



# THEOREM OF THE DAY

**Gauss's Law of Quadratic Reciprocity** For a positive integer  $a$  and odd prime  $p$  not a multiple of  $a$ , let the Legendre symbol  $\left(\frac{a}{p}\right)$  be defined by:  $\left(\frac{a}{p}\right) = 1$ , if the congruence equation  $x^2 \equiv a \pmod{p}$  is solved by some integer  $x$ ; otherwise  $\left(\frac{a}{p}\right) = -1$ . Then for odd primes  $p$  and  $q$  we have

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & p \equiv q \equiv 3 \pmod{4} \end{cases}$$

The quadratic equation  $x^2 \equiv 12007 \pmod{49499}$  is hereby solvable!

$$\begin{aligned} &\stackrel{\equiv 3 \pmod{4}}{\left(\frac{12007}{49499}\right)} \stackrel{=4 \times 12007 + 1471}{=} -\stackrel{\equiv 3 \pmod{4}}{\left(\frac{49499}{12007}\right)} \stackrel{=8 \times 1471 + 239}{=} -\stackrel{\equiv 3 \pmod{4}}{\left(\frac{1471}{12007}\right)} \stackrel{=6 \times 239 + 37}{=} +\stackrel{\equiv 3 \pmod{4}}{\left(\frac{12007}{1471}\right)} \stackrel{=5 \times 239 + 37}{=} \left(\frac{239}{1471}\right) \stackrel{=6 \times 239 + 37}{=} -\left(\frac{1471}{239}\right) \\ &\stackrel{\equiv 3 \pmod{4}}{=} -\stackrel{\equiv 1 \pmod{4}}{\left(\frac{37}{239}\right)} \stackrel{=6 \times 37 + 17}{=} -\stackrel{\equiv 1 \pmod{4}}{\left(\frac{239}{37}\right)} \stackrel{=2 \times 17 + 3}{=} -\stackrel{\equiv 3 \pmod{4}}{\left(\frac{17}{37}\right)} \stackrel{=5 \times 3 + 2}{=} -\stackrel{\equiv 1 \pmod{4}}{\left(\frac{37}{17}\right)} \stackrel{=5 \times 3 + 2}{=} -\stackrel{\equiv 1 \pmod{4}}{\left(\frac{3}{17}\right)} \stackrel{=5 \times 3 + 2}{=} -\left(\frac{17}{3}\right) \stackrel{=5 \times 3 + 2}{=} -\left(\frac{2}{3}\right) = +1 \end{aligned}$$

Ach so! But I can prove it!



The figure shows a long sequence of inversions (via the theorem) and reductions (via the fact that  $\left(\frac{a \times p + b}{p}\right) = \left(\frac{b}{p}\right)$ ) which in this case takes us all the way down to an easily checked case:  $\left(\frac{2}{3}\right) = -1$ , i.e. no square has remainder 2 when divided by 3 (Fermat's Little Theorem is one way of confirming this). There are three reversals of sign in the reduction (where  $p \equiv q \equiv 3 \pmod{4}$ ) so the original symbol has value  $(-1)^3 \times -1 = 1$  and the original quadratic equation has a solution (in fact, solutions come in pairs and  $x^2 \equiv 12007 \pmod{49499}$  is solved by  $x = 16419$  and  $x = 33080$ ).

A version of the theorem was conjectured by Leonhard Euler in 1783. Adrien-Marie Legendre responded to the challenge in 1785 and deserves credit for its first full statement (in the form  $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$ ). He gave an incorrect proof, however, and was aggrieved when Carl Friedrich Gauss, giving the first correct proof in 1796, claimed the theorem as his own.

**Web link:** [www.math.nmsu.edu/~history/schauspiel/schauspiel.html](http://www.math.nmsu.edu/~history/schauspiel/schauspiel.html). The image of Legendre, above left, comes with an interesting little story courtesy of [www.numericana.com/answer/record.htm#legendre](http://www.numericana.com/answer/record.htm#legendre).

**Further reading:** *Elementary Number Theory* by Gareth Jones and Mary Jones, Springer, Berlin, 1998.

