Fun with Prime Numbers

Invitation to the Mysterious World of Mathematics

Tetsushi Ito

Department of Mathematics,
Kyoto University

Congruences

Definition

Let $N \geqq 1$, A,B be integers. If $A-B$ is divisible by N, we say

'A,B are congruent modulo N',

and we write

$$A \equiv B \pmod{N}.$$

Congruences (2)

- If $A \equiv B$, $C \equiv D \pmod{N}$, then we have

$$A+C \equiv B+D \pmod{N},$$
$$A-C \equiv B-D \pmod{N},$$
$$AC \equiv BD \pmod{N}.$$

- For a prime number P,

$$(P-1)! \equiv -1 \pmod{P}$$

(Wilson's theorem)

<u>Example</u> (P=5)

$$(5-1)! = 4 \times 3 \times 2 \times 1 = 24 \equiv -1 \pmod{5}$$

Sums of squares

<u>Proposition</u>

An integer congruent to 3 modulo 4 cannot be written as a sum of two squares.

- X : integer, $X \equiv 0,1,2,3 \pmod 4$.

⇨ $X^2 \equiv 0,1,4,9 \pmod 4$.

⇨ $X^2 \equiv 0,1 \pmod 4$ because $4 \equiv 0$ and $9 \equiv 1$.

- X,Y : integer, $X^2+Y^2 \equiv 0,1,2 \pmod 4$.

  X^2+Y^2 cannot be congruent to 3 modulo 4.

Sums of squares (2)

<u>Proposition</u> (First supplement law)
Let P be a prime number congruent to 1 mod 4.
Then, there is an integer A with

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

Write $P = 4K+1$. Put $A = (2K)!$.

By Wilson's theorem, $(P-1)! \equiv -1 \pmod{P}$.

Then, $A^2 \equiv (2K)! \times (-1)^{2K} (4K)!/(2K)!$

$$\equiv (P-1)! \equiv -1 \pmod{P}$$

Sums of squares (3)

- We shall give a proof of Fermat's theorem on sums of two squares.
- Let P be a prime number with $P \equiv 1 \pmod 4$. By Proposition, take A with $A^2 \equiv -1 \pmod P$.
- Take the largest integer B satisfying $B^2 < P$.
- There are $(B+1)^2$ pairs (X,Y) with $0 \leq X,Y \leq B$. Since the number of pairs is $(B+1)^2 > P$, there are $(X,Y) \neq (U,V)$ with

$$X+AY \equiv U+AV \pmod P.$$

Sums of squares (4)

- Recall: $X+AY \equiv U+AV$.
- Put $S=X-U$, $T=Y-V$. Then $S\equiv -AT$. Hence $S^2\equiv -T^2$, and,

$$S^2+T^2 \equiv 0 \pmod{P}.$$

- On the other hand, since $0\leq|S|,|T|\leq B$, we have

$$0 < S^2+T^2 < 2B^2 < 2P.$$

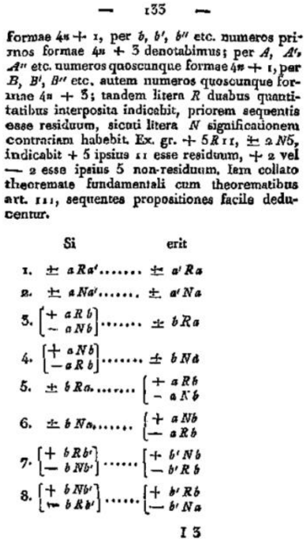
- Hence we conclude $S^2+T^2=P$. The prime number P is the sum of two squares.

This week

- We consider the remainder of a prime number when we divide it by 4.
- Dirichlet's theorem on arithmetic progressions and Fermat's theorem on sums of two squares.
- Congruences, Wilson's theorem.
- Proof of Fermat's theorem on sums of two squares.

Plan of the next week

Fermat's theorem on sums of two squares is just the tip of the iceberg. In the next week, we shall study more general laws of prime numbers, Reciprocity Laws, and discuss open problems and recent developments. See you next week!


— 133 —

formae $4n+1$, per b, b', b'' etc. numeros primos formae $4n+3$ denotabimus; per A, A', A'' etc. numeros quoscunque formae $4n+1$, per B, B', B'' etc. autem numeros quoscunque formae $4n+3$; tandem litera R duabus quantitatibus interposita indicabit, priorem sequentis esse residuum, sicuti litera N significationem contrariam habebit. Ex. gr. $+5R11$, $\pm 2N5$, indicabit $+5$ ipsius 11 esse residuum, $+2$ vel -2 esse ipsius 5 non-residuum. Iam collato theoremate fundamentali cum theorematibus art. 111, sequentes propositiones facile deducentur.

	Si		erit
1.	$\pm aRa'$	....	$\pm a'Ra$
2.	$\pm aNa'$	....	$\pm a'Na$
3.	$\begin{bmatrix} +aRb \\ -aNb \end{bmatrix}$	....	$\pm bRa$
4.	$\begin{bmatrix} +aNb \\ -aRb \end{bmatrix}$	....	$\pm bNa$
5.	$\pm bRa$	....	$\begin{bmatrix} +aRb \\ -aNb \end{bmatrix}$
6.	$\pm bNa$	....	$\begin{bmatrix} +aNb \\ -aRb \end{bmatrix}$
7.	$\begin{bmatrix} +bRb' \\ -bNb' \end{bmatrix}$	......	$\begin{bmatrix} +b'Nb \\ -b'Rb \end{bmatrix}$
8.	$\begin{bmatrix} +bNb' \\ -bRb' \end{bmatrix}$	......	$\begin{bmatrix} +b'Rb \\ -b'Na \end{bmatrix}$

13

'Disquisitiones Arithmeticae'
C. F. Gauss (1801)