Sums of Two Squares (1)

- Now we shall prove Fermat's Thm on Sums of Two Squares.

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

$$P = 2 \quad \text{or} \quad P \equiv 1 \pmod 4.$$

Pierre de Fermat (1607?-1665)

Sums of Two Squares (2)

Proof (Step 1): we may assume P is an **odd prime number** ($P \neq 2$), and $P = X^2 + Y^2$. By the following tables, $\mathbf{P \equiv 1 \pmod 4}$.

$X \pmod 4$	0	1	2	3
$X^2 \pmod 4$	0	1	0	1

$Y \pmod 4$	0	1	2	3
$Y^2 \pmod 4$	0	1	0	1

$X \backslash Y$	0	1	2	3
0	0	1	0	1
1	1	2	1	2
2	0	1	0	1
3	1	2	1	2

$X^2 + Y^2 \pmod 4$

Sums of Two Squares (3)

Proof (Step 2): for the converse direction, we put $\mathbf{P = 4N + 1}$ and $\mathbf{A = (2N)!}$.

By **Wilson's Thm**,

$$-1 \equiv (P-1)!$$

$$\equiv 1\times 2\times\cdots\times(2N) \times (2N+1)\times\cdots\times(4N)$$

Since $2N+K \equiv -(2N+1-K)$ (for any K),

$$(P-1)! \equiv (2N)! \times (2N)! \times (-1)^{2N} \equiv A^2.$$

Hence $\mathbf{A^2 \equiv -1 \pmod{P}}$.

Sums of Two Squares (4)

Proof (Step 3): recall $A^2 \equiv -1 \pmod{P}$.

Consider

$$A\,B + C \pmod{P} \quad \text{for} \quad 0 \le B, C < \sqrt{P}.$$

Since the number of pairs (B,C) is > P,

$$\mathbf{A\,B + C \equiv A\,D + E} \pmod{P}$$

for some $0 \le B, C, D, E < \sqrt{P}$, $(B,C) \ne (D,E)$.

Put $X = C - E$ and $Y = D - B$. Then

$$X \equiv A\,Y \;\Rightarrow\; X^2 \equiv A^2\,Y^2 \equiv -Y^2 \;\Rightarrow\; \mathbf{X^2 + Y^2 \equiv 0}.$$

Since $X^2 + Y^2 < 2P$, $\mathbf{X^2 + Y^2 = P}$.

Summary of Week 2

- Fermat and his Theorems:
  - Reciprocity Laws
  - Sums of Two Squares
- Modular Arithmetic
- Fermat's Little Thm, Wilson's Thm, Lagrange's Thm
- Proof of Fermat's Thm on Sums of Two Squares.

Plan of Week 3

We will learn more general Reciprocity Laws; the Quadratic Reciprocity Law of Gauss, and its generalizations.
Let’s discover hidden laws of prime numbers.
See you next week!

Carl Friedrich Gauss (1777-1855)