CUBIC RECIPROCITY

By Kyle and Moose

Question: Does $X^3 \equiv p \pmod{q}$ have a solution?

Recall a similar question, $x^2 \equiv a \pmod{b}$**, being the basis of quadratic reciprocity.**
We used the Legendre symbol to determine whether $x^2 \equiv a \pmod{b}$ **has a solution, assuming b is an odd prime.**

History of cubic reciprocity

- Euler was the fist known mathematician to work on this idea.
- The earliest proofs and theorems about cubic reciprocity were found dating back to around 1814, but it is unclear whether they were done by Gauss or Eisenstein.
- The first ever official proofs were published in 1844 by Eisenstein.

The Eisenstein Integer Ring

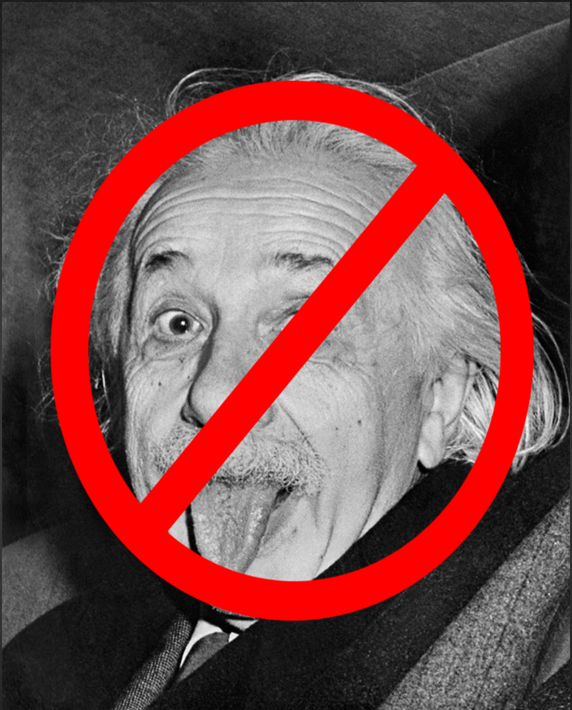
- The Eisenstein integer ring is often denoted as $\mathbb{Z}[\omega]$.
- The ring is defined as $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$.

The Eisenstein Integer Ring Cont.

The ω symbol is equal to $\frac{-1+i\sqrt{3}}{2}$, which is equivalent to $e^{\frac{2\pi}{3}}$ as well. Also note that $\omega^3 = 1$.

Units of the Eisenstein integer ring

The units of the ring are $\pm 1, \pm \omega,$ **and** $\pm \omega^2$**.**



Primary in Eisenstein Ring

A number p is prime in $\mathbb{Z}[\omega]$ if $gcd(p, 3) = 1$ and $p \equiv b \in \mathbb{Z} \pmod{1 - \omega^2}$. In other words, $p \equiv \pm 2 \pmod{3}$ if $gcd(N(a), 3) = 1$, where N is the norm, then a times some unit is primary.

Norm Function

The norm function is defined as $N(a+b\omega) = a^2 - ab + b^2$. This will always be congruent to 0 **or** $1 \pmod 3$**.**

Cubic residues

$x^3 \equiv a \pmod{p}$**: if this equation has an integer solution for** a**, then** a **is a cubic residue. Conversely, if it does not it is a cubic non-residue.**

Sets of Residues

- (mod 7):0,1,2,3,4,5,6
- quadratic residues:0,1,4,2,2,4,1
- cubic residues:0,1,1,6,1,6,6
- quartic residues:0,1,2,4,4,2,1

Similarly to the Legendre symbol, $[\frac{m}{n}]_3 = 1$ if m is a cubic residue, and -1 if m is not a cubic residue. This is used under $\pmod{n}$ and m and n are integers.

The Jacobi Symbol is a generalization of the Legendre Symbol, a is an integer and n is an odd integer then $\left(\frac{a}{n}\right)$ is equal to the Legendre's of the prime factorization.

Cubic residues

Determining the cubic symbol can be difficult. Euler created some rules to apply when working with a prime $p \equiv 1 \pmod{3}$. p would also follow the form $p = a^2 + 3b^2$.

The Rules

- $[\frac{2}{p}]_3 = 1 \leftrightarrow 3|b$
- $[\frac{3}{p}]_3 = 1 \leftrightarrow 9|b$ or $9|(a \pm b)$
- $[\frac{5}{p}]_3 = 1 \leftrightarrow 15|b$, or $3|b$ and $5|a$, or $15|(a \pm b)$, or $15|(2a \pm b)$
- $[\frac{6}{p}]_3 = 1 \leftrightarrow 9|b$ or $9|(a \pm 2b)$
- $[\frac{7}{p}]_3 = 1 \leftrightarrow 3|b$ and $7|a$, or $21|(b \pm a)$, or $7|(4b \pm a)$, or $21|b$, or $7|b(b \pm 2a)$

Let $h = a + b\omega$ **be primary,** $a = 3m + 1$ **and** $b = 3n$**. Then**

$$[\frac{\omega}{h}]_3 = \omega^{-m-n}$$

$$[\frac{1-\omega}{h}]_3 = \omega^{m}$$

$$[\frac{3}{h}]_3 = \omega^{n}$$

If $a \equiv b \pmod{p}$**, where p is prime, then**

$$\left[\frac{a}{p}\right]_3 = \left[\frac{b}{p}\right]_3$$

$$\left[\frac{ab}{p}\right]_3 = \left[\frac{a}{p}\right]_3 \left[\frac{b}{p}\right]_3$$

$$\overline{\left[\frac{a}{p}\right]_3} = \left[\frac{\bar{a}}{p}\right]_3$$

$x^3 = a \pmod{p}$ **has a solution in the Eisenstein Integers if and only if** $[\frac{a}{p}]_3 = 1$**.**

Given c **and** d **are integers and** $gcd(c, d) = gcd(d, 3) = 1$**, then** $[\frac{c}{d}]_3 = 1$**.**

Theorem: p **and** q **are primary numbers in the Eisenstein Ring and** $x^3 \equiv p \pmod{q}$ **has a solution if and only if** $x^3 \equiv q \pmod{p}$ **has a solution.**

The Law of Cubic Reciprocity

(restatement of previous slide :))

Let a and b be relatively prime and primary in Eisenstein's integers. Then $[\frac{a}{b}]_3 = [\frac{b}{a}]_3$.

BY: KYLE AND MOOSE