Last time, defined cubic res. symbol $\left(\frac{\alpha}{\pi}\right)_3 : \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \xrightarrow{\text{hom.}} \mathbb{Z}/3\mathbb{Z}$

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \ (\pi) \qquad (\text{i.e. } \in \{1, \omega, \omega^2\})$$

N: really is proper generalization from $\mathbb{Z}$: $\lambda : n \mapsto |n|$.
for Euc. domain.

—

Wanted to solve $x^3 \equiv a \ (p)$. Work in $\mathbb{Z}[\omega]$. Then

if $p \equiv 1 \ (3)$, write $p = \pi \cdot \bar{\pi}$.

e.g.: $p = 13. = (3-\omega)(4+\omega)$ (prime since both have norm 13.)

—

Want to formulate cubic reciprocity. Call a prime π "primary" if

$\pi \equiv 2 \ (3)$. if $\pi = q$, clear.

if $\pi = a + b\omega$, some $a, b \in \mathbb{Z}$, then must have $a \equiv 2 \ (3)$, $b \equiv 0 \ (3)$

claim (HW): if $p \equiv 1 \ (3)$, $N(\pi) = p.$, then π has unique associate in $\{\pm\pi, \pm\omega\pi, \pm\omega^2\pi\}$ which is primary.

(clearly true for $q \equiv 2 \ (3)$ as well).

—

back to example:

$$(3-\omega) \cdot \omega^2 = -1 + 3\omega^2$$
$$(4+\omega) \cdot (\omega) = \omega^2 + 4\omega$$
$$= \omega^2 + \omega + 3\omega$$
$$= -1 + 3\omega. \ \checkmark$$

Law of Cubic Reciprocity: π_1, π_2 primary primes.

$N(\pi_1) \neq N(\pi_2)$, both $\neq 3$.

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

Notes: proof in cases. Do this Friday.

- worry about units and prime $(1-\omega) \mid 3$.

$\left(\frac{1}{\pi}\right)_3 = \left(\frac{-1}{\pi}\right)_3 = 1.$ since $(-1)^3 = -1$ ✓. always a cube.

these are distinct res. mod. π so actually $=$

Now for ω, ω^2, know $\left(\frac{\omega}{\pi}\right)_3 \equiv \omega^{N(\pi)-1/3} \ (\pi)$

then: done since we can handle all other units via multiplicativity.

just depends on $N(\pi)$ mod 9. (always $\equiv 1 \ (3)$, so $1, 4, 7$)

$\left(\frac{1-\omega}{\pi}\right)_3$ is much trickier. Here's the law:

if $\pi = q \equiv 2 \ (3)$, write $q = 3m-1$

if $\pi = a + b\omega$, primary, write $a = 3m-1$.
$N(\pi) \equiv 1 \ (3)$

then $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}$.

$\omega = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$

-

e.g. $\left(\frac{5}{3-\omega}\right) = \left(\frac{5}{-1+3\omega}\right)$

not primary

$-1+3\omega \overline{)\ 5}$

$\frac{5 \cdot (\overline{-1+3\omega})}{(-1+3\omega)(\overline{-1+3\omega})} = \frac{5}{13} \cdot \left(-\frac{5}{2} - \frac{3i\sqrt{3}}{2}\right)$

Use complex rts. of unity to describe elts. mod p.

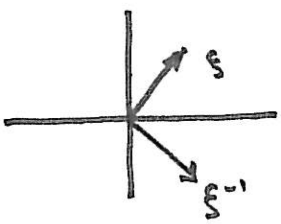
e.g. $$\left(\frac{q}{p}\right) \equiv q^{p-1/2} \quad (p).$$

so could try to find expression for q, $\sqrt{q}$ in complex rts. of unity. use identities to conclude values of symbol.

e.g. $q=2$. Find natural expression in rts. of unity for 2? or for $\sqrt{2}$?

winner: if $\xi = e^{2\pi i/8}$, can sum these.

$$\xi = e^{2\pi i/8} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}.$$



i.e. $(\xi+\xi^{-1})^2 = 2.$

cute pf: $(\xi+\xi^{-1})^2 = \underbrace{\xi^2}_{i} + 2(\xi\cdot\xi^{-1}) + \underbrace{(\xi^{-1})^2}_{-i}$ ✓.

Do modular arithmetic in ring containing $\xi = e^{2\pi i/8}$.

$$(\xi+\xi^{-1})^{p-1} = ((\xi+\xi^{-1})^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \quad (p) \checkmark$$

i.e. $$(\xi+\xi^{-1})^p \equiv \left(\frac{2}{p}\right)(\xi+\xi^{-1}) \quad (p)$$

now use fact that they're 8^{th} rts. of unity.

Note: $$\xi^p + \xi^{-p} = \begin{cases} \xi+\xi^{-1} & \text{if } p \equiv \pm 1 \ (8) \\ \underbrace{\xi^3+\xi^{-3}}_{-(\xi+\xi^{-1})} & \text{if } p \equiv \pm 3 \ (8) \end{cases}$$

but $\xi^4 = -1$ so $\xi^3 = -\xi^{-1}$

gives congruence, then cancel. ✓.

$(\xi = e^{2\pi i/p}$

Simple facts about "exponential sums": $$\sum_{t=0}^{p-1} \xi^{at} = \begin{cases} p & \text{if } a \equiv 0 \ (p) \\ 0 & \text{else} \end{cases}$$

pf: if $a \equiv 0$ (p), then clear. if $a \not\equiv 0$ (p),

then $\xi^a \neq 1$. $\sum \xi^{at} = (\xi^{ap}-1) / (\xi^a - 1) = 0$. ✓.

Fact 2: $\sum_{t \pmod p} (t/p)_2 = 0$. (know ½ res, ½ non-res.)

Define: Gauss sum: $g(a,p) = \sum_t \left(\frac{t}{p}\right) \xi^{at}$

Fact 3: $g(a,p) = \left(\frac{a}{p}\right) \cdot g(1,p)$.

if $a \equiv 0$ (p), then $g(a,p) = \sum_t \left(\frac{t}{p}\right) = 0$.

if $a \not\equiv 0$ (p), $\left(\frac{a}{p}\right) \cdot g(a,p) = \sum_t \left(\frac{at}{p}\right) \xi^{at}$

$at \mapsto x$: $\sum_x \left(\frac{x}{p}\right) \xi^{x} = g(1,p)$.

claim:
as at runs over all res. mod p,

Sometimes denote, simply,

$g(1,p) = g(p)$

at runs over all res. mod p

Prop: $g(p)^2 = (-1)^{\frac{p-1}{2}} \cdot p$.

idea: evaluate $\sum_a g(a,p)\, g(-a,p)$ in two different ways.

if $a \not\equiv 0 \ (p)$. $\quad g(a,p)\,g(-a,p) = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g(1,p)^2 = \left(\frac{-1}{p}\right)\cdot g(1,p)^2$

Hence: $\displaystyle\sum_a g(a,p)\,g(-a,p) = p-1\cdot\left(\frac{-1}{p}\right)\cdot g(1,p)^2.$

alternatively,

$$g(a,p)\,g(-a,p) = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \xi^{a(x-y)}$$

summing both sides over a,

$$\sum_a g(a,p)\,g(-a,p) = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\cdot p\cdot \delta(x,y)$$

Kronecker delta

$$= (p-1)\cdot p. \quad //.$$