his Theorems (2)

Fermat discovered many beautiful laws of prime numbers in the 17th century.

Fermat's Last Theorem

No $X, Y, Z \geq 1$ satisfy

$$X^N + Y^N = Z^N \quad (N \geq 3)$$

It is proved by Wiles in the end of the 20th century by establishing new laws.

Pierre de Fermat (1607?-1665)

Andrew John Wiles (1953-)

https://en.wikipedia.org/wiki/Pierre_de_Fermat
https://en.wikipedia.org/wiki/Andrew_Wiles

Fermat and his Theorems (3)

Fermat's Thm on Sums of Two Squares:
A prime number P is a **sum of two squares** if and only if

P = 2 or P = 4N + 1 (for some N).

Examples

$5=1^2+2^2$ $13=2^2+3^2$ $17=1^2+4^2$ $29=2^2+5^2$

- Observed by Girard in 1625.
- The first complete proof was given by Euler in 1740's.

Fermat and his Theorems (4)

- **Fermat's Thm on Sums of Two Squares** is an extremely influential theorem:
  - Surprising connection between squares and prime numbers
  - The first non-trivial case of the **Reciprocity Laws** on prime numbers
  - Several different proofs

Fermat and his Theorems (5)

Uniqueness: if P can be written as

$$P = X^2 + Y^2 = S^2 + T^2$$

then $(X,Y) = (S,T)$ or (T,S).

Remark

Thm does **not hold** for non-prime numbers:

$$21 = 4 \times 5 + 1 \neq X^2 + Y^2$$

$$65 = 1^2 + 8^2 = 4^2 + 7^2$$

(21 and 65 are **not** prime numbers.)

Interlude: Zagier's proof

Zagier proved it in `one-sentence.'

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. ZAGIER
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{if } x < y - z \\ (2y - x,\ y,\ x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point. □

Don Bernard Zagier (1951-)

Amer. Math. Monthly Vol.97, (No.2) (Feb. 1990)
https://en.wikipedia.org/wiki/Don_Zagier