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 3

The Reciprocity Laws

Tetsushi Ito

Department of Mathematics
Kyoto University

Gauss and his Reciprocity Laws (1)

Fermat's Thm on Sums of Two Squares

A prime number P is a **sum of two squares** if and only if

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

- Fermat generalized it in several directions.

Pierre de Fermat (1607?-1665)

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

Gauss and his Reciprocity Laws (2)

- For example, Fermat proved:

Theorem

A prime number P is

$$P = X^2 + 3 \times Y^2 \quad \text{for some } X, Y$$

if and only if

$$P = 3 \quad \text{or} \quad P \equiv 1 \pmod 3.$$

- The **Quadratic Reciprocity Law** is a further generalization of Fermat's theorems.

Carl Friedrich Gauss (1777-1855)

https://en.wikipedia.org/wiki/Carl_Friedrich_Gauss

Gauss and his Reciprocity Laws (3)

- For a given integer A, the **Quadratic Reciprocity Law** (**QRL**) determines when

  $$A \equiv X^2 \pmod{P}$$ for some X.

- QRL was conjectured by Euler and Legendre.

Leonhard Euler (1707-1783)

Adrien-Marie Legendre (1752-1833)

https://en.wikipedia.org/wiki/Leonhard_Euler
https://en.wikipedia.org/wiki/Adrien-Marie_Legendre

Gauss and his Reciprocity Laws (4)

- The first proof of QRL was given by Gauss when he was 19 years old.
  (19 is a prime number!)
- Gauss called it
  the`**Golden Theorem**.'
- He gave (at least) 8 different proofs in his life.

Carl Friedrich Gauss
(1777-1855)

Gauss and his Reciprocity Laws (5)

Definition

Let A be an integer not divisible by P.

We say A is **Quadratic Residue (mod P)** if

$$A \equiv X^2 \pmod{P}$$ for some X.

Example (P=7)

- $2 \equiv 9 \equiv 3^2 \pmod{7} \Rightarrow$ 2 is **QR** (mod 7)
- $5 \not\equiv X^2 \pmod{7}$ for any X

  $\Rightarrow$ 5 is **not QR** (mod 7)

Gauss and his Reciprocity Laws (6)

Examples (P=7, continued)

$X \pmod 7$	0	1	2	3	4	5	6
$X^2 \pmod 7$	0	1	4	2	2	4	1

- 1, 2, 4 are **QR** (mod 7),
- 3, 5, 6 are **not QR** (mod 7).

Gauss and his Reciprocity Laws (7)

Definition (**Legendre symbol**)

For a prime number P and an integer A,

$$\left(\frac{A}{P}\right) = \begin{cases} 0 & \text{if A is divisible by P} \\ 1 & \text{if A is QR (mod P)} \\ -1 & \text{if A is not QR (mod P)} \end{cases}$$

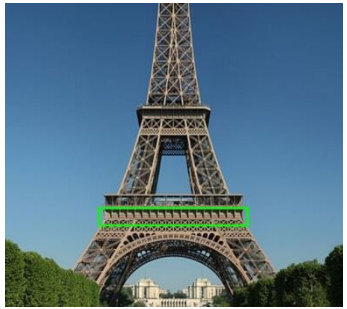
Example (P=7)

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1 \qquad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

Adrien-Marie Legendre
(1752-1833)

Interlude: Who is Legendre? (1)

For 200 years, a black-and-white portrait of a person showing his profile had been used as the portrait of Adrien-Marie Legendre. However, he was not Adrien-Marie!



Adrien-Marie Legendre **(???)**

https://en.wikipedia.org/wiki/List_of_the_72_names_on_the_Eiffel_Tower
https://en.wikipedia.org/wiki/Adrien-Marie_Legendre

Interlude: Who is Legendre? (2)

He was Louis Legendre, a French politician. The error was found in 2005. The portrait of Adrien-Marie Legendre was found in 2008.

Louis Legendre
(1752-1797)

Adrien-Marie Legendre
(1752-1833)

https://en.wikipedia.org/wiki/Adrien-Marie_Legendre