The Cubic and biquadratic reciprocity laws

Is there a reciprocity law for n-th powers, for $n>2$?
In concrete terms, given $a \in \mathbb{Z}\setminus\{0\}$, is there a rule determining whether the congruence $x^n \equiv a \pmod p$ is solvable (i.e., whether $\bar a = a \pmod p \in \mathbb{F}_p^{\times n}$), for a variable prime $p \nmid a$?

We know that $\mathbb{F}_p^{\times n} = \mathbb{F}_p^{\times m}$, where $m = \gcd(n, p-1)$, so the only interesting case is $m = n$ ($\iff p \equiv 1 \pmod n$).

Generalised Euler criterion: if $p \equiv 1 \pmod n$, $\mathbb{F}_p^\times$ is cyclic of order $p-1$, hence both $\mathbb{F}_p^\times / \mathbb{F}_p^{\times n}$ and $\mathbb{F}_p^\times[n] = \{x \in \mathbb{F}_p^\times \mid x^n = 1\}$ are cyclic of order n, and the map

$$\begin{array}{ccc} \mathbb{F}_p^\times / \mathbb{F}_p^{\times n} & \xrightarrow{\sim} & \mathbb{F}_p^\times[n] \\ \downarrow & & \downarrow \\ \bar a \bmod \mathbb{F}_p^{\times n} & \longmapsto & a^{\frac{p-1}{n}} \end{array}$$

is an isomorphism of groups.
In particular, $\bar a \in \mathbb{F}_p^{\times n} \iff a^{\frac{p-1}{n}} \equiv 1 \pmod p$.

Ex: ($p \neq 2$) $-1 \in \mathbb{F}_p^{\times n} \iff (-1)^{\frac{p-1}{n}} \equiv 1 \pmod p \iff (-1)^{\frac{p-1}{n}} = 1 \iff p \equiv 1 \pmod{2n}$

From now on: $n = 3$ or 4 (and $p \equiv 1 \pmod n$)

$n=3$: $a \in \mathbb{F}_p^{\times 3} \iff -a \in \mathbb{F}_p^{\times 3}$

$n=4$: $a \in \mathbb{F}_p^{\times 4} \iff \left(\frac{a}{p}\right) = 1$ and both solutions of $(\pm b)^2 \equiv a \pmod p$ satisfy $\left(\frac{\pm b}{p}\right) = 1$.

($\left(\frac{-1}{p}\right) = 1$ if $n=4$, since $p \equiv 1 \pmod n$)

Euler: observed experimentally (but was unable to prove) that:

(1) If $p \equiv 1 \pmod 3$, then: $2 \in \mathbb{F}_p^{\times 3} \overset{?}{\iff} p = x^2 + 27y^2$

(2) If $p \equiv 1 \pmod 4$, then: $2 \in \mathbb{F}_p^{\times 4} \overset{?}{\iff} p = x^2 + 64y^2$ $\quad (x, y \in \mathbb{Z})$

What is going on? What if we replace 2 by another integer?

Numerical experiments: $\pm 3, \pm 5 \overset{?}{\in} \mathbb{F}_p^{\times 4}$ $\quad (5 \neq p \equiv 1 \pmod 4)$

Note: $-3 \in \mathbb{F}_p^{\times 4} \Rightarrow \left(\frac{-3}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod 3 \Rightarrow p \equiv 1 \pmod{12}$

$3 \in \mathbb{F}_p^{\times 4} \Rightarrow \left(\frac{3}{p}\right) = 1 \Uparrow \leftarrow \left(\frac{-1}{p}\right) = 1$

$5 \in \mathbb{F}_p^{\times 4} \Rightarrow \left(\frac{5}{p}\right) = 1 \Rightarrow \left(\frac{p}{5}\right) = 1 \Rightarrow p \equiv \pm 1 \pmod 5 \Rightarrow p \equiv 1, 9 \pmod{20}$

$-5 \in \mathbb{F}_p^{\times 4} \Rightarrow \left(\frac{-5}{p}\right) = 1 \Uparrow$

$-1 \in \mathbb{F}_p^{\times 4} \iff p \equiv 1 \pmod 8$

How do we check whether $3 \in \mathbb{F}_p^{\times 4}$? Either we compute $3^{\frac{p-1}{4}} \pmod p$ using the binary expansion of $\frac{p-1}{4}$ and successive squarings ($3^{20} = 3^{16+4} = (((3^2)^2)^2)^2 (3^2)^2$) and checking whether $3^{\frac{p-1}{4}} \equiv 1 \pmod p$, or we try to find b such that $b^2 \equiv 3 \pmod p$ & computing several random values of $a^2 \pmod p$ ($p=37$: $5^2 \equiv -12$, $6^2 \equiv -1$ $\Rightarrow 3 \equiv (5/12)^2$, $1/12 \equiv -3$, $5/12 \equiv -15$) and checking $\left(\frac{b}{p}\right) \stackrel{?}{=} 1$.

Results:

$p \equiv 1 \pmod{12}$:

p	13	37	61	73	97	109	157
$-3 \in \mathbb{F}_p^{\times 4}$		YES	YES				YES
$3 \in \mathbb{F}_p^{\times 4}$	YES					YES	

Do the answers depend only on $p \pmod{12M}$? Not for $M = 1, 2, 3, 4, 5, 6$.

$p \equiv 1, 9 \pmod{20}$

p	29	41	61	89	101	109	149	
$5 \in \mathbb{F}_p^{\times 4}$					YES	YES	YES	
$-5 \in \mathbb{F}_p^{\times 4}$	YES		YES					

Do the answers depend only on $p \pmod{20N}$? Not for $N = 1, 2, 3, 4, 6$.

What is going on? As in Euler's observation on $\left[2 \in \mathbb{F}_p^{\times 4} \stackrel{?}{\Leftrightarrow} p = x^2 + 64y^2\right]$ we need to consider not only p but its decomposition $p = u^2 + v^2 = (u+iv)(u-iv)$ in $\mathbb{Z}[i]$. We assume that $2 \nmid u$, $2 \mid v$ (which still gives us a freedom to replace u by $-u$ and/or v by $-v$). In terms of this decomposition, $u^2 \equiv 1 \pmod 8$ and $v^2 \equiv \begin{cases} 0 \\ 4 \end{cases} \pmod 8$ if $\begin{cases} 4 \mid v \\ 4 \nmid v \end{cases}$, which means that

$-1 \in \mathbb{F}_p^{\times 4} \Leftrightarrow p (= u^2 + v^2) \equiv 1 \pmod 8 \Leftrightarrow 4 \mid v$.

Results revisited: $p = u^2 + v^2$, $2 \nmid u$, $2 \mid v$

p	13	37	61	73	97	109	157
$\pm u$	3	1	5	3	9	3	11
$\pm v$	2	6	6	8	4	10	6
$-3 \in \mathbb{F}_p^{\times 4}$		YES	YES				YES
$3 \in \mathbb{F}_p^{\times 4}$	YES					YES	

It looks as if:

$$-3 \in \mathbb{F}_p^{\times 4} \overset{?}{\iff} 6 \mid v \iff p = x^2 + 36y^2$$

$$3 \in \mathbb{F}_p^{\times 4} \overset{?}{\iff} \begin{cases} -3 \in \mathbb{F}_p^{\times 4} \wedge -1 \in \mathbb{F}_p^{\times 4} \iff 6 \mid v \wedge 4 \mid v \iff 12 \mid v \iff p = x^2 + 144y^2 \\ \text{OR} \\ -3 \notin \mathbb{F}_p^{\times 4} \wedge -1 \notin \mathbb{F}_p^{\times 4} \iff 3 \nmid u \wedge 4 \nmid v \iff p = 9x^2 + 4y^2,\ 2 \nmid xy \end{cases}$$

p	29	41	61	89	101	109	149
$\pm u$	5	5	5	5	1	3	7
$\pm v$	2	4	6	8	10	10	10
$5 \in \mathbb{F}_p^{\times 4}$					YES	YES	YES
$-5 \in \mathbb{F}_p^{\times 4}$	YES		YES				

It looks as if:

$$5 \in \mathbb{F}_p^{\times 4} \overset{?}{\iff} 10 \mid v \iff p = x^2 + 100y^2$$

$$-5 \in \mathbb{F}_p^{\times 4} \overset{?}{\iff} \begin{cases} 5, -1 \in \mathbb{F}_p^{\times 4} \iff 10 \mid v \wedge 4 \mid v \iff 20 \mid v \iff p = x^2 + 400y^2 \\ \text{OR} \\ 5, -1 \notin \mathbb{F}_p^{\times 4} \iff 5 \mid u \wedge 4 \nmid v \iff p = 25x^2 + 4y^2,\ 2 \nmid xy \end{cases}$$

Summary: for $p \equiv 1 \pmod 4$, solvability of $x^4 \equiv a \pmod p$ (at least for $a = \pm 3, \pm 5$) does not seem to involve a congruence condition on p, but a congruence condition on the (suitably normalised) irreducible element $\pi = u+vi \in \mathbb{Z}[i]$ such that $p = N(\pi) = \pi\overline{\pi} = u^2+v^2$.

Normalising π: π is not unique; other possible choices are $i^k\pi$, $i^k\overline{\pi}$. the condition $2 \nmid u$ ($\Leftrightarrow 2 \nmid v$) is equivalent to $\pi \equiv 1 \pmod{2\mathbb{Z}[i]}$ ($\Leftrightarrow \pi \equiv 1 \pmod{(1+i)^2\mathbb{Z}[i]}$), which still leaves the possibility of replacing π by $\pm\pi$ or $\pm\overline{\pi}$.

Toy model: normalising irreducible elements of $\mathbb{Z}$ (numbers of the form $\pm p$, p = prime) by a congruence condition. We can distinguish between $\pm p$ (for $p \neq 2$) by considering their residue classes (mod 4), since the canonical projection $\mathbb{Z}^\times = \{\pm 1\} \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times = \{\pm 1 \pmod 4\}$ is an isomorphism:

$\exists!\ p^* \in \{p, -p\}$ $\quad p^* \equiv 1 \pmod 4$ $\qquad \left[\ p^* = (-1)^{\frac{p-1}{2}} p\ \right]$.

Back to $\mathbb{Z}[i]$: the projection $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} \longrightarrow \underbrace{\left(\mathbb{Z}[i]/(1+i)^3\mathbb{Z}[i]\right)^\times}_{\left(\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i]\right)^\times}$ is an isomorphism, which means that, for every $\alpha \in \mathbb{Z}[i]$ such that $2 \nmid N(\alpha)$, there is a unique element $\beta \in \{\pm\alpha, \pm i\alpha\}$ such that $\beta \equiv 1 \pmod{(2+2i)\mathbb{Z}[i]}$.

Def. A prime element (irreducible element) $\pi \neq 2$ of $\mathbb{Z}[i]$ is primary if $\pi \equiv 1 \pmod{(2+2i)}$.

$\Leftrightarrow$ $\begin{cases} \pi = -p, & p \equiv 3 \pmod 4 \text{ prime number} \\ \pi = u \pm vi, & u^2+v^2 = p \equiv 1 \pmod 4 \quad \text{OR} \quad \text{—"—}, \end{cases}$ $\quad (1 \pm i)\pi \equiv 1 \pmod{4\mathbb{Z}[i]}$

$\Updownarrow$

$u \pm v \equiv 1 \pmod 4$

The biquadratic residue symbol

Legendre symbol:

group isomorphism

$$\begin{array}{ccc} \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} & \xrightarrow{\sim} & \mu_2(\mathbb{F}_p) \\ \downarrow & & \downarrow \\ a\,\mathbb{F}_p^{\times 2} & \longmapsto & a^{\frac{p-1}{2}} \end{array} \qquad \begin{array}{c} \text{reduction (mod } p) \\ \longleftarrow \\ \mu_2(\mathbb{Z}) = \mu_2(\mathbb{C}) \end{array}$$

$$\longleftrightarrow \left(\frac{a}{p}\right)$$

(notation: A = commutative ring, $n \in \mathbb{N}_+$, $\mu_n(A) = \{x \in A \mid x^n = 1\}$)

If $p, q \equiv 1 \pmod 4$ are prime numbers, then there are isomorphisms

$$\begin{array}{ccc} \mathbb{F}_p^\times/\mathbb{F}_p^{\times 4} & \xrightarrow{\sim} & \mu_4(\mathbb{F}_p) \\ \downarrow & & \downarrow \\ a\,\mathbb{F}_p^{\times 4} & \longmapsto & a^{\frac{p-1}{4}} \end{array}$$

and $\mathbb{F}_q^\times/\mathbb{F}_q^{\times 4} \xrightarrow{\sim} \mu_4(\mathbb{F}_q)$, but there is no canonical isomorphism between the two cyclic groups of order 4 $\mu_4(\mathbb{F}_p)$ and $\mu_4(\mathbb{F}_q)$.

We need to specify which element of $\mu_4(\mathbb{F}_p)$ (and $\mu_4(\mathbb{F}_q)$) corresponds to $i \in \mu_4(\mathbb{C})$, by making i (and $\mathbb{Z}[i]$) a part of the picture from the very beginning. This fundamental insight is due to Gauss (and this was the reason why Gauss developed arithmetic of the ring $\mathbb{Z}[i]$).

Let $\pi \nmid 2$ be an irreducible element of $\mathbb{Z}[i]$. There is a unique prime number p divisible by π. The residue ring $\mathbb{F}_\pi = \mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is finite and contains $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Euclid's lemma for $\mathbb{Z}[i] \Rightarrow \mathbb{F}_\pi$ is an integral domain $\overset{|\mathbb{F}_\pi| < \infty}{\Longrightarrow}$ $\mathbb{F}_\pi$ is a field. It has $N(\pi) = \begin{cases} p & \text{if } p \equiv 1 \pmod 4 \\ p^2 & \text{if } p \equiv 3 \pmod 4 \end{cases}$ elements.

Note: (1) the reduction (mod π) induces an isomorphism

$$\mathrm{red}_\pi: \{\pm 1, \pm i\} = \mu_4(\mathbb{Z}[i]) \xrightarrow{\sim} \mu_4(\mathbb{F}_\pi)$$

[$N(\pi) \equiv 1 \pmod 4 \Rightarrow \mathbb{F}_\pi^\times$ is cyclic of order 4. $\frac{N(\pi)-1}{4} \Rightarrow |\mu_4(\mathbb{F}_\pi)| = 4$;
$(\pm 1 \pm i) \mid 2 \overset{\pi \nmid 2}{\Longrightarrow} \pi \nmid (\pm 1 \pm i), \pm 2, \pm 2i \Rightarrow \ker(\mathrm{red}) = \{1\}$]

(2) the map

$$\begin{array}{ccc} \mathbb{F}_\pi^\times/\mathbb{F}_\pi^{\times 4} & \xrightarrow{\sim} & \mu_4(\mathbb{F}_\pi) \\ \downarrow & & \downarrow \\ a\,\mathbb{F}_\pi^{\times 4} & \longmapsto & a^{\frac{N(\pi)-1}{4}} \end{array}$$

is an isomorphism of cyclic groups of order 4

(3) $\mathbb{Z}/5\mathbb{Z}$ $\xrightarrow{\text{can}}$ $\mathbb{Z}[i]/(2 \pm i)\mathbb{Z}[i] = \mathbb{F}_{2\pm i}$, hence $\mathrm{red}_{2\pm i}(i) = \mp 2 \pmod 5$

$\downarrow$ $\qquad\qquad$ $\downarrow$ $\qquad\qquad$ $\uparrow$

$\mp 2 \pmod 5 \longleftrightarrow i \pmod{(2 \pm i)}$ $\qquad$ $\mathbb{F}_5$

Def. If $\pi \neq 2$ is an irreducible element of $\mathbb{Z}[i]$ and $a \in \mathbb{Z}[i]$ is not divisible by π, the <u>biquadratic residue symbol</u> $\left(\frac{a}{\pi}\right)_4 \in \mu_4(\mathbb{C})$ is defined by

$$\begin{array}{ccccc} \mathbb{F}_\pi^\times / \mathbb{F}_\pi^{\times 4} & \xrightarrow{\sim} & \mu_4(\mathbb{F}_\pi) & \xleftarrow[\sim]{\text{red}_\pi} & \mu_4(\mathbb{Z}[i]) = \mu_4(\mathbb{C}) = \{\pm 1, \pm i\} \\ \downarrow & & \downarrow & & \uparrow \\ a\,\mathbb{F}_\pi^{\times 4} & \longmapsto & a^{\frac{N(\pi)-1}{4}} & \longleftrightarrow & \left(\frac{a}{\pi}\right)_4 . \end{array}$$

Equivalently: $\left(\frac{a}{\pi}\right)_4$ is the unique element of $\{\pm 1, \pm i\}$ such that $\boxed{\left(\frac{a}{\pi}\right)_4 \equiv a^{\frac{N(\pi)-1}{4}} \pmod{\pi}}$

Properties: (1) $\left(\frac{a}{\pi}\right)_4 = 1 \iff \exists\, \alpha \in \mathbb{Z}[i] \quad \alpha^4 \equiv a \pmod{\pi}$.

(2) $a \equiv b \pmod{\pi} \Rightarrow \left(\frac{a}{\pi}\right)_4 = \left(\frac{b}{\pi}\right)_4$.

(3) $\left(\frac{a}{i^k \pi}\right)_4 = \left(\frac{a}{\pi}\right)_4$, $\left(\frac{ab}{\pi}\right)_4 = \left(\frac{a}{\pi}\right)_4 \left(\frac{b}{\pi}\right)_4$, $\left(\frac{i^k}{\pi}\right)_4 = (i^k)^{\frac{N(\pi)-1}{4}}$, $\overline{\left(\frac{a}{\pi}\right)_4} = \left(\frac{\bar{a}}{\bar{\pi}}\right)_4$.

Biquadratic reciprocity law: if $\pi, \pi' \equiv 1 \pmod{(2+2i)\mathbb{Z}[i]}$ are irreducible elements of $\mathbb{Z}[i]$ and $\pi \neq \pi'$, then

$$\boxed{\left(\frac{\pi}{\pi'}\right)_4 = \left(\frac{\pi'}{\pi}\right)_4 (-1)^{\frac{N(\pi)-1}{4} \cdot \frac{N(\pi')-1}{4}}}$$

Complements: $\left(\frac{i}{\pi}\right)_4 = i^{\frac{N(\pi)-1}{4}}$, $\left(\frac{1+i}{\pi}\right)_4 = i^{(a-b-b^2-1)/4}$, $\pi = a+bi$

Ex: (1) $\pi' = -3$, $\pi \equiv 1 \pmod{(2+2i)}$, $N(\pi) = p \equiv 1 \pmod{12}$, $N(\pi') = 9$

$\pi = u+vi$, $u \pm v \equiv 1 \pmod 4$, $p = u^2+v^2 \equiv 1 \pmod 3$

$u^2, v^2 \equiv 0, 1 \pmod 3 \Rightarrow 3 \mid uv,\ 3 \nmid (u+v) \Rightarrow \pi \equiv t \pmod{3\mathbb{Z}[i]},\ t \in \{\pm 1, \pm i\}$

$\mathbb{Z}[i]/3\mathbb{Z}[i] = \{0, \pm 1, i, i \pm 1, -i, -i \pm 1 \pmod{3\mathbb{Z}[i]}\}$

$$\left(\frac{-3}{\pi}\right)_4 \overset{BRL}{=} \left(\frac{\pi}{-3}\right)_4 \equiv \pi^{\frac{9-1}{4}} = \pi^2 \pmod{3\mathbb{Z}[i]} \equiv t^2 \pmod{3\mathbb{Z}[i]} \Rightarrow \underline{\left(\frac{-3}{\pi}\right)_4 = t^2}.$$

$\mathbb{F}_\pi = \mathbb{Z}[i]/\pi\mathbb{Z}[i] = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, so:

$-3 \in \mathbb{F}_p^{\times 4} = \mathbb{F}_\pi^{\times 4} \iff \left(\frac{-3}{\pi}\right)_4 = 1 \iff t = \pm 1 \iff \pi \equiv \pm 1 \pmod{3\mathbb{Z}[i]} \iff 3 \mid v \iff 6 \mid v$

$\Updownarrow$

$p = x^2 + 36y^2$

$\left(\frac{-3}{\pi}\right)_4 = -1 \iff t = \pm i \iff \pi \equiv \pm i \pmod{3\mathbb{Z}[i]} \iff 3 \mid u \iff p = 9x^2 + 4y^2 \quad (\pi = 3x + 2yi)$

As $\left(\frac{-1}{\pi}\right)_4 = (-1)^{\frac{p-1}{4}} = (-1)^{v/2}$, we obtain, as before,

$$\underbrace{\left(\frac{3}{\pi}\right)_4 = 1}_{3 \in \mathbb{F}_p^{\times 4}} \iff \left\{ \begin{array}{l} \left(\frac{-3}{\pi}\right)_4 = 1 \wedge 4 \mid v \\ \text{OR} \\ \left(\frac{-3}{\pi}\right)_4 = -1 \wedge 4 \nmid v \end{array} \right\} \iff \left\{ \begin{array}{l} 12 \mid v \\ \text{OR} \\ 3 \mid u \wedge 4 \nmid v \end{array} \right\} \iff \left\{ \begin{array}{l} p = x^2 + 144y^2 \\ \text{OR} \\ p = 9x^2 + 4y^2,\ 2 \nmid y \end{array} \right\}$$

(2) $\pi' = -1 \pm 2i$, $N(\pi') = 5$, $\pi = u+vi \equiv 1 \pmod{(2+2i)}$, $p = \pi\overline{\pi} = u^2+v^2 \equiv \pm 1 \pmod 5$ (p prime)

$u^2, v^2 \equiv 0, \pm 1 \pmod 5 \Rightarrow 5 \mid uv$, $5 \nmid u+v \Rightarrow \pi \equiv t$ or $2t \pmod{5\mathbb{Z}[i]}$, $t \in \{\pm 1, \pm i\}$

$\mathbb{F}_\pi = \mathbb{Z}[i]/\pi\mathbb{Z}[i] = \mathbb{F}_p$

$\left(\frac{-1\pm 2i}{\pi}\right)_4 \overset{\text{RDL}}{=} \left(\frac{\pi}{-1\pm 2i}\right)_4 (-1)^{\frac{p-1}{4}}$, $\left(\frac{\pi}{-1\pm 2i}\right)_4 \equiv \pi^{\frac{5-1}{4}} \equiv \begin{Bmatrix} t \\ 2t \end{Bmatrix} \bmod(-1\pm 2i) \equiv \begin{Bmatrix} t \\ \mp it \end{Bmatrix} \bmod(-1\pm 2i)$

$\Rightarrow \left(\frac{5}{\pi}\right)_4 = \left(\frac{\pi}{-1\pm 2i}\right)_4 \left(\frac{\pi}{-1-2i}\right)_4 = \begin{Bmatrix} t\cdot t \\ (-it)\cdot(it) \end{Bmatrix} = t^2$. Therefore

$5 \in \mathbb{F}_p^{\times 4} = \mathbb{F}_\pi^{\times 4} \iff \left(\frac{5}{\pi}\right)_4 = 1 \iff \pi \equiv \pm 1, \pm 2 \pmod{5\mathbb{Z}[i]} \iff 5 \mid v \iff 10 \mid v \iff p = x^2 + 100y^2$

$\left(\frac{5}{\pi}\right)_4 = -1 \iff \pi \equiv \pm i, \pm 2i \pmod{5\mathbb{Z}[i]} \iff 5 \mid u \iff p = 25x^2 + 4y^2$

As before, $\left(\frac{-1}{\pi}\right)_4 = (-1)^{v/2}$, hence:

$-5 \in \mathbb{F}_p^{\times 4} = \mathbb{F}_\pi^{\times 4} \iff \left(\frac{-5}{\pi}\right)_4 = 1 \iff \begin{cases} \left(\frac{5}{\pi}\right)_4 = 1 \wedge 4 \mid v \\ \text{OR} \\ \left(\frac{5}{\pi}\right)_4 = -1 \wedge 4 \nmid v \end{cases} \iff \begin{cases} 20 \mid v \\ \text{OR} \\ 5 \mid u \wedge 4 \nmid v \end{cases} \iff \begin{cases} p = x^2 + 400y^2 \\ \text{OR} \\ p = 25x^2 + 4y^2,\ 2 \nmid y \end{cases}$

The cubic residue symbol

$\mathbb{Z}[\zeta_3] = \{a + b\zeta_3 \mid a, b \in \mathbb{Z}\}$, $\zeta_3 = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. If π is an irreducible element of $\mathbb{Z}[\zeta_3]$ dividing a prime number $p \neq 3$, then $\mathbb{F}_\pi = \mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]$ is a finite field with $N(\pi) = \pi\overline{\pi} = \begin{cases} p, & \text{if } p \equiv 1 \pmod 3 \\ p^2, & \text{if } p \equiv -1 \pmod 3 \end{cases}$ elements, and $\mathbb{F}_\pi^\times$ is cyclic of order $N(\pi) - 1 = 3 \cdot \frac{N(\pi)-1}{3}$. As in the biquadratic case, the reduction map $\text{red}_\pi : \mu_3(\mathbb{Z}[\zeta_3]) = \{1, \zeta_3, \zeta_3^2\} \longrightarrow \mu_3(\mathbb{F}_\pi)$ is an isomorphism (since $\pi \nmid 1-\zeta_3$).

Def. If π is as above and $a \in \mathbb{Z}[\zeta_3]$, $\pi \nmid a$, then $\left(\frac{a}{\pi}\right)_3 \in \{1, \zeta_3, \zeta_3^2\} = \mu_3(\mathbb{C})$ is defined by

$$\begin{array}{ccccc} \mathbb{F}_\pi^\times / \mathbb{F}_\pi^{\times 3} & \xrightarrow{\sim} & \mu_3(\mathbb{F}_\pi) & \xleftarrow[\sim]{\text{red}_\pi} & \mu_3(\mathbb{Z}[\zeta_3]) = \mu_3(\mathbb{C}) \\ \Psi & & \Psi & & \Psi \\ a\,\mathbb{F}_3^{\times 3} & \longmapsto & a^{\frac{N(\pi)-1}{3}} & \longleftarrow & \left(\frac{a}{\pi}\right)_3 \end{array}$$

$$\left(\frac{a}{\pi}\right)_3 \equiv a^{\frac{N(\pi)-1}{3}} \pmod{\pi\mathbb{Z}[\zeta_3]}$$

Properties: (1) $\left(\frac{a}{\pi}\right)_3 = 1 \iff \exists \alpha \in \mathbb{Z}[\zeta_3] \quad \alpha^3 \equiv a \pmod{\pi\mathbb{Z}[\zeta_3]}$.

(2) $a \equiv b \pmod{\pi\mathbb{Z}[\zeta_3]} \Rightarrow \left(\frac{a}{\pi}\right)_3 = \left(\frac{b}{\pi}\right)_3$.

(3) $\left(\frac{a}{\pm\zeta_3^k\pi}\right)_3 = \left(\frac{a}{\pi}\right)_3$, $\left(\frac{ab}{\pi}\right)_3 = \left(\frac{a}{\pi}\right)_3\left(\frac{b}{\pi}\right)_3$, $\left(\frac{\pm\zeta_3^k}{\pi}\right)_3 = (\zeta_3^k)^{\frac{N(\pi)-1}{3}}$.

(4) $\overline{\left(\frac{a}{\pi}\right)_3} = \left(\frac{\overline{a}}{\overline{\pi}}\right)_3$.

The cubic reciprocity law

Normalisation of irreducible elements $\pi \in \mathbb{Z}[\zeta_3]$, $\pi \nmid 3$:

π can be multiplied by any element of $\mathbb{Z}[\zeta_3]^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\} = \mu_6(\mathbb{Z}[\zeta_3])$.

The reduction map $(\bmod 3\mathbb{Z}[\zeta_3])$ induces an isomorphism $\mathbb{Z}[\zeta_3]^\times \xrightarrow{\sim} (\mathbb{Z}[\zeta_3]/3\mathbb{Z}[\zeta_3])^\times$, which means that, for each $\alpha \in \mathbb{Z}[\zeta_3]$ such that $3 \nmid N(\alpha)$, there exists a unique element $\beta \in \{\pm\alpha, \pm\zeta_3\alpha, \pm\zeta_3^2\alpha\}$ such that $\beta \equiv 1 \pmod{3\mathbb{Z}[\zeta_3]}$.

The cubic reciprocity law: if $\pi, \pi' \equiv \pm 1 \pmod{3\mathbb{Z}[\zeta_3]}$ are irreducible elements of $\mathbb{Z}[\zeta_3]$ and $N(\pi) \neq N(\pi')$, then $\boxed{\left(\frac{\pi}{\pi'}\right)_3 = \left(\frac{\pi'}{\pi}\right)_3}$.

Complements: $\left(\frac{1-\zeta_3}{\pi}\right)_3 = \zeta_3^m$, if $\pm\pi = 3m+1+3n\zeta_3$ $(m, n \in \mathbb{Z})$

$\left(\frac{\pm\zeta_3^k}{\pi}\right)_3 = \left(\zeta_3^k\right)^{\frac{N(\pi)-1}{3}}$

Ex: $\pi' = 2$, $N(\pi') = 4$, $\pi = a + b\zeta_3$, $3 \nmid b$, $N(\pi) = p \equiv 1 \pmod 3$ prime

$\left(\frac{\pi}{2}\right)_3 \equiv \pi^{\frac{N(\pi)-1}{3}} \equiv \pi \pmod{2\mathbb{Z}[\zeta_3]}$. As $\mathbb{F}_\pi = \mathbb{F}_p$,

$2 \in \mathbb{F}_p^{\times 3} = \mathbb{F}_\pi^{\times 3} \iff \left(\frac{2}{\pi}\right)_3 = 1 \overset{\text{CRL}}{\iff} \left(\frac{\pi}{2}\right)_3 = 1 \iff \pi \equiv 1 \pmod{2\mathbb{Z}[\zeta_3]} \iff 2 \mid b$

$\iff 6 \mid b \iff \pi = x + 3iy\sqrt{3}$ $(x, y \in \mathbb{Z}) \iff p = x^2 + 27y^2$

Rmks: (1) if $\pi \nmid a$, then $\left(\frac{a}{\pi}\right)_3 = \left(\frac{\bar{a}}{\bar{\pi}}\right)_3$. In particular, if $\bar{a} = a$ and $\bar{\pi}/\pi \in \mu_3(\mathbb{C}) = \{1, \zeta_3, \zeta_3^2\}$, then $\left(\frac{a}{\pi}\right)_3 = \left(\frac{\bar{a}}{\bar{\pi}}\right)_3 = \overline{\left(\frac{a}{\pi}\right)_3} \in \mathbb{R} \cap \mu_3(\mathbb{C}) = \{1\}$.

(2) this implies that the reciprocity law $\left(\frac{\pi}{\pi'}\right)_3 = \left(\frac{\pi'}{\pi}\right)_3$ is automatically true if $\pi = \pm p$ and $\pi' = \pm p'$, where $p, p' \equiv 2 \pmod 3$ are prime numbers $(p \neq p')$, since

$$\left(\frac{\pm p}{\pm p'}\right)_3 = 1 = \left(\frac{\pm p'}{\pm p}\right)_3.$$

---

(3) It is enough, therefore, to consider the case when $N(\pi) = \pi\bar{\pi} = p \equiv 1 \pmod 3$, p = prime number. The proof given here will use Gauss and Jacobi sums attached to $\left(\frac{\cdot}{\pi}\right)_3 : \mathbb{F}_\pi^\times \longrightarrow \mu_3(\mathbb{C})$.

Characters of finite abelian groups

Def. A *character* of a finite abelian group G is a group homomorphism $\chi: G \to \mathbb{C}^\times$. The characters of G form an abelian group $\widehat{G}$ (the *dual group* of G) under multiplication: $(\chi_1 \chi_2)(g) = \chi_1(g)\chi_2(g)$.

Ex: $G = \mathbb{Z}/n\mathbb{Z}$, $\chi = \chi_a : x \pmod n \longmapsto \zeta_n^{ax}$ $\quad (a \in \mathbb{Z}/n\mathbb{Z},\ \zeta_n = e^{2\pi i/n})$

Properties: (1) If G is *cyclic of order n* (generated by $g_1 \in G$) $\Rightarrow$ $\widehat{G}$ *is also cyclic of order n*, generated by $\chi_1 : G \to \mathbb{C}^\times$ given by $\chi_1(g_1^k) = \zeta_n^k$.

(2) $\widehat{G_1 \oplus G_2} = \widehat{G}_1 \oplus \widehat{G}_2$: every character of $G_1 \oplus G_2$ is of the form $\chi((g_1, g_2)) = \chi_1(g_1)\chi_2(g_2)$, where $\chi_i : G_i \to \mathbb{C}^\times$ is a character of G_i.

(3) Every finite abelian group G is isomorphic to a direct sum of cyclic groups. Applying (1) and (2), we see that $\widehat{G}$ is (non-canonically) isomorphic to G, and that for each $g \in G$ different from the neutral element $1 \in G$ there exists $\chi \in \widehat{G}$ such that $\chi(g) \neq 1 \in \mathbb{C}^\times$.

(4) $\forall \chi \in \widehat{G}$ $\quad \displaystyle\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = 1 \\ 0 & \text{if } \chi \neq 1 \end{cases}$

Pf: If $\chi \neq 1$: $\exists h \in G$ $\chi(h) \neq 1$, hence $S = \displaystyle\sum_{g \in G} \chi(g) = \sum_{g' \in G} \chi(hg') = \chi(h) S \Rightarrow S = 0$

(5) $\forall g \in G$ $\quad \displaystyle\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases}$

Pf: If $g \neq 1 \overset{(3)}{\Rightarrow} \exists\, \chi_g \in \widehat{G}$ $\chi_g(g) \neq 1$, hence $S' = \displaystyle\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi' \in \widehat{G}} (\chi_g \chi')(g) = \chi_g(g)\, S'$
$\Rightarrow S' = 0$.

(6) One can also consider group homomorphisms $\chi: G \to K^\times$, where K is an arbitrary field. The proof of (4) still applies, showing that $\displaystyle\sum_{g \in G} \chi(g) = \begin{cases} |G| \cdot 1_K \in K & \text{if } \chi = 1 \\ 0_K \in K & \text{if } \chi \neq 1. \end{cases}$

(7) For example, if $G = \mathbb{F}_p^\times$, $K = \mathbb{F}_p$ and $\chi(a) = a^n$ $(n \in \mathbb{N}_+)$, one obtains $\forall n \geq 1$ $\displaystyle\sum_{a=0}^{p-1} a^n \equiv \begin{cases} p-1 \equiv -1 \pmod p & \text{if } (p-1) \mid n \\ 0 \pmod p & \text{if } (p-1) \nmid n \end{cases}$

(8) The (canonical) biduality homomorphism $G \to \widehat{\widehat{G}}$, $g \longmapsto (\chi \longmapsto \chi(g))$ is injective, by (3).
As $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$, it is an isomorphism (which explains the symmetry between (4) and (5)).

Gauss sums, Jacobi sums

Analogy: Gauss sums $\longleftrightarrow$ Γ-function $\quad \Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$

Jacobi sums $\longleftrightarrow$ B-function $\quad B(a,b) = \int_0^1 x^{a-1}(1-x)^{b-1} dx = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$

We consider these objects only in the simplest case, over the field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ (p = prime).

Notation: (1) $\psi : (\mathbb{F}_p, +) \longrightarrow \mathbb{C}^\times$ is the standard additive character

$\psi(x+y) = \psi(x)\psi(y)$ $\qquad \psi(x) = \xi_p^x = e^{2\pi i x/p}$ (analogue of $t \longmapsto e^{-t}$)

(2) For a (multiplicative) character $\chi : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ we extend χ to $\mathbb{F}_p$ by $\chi(0) = \begin{cases} 1 & \text{if } \chi = 1 \\ 0 & \text{if } \chi \neq 1 \end{cases} \Longrightarrow \forall x, y \in \mathbb{F}_p \quad \chi(xy) = \chi(x)\chi(y)$

Def. the **Gauss sum** attached to $\chi : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ is

$$G(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\psi(x) = \sum_{x \in \mathbb{F}_p} \chi(x) e^{2\pi i x/p}$$

Properties: (0) $G(1) = \sum_{x \in \mathbb{F}_p} \psi(x) = 0$.

(1) $\overline{G(\chi)} = \sum_x \overline{\chi(x)}\,\psi(-x) \underset{x=-y}{=} \sum_y \overline{\chi(-y)}\,\psi(y) = \overline{\chi(-1)}\, G(\overline{\chi}) = \chi(-1)\, G(\chi^{-1})$

(2) $\forall \chi \neq 1 \quad |G(\chi)|^2 = p \overset{(1)}{\Longrightarrow} G(\chi)G(\chi^{-1}) = \chi(-1)p$.

Pf: $G(\chi)\overline{G(\chi)} = \sum_{\substack{x,y \\ y \neq 0}} \chi(x)\chi(y)^{-1}\psi(x-y) \overset{x=yz}{=} \sum_{\substack{y,z \\ y \neq 0}} \underbrace{\chi(yz)\chi(y)^{-1}}_{\chi(z)}\psi(y(z-1)) =$

$= \sum_z \chi(z)\Big(\sum_{y \neq 0} \psi(y(z-1))\Big) = \sum_z \chi(z) \begin{cases} -1 & z \neq 1 \\ p-1 & z = 1 \end{cases} = p\chi(1) - \sum_z \chi(z) = p$.

Def. the **Jacobi sum** attached to $\chi_1, \dots, \chi_r : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ is

$$J(\chi_1, \dots, \chi_r) = \sum_{\substack{x_1 + \cdots + x_r = 1 \\ x_i \in \mathbb{F}_p}} \chi_1(x_1) \cdots \chi_r(x_r)$$

($r \geq 2$)

Rmk: The **order** of $\chi : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ is the smallest integer $n \geq 1$ such that $\chi^n = 1$. As $\chi \in \widehat{\mathbb{F}_p^\times}$ (= cyclic group of order $p-1$), n divides $p-1$. The values of χ are given by $\chi(\mathbb{F}_p^\times) = \mu_n(\mathbb{C}) = \{1, \xi_n, \dots, \xi_n^{n-1}\}$.

If $n = \text{order}(\chi) \Rightarrow G(\chi) \in \mathbb{Z}[\xi_n, \xi_p]$ $\left(= \mathbb{Z}[\xi_{\text{lcm}(n,p)}] = \mathbb{Z}[\xi_{np}]\right)$.

If $n_j = \text{order}(\chi_j) \Rightarrow J(\chi_1, \dots, \chi_r) \in \mathbb{Z}[\xi_{n_1}, \dots, \xi_{n_r}]$ $\left(= \mathbb{Z}[\xi_{\text{lcm}(n_1, \dots, n_r)}]\right)$.

(3) $\forall \chi \neq 1$ $\quad J(\chi, \chi^{-1}) = -\chi(-1)$.

Pf: $J(\chi,\chi^{-1}) = \sum_{\substack{u+v=1 \\ u,v\neq 0}} \chi(u)\chi(v)^{-1} = \sum_{t\neq 0,-1} \chi(t) = -\chi(-1)$ ∎

$\left(u = \frac{t}{1+t},\ v = \frac{1}{1+t},\ t = \frac{1}{v} - 1 \neq 0,-1\right)$

---

(4) If $\chi_1 \cdots \chi_r \neq 1$, then $\boxed{G(\chi_1)\cdots G(\chi_r) = G(\chi_1\cdots\chi_r)\, J(\chi_1,\dots,\chi_r)}$ ("$\Gamma(a)\Gamma(b) = \Gamma(a+b)B(a,b)$")

Pf: $\prod_1^r G(\chi_j) = \sum_{x_1,\dots,x_r} \left(\prod_1^r \chi_j(x_j)\right)\psi\left(\underbrace{\sum_1^r x_j}_{t}\right) = \sum_t J_t\,\psi(t)$, $J_t = \sum_{x_1+\cdots+x_r=t} \prod_1^r \chi_j(x_j)$

$t=0$: $\exists\, a \in \mathbb{F}_p^\times$ $\left(\prod_1^r \chi_j\right)(a) \neq 1$: $J_0 \underset{x_j = a y_j}{=} \sum_{y_1+\cdots+y_r=0} \left(\prod_1^r \chi_j(a y_j)\right) = \underbrace{\left(\prod_1^r \chi_j\right)(a)}_{\neq 1} J_0 \Rightarrow J_0 = 0$

$t\neq 0$: $J_t \overset{x_j = t y_j}{=} \left(\prod_1^r \chi_j\right)(t)\, J_1 \Rightarrow \prod_1^r G(\chi_j) = \underbrace{J_1}_{J(\chi_1,\dots,\chi_r)} \underbrace{\sum_{t\neq 0} \left(\prod_1^r \chi_j\right)(t)\,\psi(t)}_{G\left(\prod_1^r \chi_j\right)}$

---

(5) If χ is of order n ($\Leftrightarrow p \equiv 1 \pmod n$) and if $q \neq p$ is a prime number, then

$J(\underbrace{\chi,\dots,\chi}_{q \text{ times}}) \equiv \chi(q)^{-q} \pmod{q\mathbb{Z}[\zeta_n]}$.

Pf: $J(\underbrace{\chi,\dots,\chi}_{q}) = \sum_{x_1+\cdots+x_q=1} \chi(x_1\cdots x_q)$. The set $\{(x_1,\dots,x_q) \in \mathbb{F}_p^q \mid \sum_1^q x_j = 1\}$ is stable by the action of the cyclic permutation $\sigma : \underbrace{(x_1,\dots,x_q)}_{x} \mapsto \underbrace{(x_2,\dots,x_q,x_1)}_{\sigma(x)}$.

If $x \neq \sigma(x) \Rightarrow$ the q terms $\underbrace{x, \sigma(x), \dots, \sigma^{q-1}(x)}_{\text{distinct}}$ give the same contribution $\chi(x_1\cdots x_q)$ to $J(\chi,\dots,\chi)$.

If $x = \sigma(x)$, then $x_1 = \cdots = x_q = q \pmod p^{-1} \in \mathbb{F}_p^\times$. Modulo $q\mathbb{Z}[\zeta_n]$, this is the only term that will contribute to $J(\chi,\dots,\chi) \pmod{q\mathbb{Z}[\zeta_n]}$.

---

(6) If χ is of order 3 ($\Leftrightarrow p \equiv 1 \pmod 3$), then $G(\chi)^3 = p\, J(\chi,\chi)$.

Pf: $G(\chi)^2 \overset{(4)}{=} J(\chi,\chi)\, G(\chi^2)$, $G(\chi)\,G(\chi^2) = G(\chi)\,G(\chi^{-1}) \overset{(2)}{=} p\,\chi(-1) = p\,\chi((-1)^3) = p$.

(7) If χ is of order 3, then $\quad -J(\chi,\chi) \equiv 1 \pmod{3\mathbb{Z}[\zeta_3]}$.

Pf: $p \equiv 1 \pmod 3 \Rightarrow -J(\chi,\chi) \equiv -G(\chi)^3 \pmod{3\mathbb{Z}[\zeta_3]}$, but

$-G(\chi)^3 = -\left(\sum_{x\neq 0} \chi(x)\psi(x)\right)^3 \equiv -\sum_{x\neq 0} \underbrace{\chi(x)^3}_{1}\,\psi(3x) = -\sum_{y\neq 0} \psi(y) = \psi(0) = 1 \pmod{3\mathbb{Z}[\zeta_3]}$.

Proof of the cubic reciprocity law (CRL)

CRL: If $\pi_1 \pi' \equiv \pm 1 \pmod{3\mathbb{Z}[\zeta_3]}$ are irreducible elements of $\mathbb{Z}[\zeta_3]$ and $N(\pi) \neq N(\pi')$, then $\left(\frac{\pi}{\pi'}\right)_3 = \left(\frac{\pi'}{\pi}\right)_3$.

Proof: As observed earlier, it is enough to consider the case when $N(\pi) = \pi\bar{\pi} = p$ is a prime number ($p \equiv 1 \pmod 3$). The cubic residue symbol then defines characters of order 3

$$\chi_\pi : \mathbb{F}_p^\times = \mathbb{F}_\pi^\times \longrightarrow \mathbb{C}^\times, \quad a \pmod p \longmapsto \left(\frac{a}{\pi}\right)_3 \quad (a \in \mathbb{Z},\ p \nmid a)$$

$$\chi_{\bar\pi} : \mathbb{F}_p^\times = \mathbb{F}_{\bar\pi}^\times \longrightarrow \mathbb{C}^\times, \quad a \pmod p \longmapsto \left(\frac{a}{\bar\pi}\right)_3 = \overline{\left(\frac{a}{\pi}\right)_3} = \left(\frac{a}{\pi}\right)_3^{-1}$$

$$\chi_{\bar\pi} = \chi_\pi^{-1}$$

Lemma 1. $J(\chi_\pi, \chi_\pi) \in \mathbb{Z}[\zeta_3]$ satisfies $J(\chi_\pi, \chi_\pi) \equiv 0 \pmod{\pi\mathbb{Z}[\zeta_3]}$.

Pf. $J(\chi_\pi, \chi_\pi) = \sum_{\substack{x \in \mathbb{F}_p \\ x \neq 0,1}} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{a=1}^{p-1} a^{\frac{p-1}{3}} (1-a)^{\frac{p-1}{3}} \equiv 0 \pmod{\pi\mathbb{Z}[\zeta_3]}$.

$\sum_{a=1}^{p-1} a^n \equiv 0 \pmod p$ if $n \geq 1$, $(p-1) \nmid n$

Lemma 2. If $\pi \equiv \pm 1 \pmod{3\mathbb{Z}[\zeta_3]}$, then $J(\chi_\pi, \chi_\pi) = \mp\pi$.

Pf. We know that $J = J(\chi_\pi, \chi_\pi)$ satisfies $J \in \mathbb{Z}[\zeta_3]$, $\pi \mid J$,

$J\bar{J} = p^{-2}\left(G(\chi_\pi)\overline{G(\chi_\pi)}\right)^3 = p = \pi\bar\pi \Rightarrow J = u\pi$, $u \in \mathbb{Z}[\zeta_3]^\times = \{\pm 1, \pm\zeta_3, \zeta_3^2\}$.

We also know that $-J \equiv 1 \pmod{3\mathbb{Z}[\zeta_3]} \Rightarrow u \equiv \mp 1 \pmod{3\mathbb{Z}[\zeta_3]}$

$\Rightarrow u = \mp 1$.

We are now ready to prove the CRL. We must distinguish two cases.

Case (I): $\pi' = \pm p'$, p' prime number ($p' \equiv 2 \pmod 3$): $\chi_\pi^{p'} = \chi_\pi^{-1} \neq 1$

$G(\chi_\pi)^{p'} \overset{(4)}{=\!=} G(\underbrace{\chi_\pi^{p'}}_{\chi_\pi^{-1}}) J(\underbrace{\chi_{\pi_1 -, 1}}_{p'}, \chi_\pi)$, $\underbrace{J(\chi_{\pi_1 -, 1}, \chi_\pi)}_{p'} \equiv \underbrace{\chi_\pi(p')^{-p'}}_{\chi_\pi(p')} \pmod{p'\mathbb{Z}[\zeta_3]}$

$G(\chi_\pi)G(\chi_\pi^{-1}) \overset{=\!=}{} p\,\chi_\pi((-1)^3) = p$, $G(\chi_\pi)^{p'+1} = (G(\chi_\pi)^3)^{(p'+1)/3} \overset{(6)}{=\!=} (p\,\underbrace{J(\chi_\pi, \chi_\pi)}_{\mp\pi})^{(p'+1)/3}$

Therefore $(\mp p\pi)^{(p'+1)/3} \equiv p\,\chi_\pi(p') \pmod{p'\mathbb{Z}[\zeta_3]}$.

Raise this to the power $p'-1$ and use $(\pm p)^{p'-1} \equiv 1 \pmod{p'} \Rightarrow$

$$\underbrace{\pi^{(p'^2-1)/3}}_{\pi^{(p'-1)(p'+1)/3}} \equiv \chi_\pi(p')^{p'-1} = \left(\frac{\pm p'}{\pi}\right)_3 \pmod{p'\mathbb{Z}[\zeta_3]} \Rightarrow \left(\frac{\pi}{\pm p'}\right)_3 = \left(\frac{\pm p'}{\pi}\right)_3.$$

$$\equiv \left(\frac{\pi}{\pm p'}\right)_3 \pmod{p'\mathbb{Z}[\zeta_3]}$$

$p' \nmid (1 - \zeta_3^{\pm 1})$

Case (II) : $N(\pi') = \pi'\overline{\pi'} = p'$ prime number $(p' \neq p,\ p' \equiv 1 \pmod 3)$,

$\pi' \equiv \pm 1 \pmod{3\mathbb{Z}[\zeta_3]}$

Again, $G(\chi_\pi)^{p'} \overset{(4)}{=\!=} G(\underbrace{\chi_\pi^{p'}}_{\chi_\pi})\, J(\underbrace{\chi_\pi, \dots, \chi_\pi}_{p'})$

$$\Rightarrow \underbrace{G(\chi_\pi)^{p'-1}}_{(\mp p\pi)^{\frac{p'-1}{3}}} = J(\underbrace{\chi_\pi, \dots, \chi_\pi}_{p'}) \equiv \underbrace{\chi_\pi(p')^{-p'}}_{\chi_\pi(p')^{-1}} \pmod{p'\mathbb{Z}[\zeta_3]}$$

$$\equiv \underbrace{\left(\frac{p\pi}{\pi'}\right)_3}_{\chi_{\pi'}(p\pi)} \pmod{\pi'\mathbb{Z}[\zeta_3]}$$

As $\pi' \equiv (1-\zeta_3^{\pm 1})$, $\chi_{\pi'}(p\pi) = \chi_\pi(p')^{-1}$

By symmetry, $\chi_{\pi'}(p)^{-1} = \chi_\pi(p\pi')$

$\Big\}$ product $\Rightarrow$ $\chi_{\pi'}(\pi) \overset{CRL}{=} \chi_\pi(\pi')$.

Rmks (1) Gauss stated the biquadratic reciprocity law, but did not give a proof.

(2) the first published proof of the cubic reciprocity law was due to Eisenstein (but Jacobi claimed to have given a proof a few years earlier in his lectures).

(3) Eisenstein then gave several different proofs of the reciprocity laws for powers $n = 2, 3, 4$, as well as a proof of a special case of the reciprocity law for higher powers.

See the book of Ireland and Rosen (ch. 9, 14) for a more detailed account.

The number of solutions of $ax^3+by^3+cz^3\equiv 0 \pmod p$

Question: given $p=$ prime number and $a,b\in\mathbb{Z}$ $(p\nmid ab)$, count the number of solutions $\pmod p$ of $ax^3+by^3\equiv 1 \pmod p$.

Equivalent formulation: given $a,b\in\mathbb{F}_p^\times$, count the number of $\mathbb{F}_p$-rational points $|C(\mathbb{F}_p)|$ on the affine plane curve $C: ax^3+by^3=1$ (defined over $\mathbb{F}_p$).

Note: (1) If $p\not\equiv 1 \pmod 3 \Rightarrow$ $\begin{array}{ccc}\mathbb{F}_p^2 & \longrightarrow & \mathbb{F}_p^2 \\ (x,y) & \longmapsto & (x^3,y^3)\end{array}$ is a bijection; it induces a bijection $C'(\mathbb{F}_p)\xrightarrow{\sim} C(\mathbb{F}_p)$, where $C': ax+by=1$ is an affine line $\Rightarrow$ $|C(\mathbb{F}_p)|=|C'(\mathbb{F}_p)|=p$.

(2) If $p\equiv 1 \pmod 3$, fix a character $\chi:\mathbb{F}_p^\times\longrightarrow\mathbb{C}^\times$ of order 3 $(\chi^3=1\neq\chi)$ and let $\chi(0)=\chi^{-1}(0)=0$. As $\mathbb{F}_p^\times$ is cyclic of order $3\cdot\frac{p-1}{3}$, $\ker(\chi)=\mathbb{F}_p^{\times 3}$ and χ induces an isomorphism $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 3}\xrightarrow{\sim}\mu_3(\mathbb{C})$, $\bar{u}\mathbb{F}_p^{\times 3}\longmapsto\chi(u)$.

As a result,

$$\forall u\in\mathbb{F}_p\quad |\{x\in\mathbb{F}_p \mid x^3=u\}|=\begin{cases}1 & u=0\\ 0 & 0\neq u\notin\mathbb{F}_p^{\times 3}\\ 3 & u\in\mathbb{F}_p^{\times 3}\end{cases}=1+\chi(u)+\chi(u)^2=1+\chi(u)+\chi^{-1}(u).$$

(3) A variant of this formula for $C: \underbrace{ax^3}_{u}+\underbrace{by^3}_{v}=1$ yields

$$|C(\mathbb{F}_p)|=\sum_{\substack{u+v=1\\ u,v\in\mathbb{F}_p}}(1+\chi(a^{-1}u)+\chi^{-1}(a^{-1}u))(1+\chi(b^{-1}v)+\chi^{-1}(b^{-1}v))=\underbrace{\sum_{u+v=1}1+\chi(a^{-1}u)+\chi^{-1}(a^{-1}u)+\chi(b^{-1}v)+\chi^{-1}(b^{-1}v)}_{p+0+0+0+0=p}$$
$$+\big(\chi(ab^{-1})+\chi(a^{-1}b)\big)\underbrace{J(\chi,\chi^{-1})}_{-\chi(-1)=-1}+\chi^{-1}(ab)J(\chi,\chi)+\chi(ab)\underbrace{J(\chi^{-1},\chi^{-1})}_{\overline{J(\chi,\chi)}}$$

$$\Rightarrow\quad |C(\mathbb{F}_p)|+\underbrace{(1+\chi(ab^{-1})+\chi^{-1}(ab^{-1}))}_{}=p+1-\alpha-\bar\alpha,\quad \alpha=\chi^{-1}(ab)\big(-J(\chi,\chi)\big),\ |\alpha|=p^{1/2}$$

(4) Interpretation of $\underbrace{\quad}$: the number of $\mathbb{F}_p$-rational points "at infinity"

Recall: the projective space of $\dim=n$ over a field K has K-rational points $\mathbb{P}^n(K)=(K^{n+1}\smallsetminus\{0\})/K^\times$. A point $P\in\mathbb{P}^n(K)$ is given by its homogeneous coordinates $P=(z_0:\cdots:z_n)=(tz_0:\cdots:tz_n)$ $(\forall t\in K^\times)$ $(z_0,\dots,z_n\in K,\ \exists j\ z_j\neq 0)$

$\mathbb{P}^1(K)=K\cup\{\infty\}$

$(1:a)\longleftrightarrow a$

$(0:1)\longleftrightarrow\infty$

$(z_0:z_1)\longmapsto\begin{cases}z_1/z_0 & z_0\neq 0\\ \infty & z_0=0\end{cases}$

$\mathbb{P}^n(K)=K^n\cup\mathbb{P}^{n-1}(K)$ ← points at infinity

$(1:a_1:\cdots:a_n)\longleftrightarrow(a_1,\dots,a_n)$

$(z_0:\cdots:z_n)\longmapsto\begin{cases}(z_1/z_0,\dots,z_n/z_0)\in K^n & \text{if } z_0\neq 0\\ (z_1:\cdots:z_n)\in\mathbb{P}^{n-1}(K) & \text{if } z_0=0\end{cases}$

The affine plane curve $\underline{C: ax^3+by^3=1}$ over $\mathbb{F}_p$ can be completed to a projective curve $\widetilde{C}\subset\mathbb{P}^2$, $\underline{\widetilde{C}: az_1^3+bz_2^3=z_0^3}$.

$\widetilde{C}\cap\{z_0\neq 0\} \xrightarrow{\sim} C$

$(z_0:z_1:z_2) \longmapsto (z_1/z_0, z_2/z_0)$

Points at infinity:

$\widetilde{C}\cap\{z_0=0\} = \{(0:z_1:z_2) \mid az_1^3+bz_2^3=0\}$

$\updownarrow$

$\{x=z_1/z_2 \mid ax^3+b=0\}$

Therefore

$$\underline{\left|\widetilde{C}(\mathbb{F}_p)\right| - \left|C(\mathbb{F}_p)\right| = \left|\{x\in\mathbb{F}_p \mid ax^3+b=0\}\right| = 1+\chi(a^{-1}b)+\chi^{-1}(a^{-1}b)}$$

If $p\not\equiv 1 \pmod 3$, then $\left|\widetilde{C}(\mathbb{F}_p)\right| - \left|C(\mathbb{F}_p)\right| = 1$, $\left|\widetilde{C}(\mathbb{F}_p)\right| = p+1 \ (= |\mathbb{P}^1(\mathbb{F}_p)|)$

---

(5) The cubic residue symbol: if $\underline{p\equiv 1 \pmod 3}$, factor

$\underline{p=\pi\overline{\pi}}$, $\pi\in\mathbb{Z}[\zeta_3]$, $\underline{\pi\equiv 1 \pmod{3\mathbb{Z}[\zeta_3]}}$ (π is unique up to $\pi\longleftrightarrow\overline{\pi}$)

Take $\chi=\chi_\pi: \mathbb{F}_p^\times = \mathbb{F}_\pi^\times = \left(\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]\right)^\times \longrightarrow \mathbb{C}^\times$; then $\chi^{-1}=\chi_{\overline{\pi}}$

$a \pmod p \longmapsto \left(\frac{a}{\pi}\right)_3$

We know: $-J(\chi,\chi)=\pi \Rightarrow -J(\chi^{-1},\chi^{-1})=\overline{\pi}$

Summary: if $a,b\in\mathbb{F}_p^\times$, $C: ax^3+by^3=1$ and $\widetilde{C}: az_1^3+bz_2^3=z_0^3$, then:

$$\left|\widetilde{C}(\mathbb{F}_p)\right| = \begin{cases} p+1-\alpha-\overline{\alpha}, & \alpha=i\sqrt{p}, \quad p\not\equiv 1 \pmod 3 \\ p+1-\alpha-\overline{\alpha}, & \alpha=\left(\frac{ab}{\pi}\right)_3^{-1}\pi, \quad p\equiv 1 \pmod 3 \end{cases} \qquad (|\alpha|=p^{1/2})$$

$(\Rightarrow \left|\widetilde{C}(\mathbb{F}_p)\right| = |\alpha-1|^2 > 0)$.

$$\left|\widetilde{C}(\mathbb{F}_p)\right| - \left|C(\mathbb{F}_p)\right| = \left|\{x\in\mathbb{F}_p \mid ax^3+b=0\}\right|$$

Ex: if $\underline{p>5}$, then $\underline{\widetilde{C}: 3z_0^3+4z_1^3+5z_2^3=0}$ is of the above form

$\Rightarrow \widetilde{C}(\mathbb{F}_p)\neq\emptyset \overset{\text{Hensel}}{\Longrightarrow} \widetilde{C}(\mathbb{Q}_p)\neq\emptyset$.

Exercise: (1) Compute $|C_j(\mathbb{F}_p)|$ for $C_1: x^4+y^2=1$, $C_2: 1+y^2=x^4$, $C_3: 1+x^4=y^2$.
(2) Compute $|C(\mathbb{F}_p)|$ for $C: x^4+y^4=1$ and relate the result to (1).
(3) Prove analogous relations for $B(\frac{j}{4},\frac{k}{4})$. What is going on?

Exercise: Compute $\left|\widetilde{C}(\mathbb{F}_p)\right|$ for $\widetilde{C}: a_0X_0^{r_0}+\cdots+a_nX_n^{r_n}=0$, $p\nmid a_0\cdots a_n$.
(see Ireland–Rosen, ch. 8)

This is the beginning of a remarkable theory of zeta-functions of varieties over finite fields (see Ireland–Rosen, ch. 11)