Reciprocity laws and their rational variants

Louis Dumont

INRIA, France

December 15, 2015

Reciprocity laws: from Legendre to Lehmer

turn left after Artin

Fundamental problem

Problem

Parameter: $k \in \mathbb{N}^\star$ a positive integer.

Let $x \in \mathbb{Z}$ be an integer and $p \in \mathbb{N}$ a prime number.

Does there exist $y \in \mathbb{Z}$ such that $x = y^k \mod p$?

Answers (but not really...but still...but actually not): Reciprocity laws

Aim of the talk:

- Use the problem as an excuse to explore the beautiful world of reciprocity laws.
- Good methods for the cases $k = 2$ and $k = 3$.

Naive method

Naive algorithm that works for any value of k:

- for all $y \in \mathbb{F}_p$, test wether $x = y^k$ or not.
- if a $y \in \mathbb{F}_p$ such that $x = y^k$ is found, the answer to the problem is "yes", otherwise it is "no"

Can we do better ?

The quadratic reciprocity law ($k=2$)

Fact: there exists a quadratic residue symbol $\left(\frac{p}{q}\right) \in \{-1, 1\}$ with the following properties.

Quadratic residue symbol

- $\left(\frac{p}{q}\right) = 1 \Leftrightarrow p$ is a square modulo q
- $\left(\frac{p_1 p_2}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)$

Quadratic reciprocity law (Legendre, Gauss)

if p and q are odd primes, then

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Example

$$\left(\frac{p_1 p_2}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) \quad \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

<u>Question:</u> is 13 a square modulo 137 ?

$$\begin{aligned}\left(\frac{13}{137}\right) = \left(\frac{137}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{13}{7}\right) \\ = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1\end{aligned}$$

<u>Answer</u>: 13 is not a square modulo 137.

More general reciprocity laws

- Quadratic reciprocity law: $k = 2$
- Eisenstein reciprocity law: any prime k but with special algebraic integers

Eisenstein reciprocity law

$$\left(\frac{\pi_1}{\pi_2}\right)_k = \left(\frac{\pi_2}{\pi_1}\right)_k$$

π_1, π_2 are primes in $\mathbb{Z}[\zeta]$, with ζ a primitive k-th root of unity

- Hilbert and Artin reciprocity laws: even more general, even more abstract

Rational reciprocity laws

- Quartic and octic reciprocity laws
- Rational cubic reciprocity: Euler, Jacobi, Lehmer,...

There is no known general rational reciprocity law.

From now on, we focus on the case $k = 3$.

Cubic reciprocity

Cubic reciprocity law (draft version)

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$$

π_1, π_2 are primes in $\mathbb{Z}[\omega]$, with ω a primitive third root of unity

Theorem (Euler, Jacobi)

Let p be a prime such that $p \equiv 1 \mod 3$. Let $q \in \{2, 3, 5, 7\}$.
Then p can be written $4p = A^2 + 27B^2$ and

$$q \text{ is a cube modulo } p \iff q \text{ divides } A \text{ or } B$$

The arithmetic of $\mathbb{Z}[\omega]$ (Eisenstein integers)

The ring $\mathbb{Z}[\omega]$ (Eisenstein integers)

From now on, ω is a primitive third root of unity: $1 + \omega + \omega^2 = 0$.

$\mathbb{A} := \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ is an Euclidean domain.

It has among other things:

- Euclidean division
- congruences
- prime numbers
- prime factorisation
- greatest common divisors
- the norm function

The norm function

If $\alpha = a + b\omega \in \mathbb{A}$, the norm of α is

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = a^2 - ab + b^2$$

The norm function, invertible elements

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = a^2 - ab + b^2$$

Properties of the norm

- $\mathrm{N}(\alpha) \in \mathbb{Z}$
- $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$
- α is invertible in $\mathbb{A} \Leftrightarrow \mathrm{N}(\alpha) = 1$
- if $N(\alpha)$ is prime in $\mathbb{Z}$, then α is prime in $\mathbb{A}$

<u>Invertible elements:</u> $\mathbb{A}^\times = \left\{\pm 1, \pm\omega, \pm\omega^2\right\}$

Remark: $\omega^2 = -1 - \omega$

Prime eisenstein integers

Some prime rational integers are not prime anymore in $\mathbb{A}$!
Example: $3 = -\omega^2(1-\omega)^2 \quad 7 = -(1+3\omega)(2+3\omega)$

Primes of $\mathbb{Z}[\omega]$

Let $p \in \mathbb{Z}$ be a rational prime integer.

- if $p \equiv 2 \mod 3$, then p is prime in $\mathbb{A}$
- if $p \equiv 1 \mod 3$, then $p = \pi_1\pi_2$, where π_1 and π_2 are prime in $\mathbb{A}$
- if $p = 3$, then $3 = -\omega^2(1-\omega)^2$ and $1-\omega$ is prime in $\mathbb{A}$

Primary primes

Definition (Primary primes)

If $p \in \mathbb{Z}$ is a prime such that $p \equiv 1 \mod 3$, then p can be uniquely written (up to conjugation) $p = \pi\overline{\pi}$, where $\pi = a + b\omega$ with

$$a \equiv 1 \mod 3 \qquad b \equiv 0 \mod 3$$

The **primary** primes are the primes π as above and the rational primes $p \equiv 2 \mod 3$

Corollary

if $p \in \mathbb{Z}$ is prime and $p \equiv 1 \mod 3$, then p has a unique decomposition

$$4p = A^2 + 27B^2$$

<u>Proof:</u> write $p = \pi\overline{\pi}$ and $\pi = a + b\omega$ with $b \equiv 0 \mod 3$.
then $4p = 4(a^2 - ab + b^2) = (2a - b)^2 - 3b^2$

Example

$p = 13 = (-4-\omega)\overline{(-4-\omega)} = (-4-\omega)(-3+\omega)$

$\pi = (-3+\omega)$ is **not** primary. Its associates are:

- $\pi = -3+\omega$
- $-\pi = 3-\omega$
- $\omega\pi = -1-4\omega$
- $-\omega\pi = 1+4\omega$
- $\omega^2\pi = 4+3\omega$
- $-\omega^2\pi = -4-3\omega$

The only primary one is $4+3\omega$

Congruences and residue fields in $\mathbb{A}$

How to compute $\alpha = a + b\omega$ modulo π in $\mathbb{A}$?

First case: $p \equiv 2 \mod 3$
If $a \equiv \tilde{a} \mod p$ and $b \equiv \tilde{b} \mod p$ then $a + b\omega \equiv \tilde{a} + \tilde{b}\omega \mod p$

$\mathbb{A}/p\mathbb{A} = \mathbb{F}_p[\omega]$ is the field with p^2 elements

Second case: $p \equiv 1 \mod 3$ and $p = \pi\overline{\pi}$
write $\pi = \mu + \lambda\omega$. then

- $p \equiv 0 \mod \pi$
- $\omega \equiv -\frac{\mu}{\lambda} \mod \pi$

conclusion: $a + b\omega \equiv a - b\frac{\mu}{\lambda} \mod \pi$

$\mathbb{A}/p\mathbb{A} = \mathbb{F}_p$ is the field with p elements

Example

$p = 7 = \pi\overline{\pi}$, with $\pi = 1 + 3\omega$.

Then $1 + 3\omega \equiv 0 \mod \pi \Longrightarrow \omega \equiv -\frac{1}{3} \equiv 2 \mod \pi$

conclusion: $a + b\omega \equiv a + 2b \mod \pi$ for any a and b

for instance: $23 + 10\omega \equiv 2 + 3\omega \equiv 8 \equiv 1 \mod 1 + 3\omega$

The cubic reciprocity law

Cubic residue symbol

- $\left(\frac{\pi_1}{\pi_2}\right)_3 \in \left\{1, \omega, \omega^2\right\}$
- $\left(\frac{\pi_1}{\pi_2}\right)_3 = 1 \Leftrightarrow \pi_1$ is a cube modulo π_2
- $\left(\frac{\pi_1 \pi_2}{\pi_3}\right)_3 = \left(\frac{\pi_1}{\pi_3}\right)_3 \left(\frac{\pi_2}{\pi_3}\right)_3$
- $\overline{\left(\frac{\pi_1}{\pi_2}\right)_3} = \left(\frac{\overline{\pi_1}}{\overline{\pi_2}}\right)_3$

Cubic reciprocity law (Gauss, Eisenstein)

If π_1 and π_2 are two non-associated **primary** primes of $\mathbb{A}$, then

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$$

Rational cubic reciprocity

Rational cubic reciprocity for $q = 2$

Question: p is given. Is 2 a cube modulo p ?

Easy case: when $p \equiv 2 \mod 3$, every element of $\mathbb{F}_p$ is a cube.
From now on, $p \equiv 1 \mod 3$, $p = \pi\overline{\pi}$ with $\pi = a + b\omega$ primary.

- since $\mathbb{A}/\pi\mathbb{A} = \mathbb{F}_p$, 2 is a cube mod $p \Leftrightarrow$ 2 is a cube mod π
- 2 is a cube mod $\pi \Leftrightarrow \left(\frac{2}{\pi}\right)_3 = 1 \Leftrightarrow \left(\frac{\pi}{2}\right)_3 = 1 \Leftrightarrow \pi$ is a cube mod 2

$\mathbb{A}/2\mathbb{A} = \mathbb{F}_2[\omega]$ et $\mathbb{F}_2[\omega]^3 = \{0, 1\}$

Conclusion: 2 is a cube mod $p \Leftrightarrow b \equiv 0 \mod 2$

Reminder: $4p = (2a - b)^2 + 3b^2 = A^2 + 27B^2$

2 is a cube mod $p \Leftrightarrow A$ and B are even

Example

Question: Is 2 a cube modulo 157 ?

$4 \times 157 = 628 = 14^2 + 27 \times 4^2$
14 and 4 are even $\Rightarrow$ 2 is a cube modulo 157

indeed: $62^3 \equiv 2 \mod 157$

Problem

- How to compute the decomposition $4p = A^2 + 27B^2$ efficiently ?

Other formulation:

- How to compute π such that $p = \pi\overline{\pi}$ efficiently ?

Efficient computation of the Eisenstein decomposition

Proposition

Let $p \equiv 1 \mod 3$ be a prime.

- There exists $c \in \mathbb{Z}$ such that $1 + c + c^2 \equiv 0 \mod p$
- The Eisenstein integer $\pi = \gcd(p, \omega - c)$ is a prime that satisfies $p = \pi\overline{\pi}$

Example: $p = 157 \to c = 12$
Euclidean algorithm: only one step! $157 = (\omega - 12)(-13 - \omega)$

the primary prime associated to $\omega - 12$ is $\pi = 13 + 12\omega$

Check: $A = 2 \times 13 - 12 = 14 \qquad B = 12/3 = 4$

Epilogue

- What about cubic rational reciprocity for other values of q ?

The computations are more complicated, but everything works the same. There is a family of theorems:

Theorem

Let $q \in \mathbb{Z}$ be a prime. Then, for all primes $p \equiv 1 \mod 3$ with decomposition $4p = A^2 + 27B^2$,

$$q \text{ is a cube mod } p \iff \text{a set of congruences on } A \text{ and } B \text{ mod } q$$

- What about rational reciprocity laws for higher odd powers ?

The method doesn't work for higher powers, because $\mathbb{Z}[\zeta]$ is not always a Euclidean domain. The question remains open.