Cyclotomic fields $\mathbb{Q}(\zeta_n)$ $(\zeta_n = e^{2\pi i/n})$

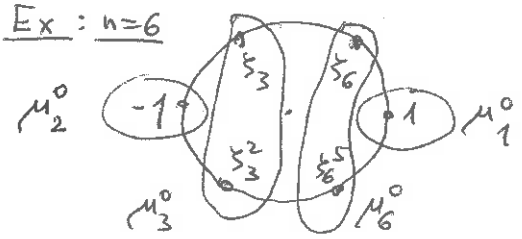
Goal (Kummer): study arithmetic of $\mathbb{Z}[\zeta_p]$ (p = prime) and apply it to the Fermat equation $z^p = x^p + y^p$ $\left(= \prod_{j \in \mathbb{Z}/p\mathbb{Z}} (x + \zeta_p^j y)\right)$.

Roots of unity ($n \geq 1$): $\mu_n(\mathbb{C}) = \{\zeta_n^a \mid a \in \mathbb{Z}/n\mathbb{Z}\}$ cyclic of order n

primitive n^{th} roots of unity: $\mu_n^\circ(\mathbb{C}) = \{\zeta_n^a \mid a \in (\mathbb{Z}/n\mathbb{Z})^*\} = \{\text{generators of } \mu_n(\mathbb{C})\}$

$$\mu_n(\mathbb{C}) = \bigsqcup_{d \mid n} \mu_d^\circ(\mathbb{C}), \quad |\mu_d^\circ(\mathbb{C})| = \varphi(d), \qquad X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta)$$

Ex: $n = 6$



$\deg(\Phi_n) = \varphi(n)$

Cyclotomic polynomials:

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^\circ(\mathbb{C})} (X - \zeta), \qquad X^n - 1 = \prod_{d \mid n} \Phi_d(X)$$

Möbius

$$\Phi_n(X) = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)} \in \mathbb{Z}[X] \quad \text{(monic)}$$

Ex: (1) $\Phi_{12}(X) = \dfrac{(X^{12}-1)(X^2-1)}{(X^6-1)(X^4-1)} = \dfrac{X^6+1}{X^2+1} = X^4 - X^2 + 1$

(2) $n = p^k$, p prime, $k \geq 1$: $\Phi_{p^k}(X) = (X^{p^k} - 1)/(X^{p^{k-1}} - 1)$

$$\Phi_{p^k}(1+Y) = \frac{(1+Y)^{p^k} - 1}{(1+Y)^{p^{k-1}} - 1} \equiv Y^{p^k - p^{k-1}} \pmod{p\,\mathbb{Z}[Y]}, \quad \Phi_{p^k}(1+Y)\big|_{Y=0} = \frac{p^k}{p^{k-1}} = p$$

$\Rightarrow$ Eisenstein polynomial with respect to p $\Rightarrow$ irreducible in $\mathbb{Q}[X]$

$\Rightarrow$ $[\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] = \deg(\Phi_{p^k}) = p^k - p^{k-1}$

Prop. $\ell \nmid n$ prime $\Rightarrow$ $X^n - 1 \pmod{\ell} \in \mathbb{F}_\ell[X]$ is separable ($\Rightarrow$ so is $\Phi_n(X) \pmod{\ell} \in \mathbb{F}_\ell[X] \Rightarrow \ell \nmid \operatorname{disc}(\Phi_n)$).

Pf: In $\mathbb{F}_\ell[X]$, $\gcd\left(X^n - 1, \underbrace{(X^n-1)'}_{nX^{n-1}}\right) = \gcd(X^n - 1, X^{n-1}) = 1$

($n \in \mathbb{F}_\ell^*$, since $\ell \nmid n$.)

Exercise. Compute $\operatorname{disc}(\Phi_{p^k})$ (p prime, $k \geq 1$, $p^k \neq 2$).

Note: $\Phi_n(\zeta_n) = 0 \Rightarrow [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \deg(\Phi_n) = \varphi(n)$, with equality $\Leftrightarrow$ Φ_n is irreducible in $\mathbb{Q}[X]$.

Properties of $\mathbb{Q}(\zeta_n)$: (1) If $\gcd(m,n)=1 \Rightarrow \mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$

[$\supseteq$: $\zeta_m = \zeta_{mn}^n$, $\zeta_n = \zeta_{mn}^m$ | $\subseteq$: $\exists u,v \in \mathbb{Z}$ $mu+nv=1 \Rightarrow \zeta_n^u \zeta_m^v = \zeta_{mn}$]

(2) If $n \equiv 2 \pmod 4 \Rightarrow (-\zeta_n)^{n/2} = 1$, $\mu_n = \mu_{n/2} \sqcup -\mu_{n/2}$, $\Phi_n(X) = \Phi_{n/2}(-X)$,
$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$. $(n/2 \equiv 1 \pmod 2)$.

(3) $\mathbb{Z}[\zeta_n] \subset \mathcal{O}_{\mathbb{Q}(\zeta_n)}$, (4) $\ell \nmid n$ prime $\Rightarrow \ell \nmid \mathrm{disc}(\Phi_n) \Rightarrow \ell \nmid D_{\mathbb{Z}[\zeta_n]/\mathbb{Z}}$
$\Rightarrow \ell$ unramified in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Thm. $\forall n \geq 1$ (1) Φ_n is irreducible in $\mathbb{Q}[X]$ ($\Rightarrow \Phi_n$ = the minimal polynomial of ζ_n over $\mathbb{Q}$) $\Rightarrow$ $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. (2) $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$

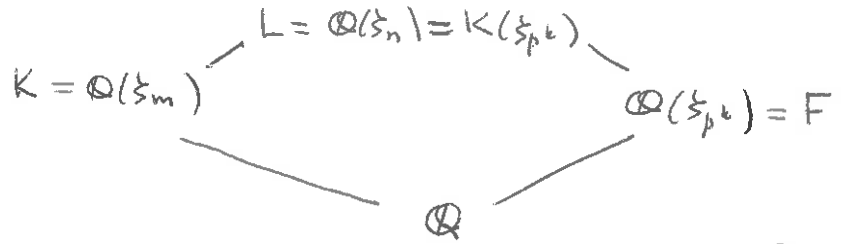
(3) $\forall$ prime ℓ: $\ell \nmid n \Rightarrow \ell$ unramified in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$
$\Leftarrow$ if $n \not\equiv 2 \pmod 4$

---

pf: Case 1: $n = p^k \neq 2, 1$ p prime: $\zeta_{p^k} - 1$ is a root of an Eisenstein polynomial with respect to p $\Rightarrow$ (1), (2) & $\ell \neq p$ is unramified] in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$

Case 2: $n = p_1^{k_1} \cdots p_r^{k_r}$, $\forall i$ $p_i^{k_i} \neq 2, 1$; $r > 1$

Induction on r: $n = p^k m$, $p \nmid m$, $m, p^k \neq 2$



$p \nmid m \Rightarrow p$ unramified in $K/\mathbb{Q}$, $p\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_t$ ($\Phi_{p^k}(1+Y)$)

$\forall i$ $v_{\mathfrak{P}_i}(p) = e_{\mathfrak{P}_i} = 1 \Rightarrow \zeta_{p^k} - 1$ is a root of the polynomial $\in \mathcal{O}_K[Y]$ which is Eisenstein with respect to $\mathfrak{P}_1$ (monic and) $\Rightarrow$ it is irreducible in $\mathcal{O}_K[Y] \Rightarrow$ irreducible in $K[Y] \Rightarrow [L:K] = \varphi(p^k) \Rightarrow$ (1).

As $K/\mathbb{Q}$ is unramified at all $\ell \nmid m$, $F/\mathbb{Q}$ — " — $\ell \nmid p$ $\Rightarrow \gcd(D_K, D_F) = 1$

Exercise some time ago $\Rightarrow$ $\mathcal{O}_L = \underbrace{\mathcal{O}_K}_{\mathbb{Z}[\zeta_m]} \underbrace{\mathcal{O}_F}_{\mathbb{Z}[\zeta_{p^k}]} = \mathbb{Z}[\zeta_n]$ (induction) $\Rightarrow$ (2).

(3) $\Rightarrow$ we know

$\Leftarrow$ if $n = p^k m$, $p^k \neq 1, 2 \Rightarrow p$ totally ramified in $F/\mathbb{Q}$, $[F:\mathbb{Q}] > 1$.

Prop. (Cyclotomic (p-)units) (1) $\forall a,b \in (\mathbb{Z}/n\mathbb{Z})^*$ $(n \neq 1)$ $\dfrac{1-\zeta_n^a}{1-\zeta_n^b} \in \mathbb{Z}[\zeta_n]^*$.

(2) $\prod_{1 \neq \zeta \in \mu_n} (1-\zeta) = \dfrac{x^n-1}{x-1}\Big|_{x=1} = n$, $\prod_{1 \neq \zeta \in \mu_n^0} (1-\zeta) = \prod_{d \mid n} (n/d)^{\mu(d)} = \begin{cases} p & n = p^k > 1,\ p \text{ prime} \\ 1 & \text{otherwise} \end{cases}$

(3) If n is divisible by more than one prime $\Rightarrow \forall a \in (\mathbb{Z}/n\mathbb{Z})^*$ $1-\zeta_n^a \in \mathbb{Z}[\zeta_n]^*$.

(4) If $n = p^k > 1$, p prime $\Rightarrow \forall a \in (\mathbb{Z}/p^k\mathbb{Z})^*$ $(1-\zeta_{p^k}^a) = (1-\zeta_{p^k})$, $(p) = (1-\zeta_{p^k})^{\varphi(p^k)}$.

Pf: (1) $\exists\, j \geq 1$ $a \equiv bj \pmod n$ $(a,b \geq 1)$ $\Rightarrow \dfrac{1-\zeta_n^a}{1-\zeta_n^b} = 1 + \zeta_n^b + \cdots + \zeta_n^{b(j-1)} \in \mathbb{Z}[\zeta_n]$

Interchange $a \leftrightarrow b$ $\Rightarrow (1-\zeta_n^b)/(1-\zeta_n^a) \in \mathbb{Z}[\zeta_n]$.

(2) Exercise $\Rightarrow$ (3).

(4) We have $(p) = p\mathcal{O}_{\mathbb{Q}(\zeta_{p^k})} \overset{(2)}{=} \left(\prod_{a \in (\mathbb{Z}/p^k\mathbb{Z})^*} (1-\zeta_{p^k}^a) \right) \overset{(1)}{=} (1-\zeta_{p^k})^{\varphi(p^k)}$.

The maximal real subfield of $\mathbb{Q}(\zeta_n)$ $(n>2)$:

$\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $[\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}] = \frac{1}{2}\varphi(n)$

Quadratic fields $\hookrightarrow$ Cyclotomic fields

Ex: (1) $\sqrt{-1} = \zeta_4 \in \underbrace{\mathbb{Q}(\zeta_4)}_{\mathbb{Q}(i)}$ ‖ (2) $\sqrt{\pm 2} \in \underbrace{\mathbb{Q}(\zeta_8)}_{\mathbb{Q}(\sqrt{2}, i)}$, $\zeta_8 = \frac{1+i}{\sqrt{2}}$, $\zeta_8^{-1} = \frac{1-i}{\sqrt{2}}$

(3) $q \neq 2$ prime $\Rightarrow$ the quadratic Gauss sum $G = \sum_{a \in \mathbb{F}_q^*} \left(\frac{a}{q}\right) \zeta_q^a \in \mathbb{Z}[\zeta_q]$ satisfies $G^2 = q^* = (-1)^{\frac{q-1}{2}} q \Rightarrow \mathbb{Q}(\sqrt{q^*}) \subset \mathbb{Q}(\zeta_q)$

(4) General quadratic field: $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z} \setminus \{0,1\}$ square-free

$D = D_K = D_{q_1} \cdots D_{q_t}$, $D_{q_j} \equiv 0,1 \pmod 4$, $D_{q_j} = \pm$ power of the prime q_j ($q_j \neq 2 \Rightarrow D_{q_j} = q_j^*$). By the above (1)–(3),

$K = \mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\sqrt{D_{q_1}}, \cdots, \sqrt{D_{q_t}}) \subset \mathbb{Q}(\zeta_{|D_{q_1}|}, \cdots, \zeta_{|D_{q_t}|}) = \mathbb{Q}(\zeta_{|D|})$.

Exercise: $K \not\subset \mathbb{Q}(\zeta_n)$ for $n < |D|$.

Factorisation of primes

Thm. If $p \nmid n$ (p = prime), then $(p) = p\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathfrak{P}_1 \cdots \mathfrak{P}_g$,
$N(\mathfrak{P}_i) = p^f$, $fg = \varphi(n)$, f = the order of $p \pmod n \in (\mathbb{Z}/n\mathbb{Z})^*$
$= \min\{d \geq 1 \mid p^d \equiv 1 \pmod n\}$.

Pf. Fix $F \supset \mathbb{F}_p$ such that $x^n - 1 \pmod p = \prod_{j=1}^{n}(x - \alpha_j)$, $\alpha_j \in F$ distinct ($p \nmid n$)
$\{\alpha_1, \dots, \alpha_n\} = \mu_n(F)$ and $\Phi_n(X) \pmod p = \prod_{d \mid n}\left((X^{n/d} - 1) \pmod p\right)^{\mu(d)} \in \mathbb{F}_p[X]$

$\Rightarrow \Phi_n(X) \pmod p = \prod(X - \alpha)$

$\alpha \in \mu_n^\circ(F) = \{\beta \in F^* \mid (\text{the order of } \beta \text{ in } F^*) = n\}$

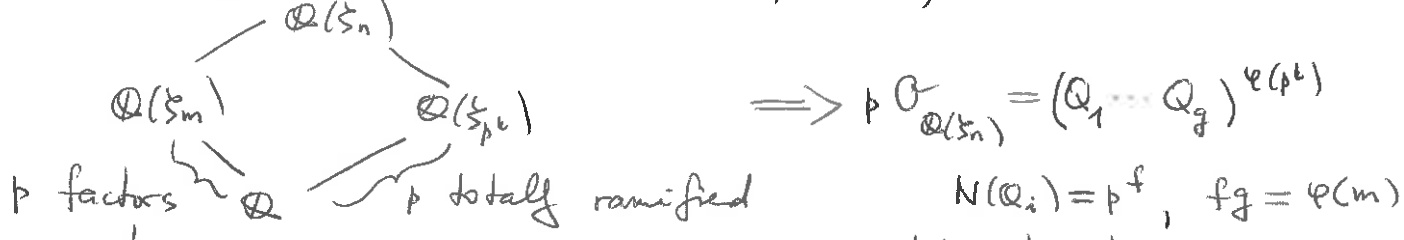
$\forall \alpha \in \mu_n^\circ(F)$ $\quad \alpha \in \mathbb{F}_{p^k} \iff \alpha^{p^k} = \alpha \iff \alpha^{p^k - 1} = 1 \iff n \mid (p^k - 1) \iff f \mid k$

Therefore $f = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ = the degree of the minimal polynomial of α over $\mathbb{F}_p$

$\Rightarrow \Phi_n(X) \pmod p = h_1 \cdots h_g \in \mathbb{F}_p[X]$, h_i distinct monic irreducible in $\mathbb{F}_p[X]$, $\deg(h_i) = f$

Kummer–Dedekind Thm $\Rightarrow$ result.

Exercise: If $n = p^k m$, $p^k \neq 1, 2$, $p \nmid m$, then



$\Rightarrow p\mathcal{O}_{\mathbb{Q}(\zeta_n)} = (\mathfrak{Q}_1 \cdots \mathfrak{Q}_g)^{\varphi(p^k)}$

$N(\mathfrak{Q}_i) = p^f$, $fg = \varphi(m)$

$f = \min\{d \geq 1 \mid p^d \equiv 1 \pmod m\}$

In other words, the factorisation of a prime number p in $\mathbb{Z}[\zeta_n]$ depends only on $p \pmod n$.

$\Downarrow$ Galois theory of finite fields

$\forall$ subfield $F \subset \mathbb{Q}(\zeta_n)$, the factorisation of p in $\mathcal{O}_F$ depends only on $p \pmod n$.

Ex: $F = \mathbb{Q}(\sqrt{D}) \hookrightarrow \mathbb{Q}(\zeta_{|D|})$ (D = a fundamental discriminant)

$\Rightarrow \left(\frac{D}{p}\right)$ depends only on $p \pmod{|D|}$ $\quad (p \nmid 2D)$

("weak Quadratic Reciprocity Law")

What about the factorisation (of p) in $\mathcal{O}_F$ if $F \not\subset \mathbb{Q}(\zeta_n)$, for any n?

Ex: $F = \mathbb{Q}(\sqrt[3]{a})$, $a \in \mathbb{Z}$, $\sqrt[3]{a} \notin \mathbb{Z}$. If p = prime, $p \nmid 3a \Rightarrow p \nmid (\mathcal{O}_F : \mathbb{Z}[\sqrt[3]{a}])$

- $X^3 - a$ = the minimal polynomial of $\sqrt[3]{a}$ over $\mathbb{Q}$
- if $p \equiv 2 \pmod 3 \Rightarrow$ $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$, $u \longmapsto u^3$ is an isomorphism $\Rightarrow \exists!\, u \in \mathbb{F}_p$, $u^3 \equiv a \pmod p$

$\Rightarrow X^3 - a \equiv (X-u)\underbrace{g(X)} \pmod p$ ($g(X)$ irreducible in $\mathbb{F}_p[X]$) $\overset{\text{Kummer}}{\underset{\text{Dedekind}}{\Longrightarrow}}$ $p\mathcal{O}_F = \mathfrak{P}_1\mathfrak{P}_2$, $N(\mathfrak{P}_i) = p^{\cdot}$

- if $p \equiv 1 \pmod 3$: if $\exists\, u_1 \in \mathbb{F}_p$, $u_1^3 \equiv a \pmod p \Rightarrow X^3 - a \equiv (X-u_1)(X-u_2)(X-u_3) \pmod p$

$\Rightarrow p\mathcal{O}_F = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$, $N(\mathfrak{P}_i) = p$

if $a \not\equiv u^3 \pmod p \Rightarrow X^3 - a \pmod p$ irreducible $\Rightarrow p\mathcal{O}_F = \mathfrak{P}$, $N(\mathfrak{P}) = p^3$

Special case: $a = 2$; when does $u^3 \equiv 2 \pmod p$ have a solution, if $p \equiv 1 \pmod 3$?

$p \equiv 1 \pmod 3 \Leftrightarrow p = x^2 + 3y^2$

$\overset{?}{\Longleftrightarrow}$ Euler's conjecture

$3 \mid y$ ($\Leftrightarrow p = x^2 + 27(y/3)^2$)

this is a very special case of the cubic reciprocity law.

Ex: $f(X) = X^3 - X + 1 = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$, $\operatorname{disc}(f) = -23$

$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_1, \sqrt{-23}\,)$ (degree 2 over $F = \mathbb{Q}(\alpha_1)$, degree 3 over $K = \mathbb{Q}(\sqrt{-23}\,)$)

$F = \mathbb{Q}(\alpha_1)$ (degree 3 over $\mathbb{Q}$)

$K = \mathbb{Q}(\sqrt{-23}\,)$ (degree 2 over $\mathbb{Q}$)

$\mathcal{O}_K \simeq \mathbb{Z}/3\mathbb{Z}$

L is the Hilbert class field of K:

(a) L/K is unramified at all primes of K

(b) $\mathfrak{P} \in \operatorname{Spec}(\mathcal{O}_K) \setminus \{(0)\}$ splits completely in L/K

$\Leftrightarrow \mathfrak{P} = (\alpha)$ is principal

(if $\mathfrak{P} \neq (\alpha) \Rightarrow$ it is inert in L/K)

Let $p \neq 2, 23$ be a prime number.

- if $\left(\frac{-23}{p}\right) = \left(\frac{p}{23}\right) = -1 \Rightarrow p\mathcal{O}_K = \mathfrak{P}$ principal $\Rightarrow p\mathcal{O}_L = Q_1 Q_2 Q_3$, $N(Q_i) = p^2$

  $p\mathcal{O}_F \neq \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ ($\operatorname{disc}(f) \pmod p \notin \mathbb{F}_p^{*2} \Rightarrow f \pmod p \in \mathbb{F}_p[X]$ does not have 3 roots in $\mathbb{F}_p$)

  $\Downarrow$

  $p\mathcal{O}_F = \mathfrak{P}_1\mathfrak{P}_2$, $N(\mathfrak{P}_i) = p^{3-i}$, $\mathfrak{P}_1\mathcal{O}_L = Q_1 Q_2$, $\mathfrak{P}_2\mathcal{O}_L = Q_3$

- if $\left(\frac{-23}{p}\right) = \left(\frac{p}{23}\right) = 1$ ($\Leftrightarrow \operatorname{disc}(f \bmod p) \in \mathbb{F}_p^{*2}$): $p\mathcal{O}_K = \mathfrak{P}\overline{\mathfrak{P}}$, $N(\mathfrak{P}) = p$

$\mathfrak{P} = (\alpha) \Leftrightarrow$ $p = N(\mathfrak{P})$ is represented by the principal form $x^2 + xy + 6y^2$ of $\Delta = -23$

(b) $\Updownarrow$ $\Leftrightarrow$ $4p = (2x+y)^2 + 23y^2 \overset{(\bmod 8)}{\Longleftrightarrow} 2 \mid y$, $p = u^2 + 23v^2$

$\mathfrak{P}\mathcal{O}_L = Q_1 Q_2 Q_3 \Leftrightarrow p\mathcal{O}_L = Q_1 \cdots Q_6$, $N(Q_i) = p$

$\Downarrow$

$p\mathcal{O}_F = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$, $N(\mathfrak{P}_i) = p$ $\overset{\text{Kummer–Dedekind}}{\Longleftrightarrow}$ $X^3 - X + 1 \equiv (X-u_1)(X-u_2)(X-u_3) \pmod p$.

$\mathfrak{P} \neq (\alpha) \Leftrightarrow$ p is represented by $p = 2x^2 + xy + 3y^2$ ($\Leftrightarrow 8p = u^2 + 23v^2$)

$\Downarrow$

$\mathfrak{P}\mathcal{O}_L = Q$, $\overline{\mathfrak{P}}\mathcal{O}_L = Q'$, $N(Q) = N(Q') = p^3$

$\Downarrow$

$p\mathcal{O}_F = \mathfrak{P}_1$, $N(\mathfrak{P}_1) = p^3 \Leftrightarrow X^3 - X + 1 \pmod p$ irreducible.

Summary: ($p \neq 2, 23$ prime)

$$X^3 - X + 1 \equiv \begin{cases} (X-u)\,(\text{irred. quadratic polynomial}) \pmod p \Leftrightarrow \left(\frac{p}{23}\right) = -1 \\ (X-u_1)(X-u_2)(X-u_3) \pmod p \Leftrightarrow p = u^2 + 23v^2 \\ \text{irreducible } \pmod p \Leftrightarrow 8p = u^2 + 23v^2 \end{cases}$$

General "class field" theory: given $\mathbb{Q} \subset K \subset L$ $([L:\mathbb{Q}] < \infty)$, factorisation of $\mathfrak{p}\mathcal{O}_L$ depends only on a suitable "congruence condition" on $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) \setminus \{(0)\}$

$\Updownarrow$

L/K is an abelian extension (Galois extension with an abelian Galois group)

(Hilbert, Weber, Takagi, Hasse, Artin ...)

Example: $a \in \mathbb{Z} \setminus \{0\}$, $p \nmid 2a$ prime, $p \equiv 1 \pmod 4$

solvability of $x^4 \equiv a \pmod p \iff$ factorisation of p in $\mathbb{Q}(\sqrt[4]{a})/\mathbb{Q}$

$\Uparrow$

factorisation $p = \pi\bar{\pi}$ in $\mathbb{Z}[i] \iff$ " " " $\mathbb{Q}(i, \sqrt[4]{a})/\mathbb{Q}$

" " AND of π in $\underbrace{\mathbb{Q}(i, \sqrt[4]{a})/\mathbb{Q}(i)}_{\text{abelian extension}}$

$\pi = u + vi$
$p = u^2 + v^2$ $(2 \mid v)$

$\Updownarrow$

congruence condition on u, v ("biquadratic reciprocity law")

Special case: $a = 2$

$x^4 \equiv 2 \pmod p$ has a solution $\overset{?}{\iff} 8 \mid v$ $(\iff p = u^2 + 64(v/8)^2)$

conjecture of Euler

A complement to the biquadratic reciprocity law.

What is a general reciprocity law?

A rule describing the factorisation of $p\mathcal{O}_K$ (or $\mathfrak{p}\mathcal{O}_L$) for a given finite extension $K/\mathbb{Q}$ (or L/K)

$\Updownarrow$ Kummer–Dedekind

factorisation of $\underbrace{f(X)}_{\text{fixed}} \underbrace{\pmod p}_{\text{variable}} \in \mathbb{F}_p[X]$

$K = \mathbb{Q}(\alpha)$, $f(\alpha) = 0$, $f \in \mathbb{Z}[X]$ monic, irreducible.

The first case of Fermat's Last Theorem for regular exponents

$p \neq 2$ prime, $K = \mathbb{Q}(\zeta_p)$, $K^+ = K \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$, $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$

$[K:\mathbb{Q}] = p-1$, $[K^+:\mathbb{Q}] = (p-1)/2$, $(\mathbb{Z}[\zeta_p], +) = \bigoplus_{j=0}^{p-2} \mathbb{Z}\zeta_p^j$

the minimal polynomial of ζ_p over $\mathbb{Q}$ is $(X^p-1)/(X-1) = X^{p-1} + X^{p-2} + \cdots + X + 1$

We know: $(p) = p\mathcal{O}_K = (1-\zeta_p)^{p-1}$, $\ell \neq p$ (prime) is unramified in $K/\mathbb{Q}$

Let $h_p = |\mathrm{Cl}_K|$ be the class number of K.

Def. (Kummer) p is a **regular prime** if $p \nmid h_p$.

Table: $p = 3, 5, 7, 11, 13, 17, 19 \iff h_p = 1 \iff \mathbb{Z}[\zeta_p]$ is a UFD

p	23	29	31	37	41	43	47	53	59	61	67
h_p	3	2^3	3^2	37	11^2	211	$5 \cdot 139$	4889	$3 \cdot 59 \cdot 233$	$41 \cdot 1861$	$67 \cdot 12739$

irregular

Thm 1 (Kummer) If $p \nmid h_p$, then $x^p + y^p = z^p$ has no solution $x, y, z \in \mathbb{Z} \setminus \{0\}$.

We are going to prove a weaker result ("the first case" of FLT):

Thm 2 (Kummer) If $p \nmid h_p$, then $x^p + y^p = z^p$ has no solution $x, y, z \in \mathbb{Z}$ with $p \nmid xyz$.

Exercise: $\{$roots of unity in $K\} = \mu_{2p} = \{\pm \zeta_p^j\} = \{\pm \zeta_p^{2k}\}$

Embeddings $\sigma_j : K \hookrightarrow \mathbb{C}$: $\{$roots of $(X^p-1)/(X-1)$ in $\mathbb{C}\} = \{\zeta_p^j \mid 1 \le j \le p-1\}$

$\Rightarrow \sigma_j(\zeta_p) = \zeta_p^j \quad (1 \le j \le p-1)$, $\sigma_j\left(\sum_{k=0}^{p-2} a_k \zeta_p^k\right) = \sum_{k=0}^{p-2} a_k \zeta_p^{jk} \quad (a_k \in \mathbb{Q})$

$\Rightarrow \forall\, \alpha \in \mathbb{Q}(\zeta_p) \quad \forall j \quad \overline{\sigma_j(\alpha)} = \sigma_j(\overline{\alpha})$

Lemma 1. $\mathcal{O}_K^* = \{\pm \zeta_p^j u \mid u \in \underbrace{\mathcal{O}_{K^+}^*}_{\mathcal{O}_K^* \cap \mathbb{R}},\ j \in \mathbb{Z}/p\mathbb{Z}\}$

Pf. If $u_1 \in \mathcal{O}_K^* \Rightarrow \forall \sigma_j : K \hookrightarrow \mathbb{C}$ $\quad |\sigma_j(u_1/\overline{u_1})|^2 = \sigma_j(u_1/\overline{u_1})\underbrace{\overline{\sigma_j(u_1/\overline{u_1})}}_{\sigma_j(\overline{u_1}/u_1)} = 1$

$\Rightarrow$ the image of $(u_1/\overline{u_1})^{\mathbb{Z}}$ under $\sigma = (\sigma_1, \ldots, \sigma_{\frac{p-1}{2}}) : K \hookrightarrow \mathbb{C}^{\frac{p-1}{2}}$ lies in the finite set $\sigma(\mathcal{O}_K) \cap \{z \mid \forall k = 1, \ldots, \frac{p-1}{2} \quad |z_k| = 1\}$

$\Rightarrow u_1/\overline{u_1}$ is a root of unity, $u_1/\overline{u_1} = \pm \zeta_p^{2a}$ for some $a \in \mathbb{Z}$

$\Rightarrow u = u_1 \zeta_p^{-a} \in \mathcal{O}_K^*$, $\overline{u} = \pm u$. If $u = \sum_{j=0}^{p-2} a_j \zeta_p^j = -\overline{u}$, $(a_j \in \mathbb{Z})$

then $-u = \overline{u} = \sum_j a_j \zeta_p^{-j} \equiv \sum_j a_j \equiv u \pmod{(1-\zeta_p)} \Rightarrow (1-\zeta_p) \mid 2u$ in $\mathbb{Z}[\zeta_p]$

$\Rightarrow p \mid 2|N_{K/\mathbb{Q}}(u)| = 2$ in $\mathbb{Z}$ — contradiction $\Rightarrow \overline{u} = u \in \mathcal{O}_K^* \cap \mathbb{R}$.

Lemma 2. If $x, y, z \in \mathbb{Z}$, $p \nmid xyz$ ($\gcd(x,y)=1$) and $z^p = x^p + y^p = \prod_{j \in \mathbb{Z}/p\mathbb{Z}} (x + \zeta_p^j y)$, then $\gcd\big((x+\zeta_p^j y), (x+\zeta_p^k y)\big) = (1)$ if $j \neq k \in \mathbb{Z}/p\mathbb{Z}$.
(ideal in $\mathbb{Z}[\zeta_p]$.)

Pf: If Q is a ($\neq 0$) prime ideal in $\mathbb{Z}[\zeta_p]$ dividing both $(x+\zeta_p^j y)$ and $(x+\zeta_p^k y)$, then $Q \mid ((\zeta_p^j - \zeta_p^k)y)$, $Q \mid ((\zeta_p^k - \zeta_p^j)x)$ $\overset{(x,y)=1}{\Longrightarrow}$ $Q \mid (1-\zeta_p) \Rightarrow Q = (1-\zeta_p)$

$\Rightarrow \forall a \quad (1-\zeta_p) \mid (x+\zeta_p^a y)$, $(p) = (1-\zeta_p)^{p-1} \mid \prod_a (x+\zeta_p^a y) = z^p$ — contradiction.

Pf of Thm 2. Assume $x^p + y^p = z^p$, $p \nmid xyz$. If $d = \gcd(x,y) > 1$ $\Rightarrow d \mid z \Rightarrow (x/d)^p + (y/d)^p = (z/d)^p$. So we can assume $\gcd(x,y)=1$ ($\Rightarrow \gcd(x,z) = \gcd(y,z) = 1$). Lemma 2 $\Rightarrow (z)^p = \prod_{j \in \mathbb{Z}/p\mathbb{Z}} (x+\zeta_p^j y)$ (ideals prime to each other)

$\overset{\text{unique factorisation for ideals}}{\Longrightarrow}$ $\forall j \quad (x+\zeta_p^j y) = I_j^p$, $I_j \subset \mathcal{O}_K$ ideal ($\neq 0$)

I_j^p principal, $I_j^{h_p}$ principal, $\gcd(p, h_p) = 1 \Rightarrow I_j = (\beta_j)$ principal $\forall j$.

$(x+\zeta_p y) = (\beta^p) \Rightarrow x + \zeta_p y = \beta^p u_1$, $u_1 \in \mathcal{O}_K^* \overset{\text{Lemma 1}}{\Longrightarrow} u_1 = u\eta$, $\eta = \zeta_p^k$, $u \in \mathcal{O}_K^* \cap \mathbb{R}$

$$\boxed{x + \zeta_p y = \beta^p u \eta}$$

$\beta = \sum_{j=0}^{p-2} b_j \zeta_p^j$ ($b_j \in \mathbb{Z}$), $\beta \equiv \underbrace{\sum_j b_j}_{b \in \mathbb{Z}} \pmod{(1-\zeta_p)} \Rightarrow \beta^p \equiv b^p \pmod{p(1-\zeta_p)}$

($a := b^p \in \mathbb{Z}$)

($p \mid \binom{p}{k}$ for $0 < k < p$ and $p \mid (1-\zeta_p)^{p-1}$)

$$\boxed{x + \zeta_p y \equiv a u \eta \pmod{p(1-\zeta_p)}}$$

$$\Downarrow$$

$$\underbrace{x+\zeta_p y}_{x+\zeta_p^{-1} y} \equiv \underbrace{a u \eta}_{a u \eta^{-1}} \pmod{\underbrace{p(1-\zeta_p)}_{p(1-\zeta_p)}}$$

$$\Rightarrow \boxed{\eta^{-1}(x+\zeta_p y) \equiv \eta(x+\zeta_p^{-1} y) \pmod{p(1-\zeta_p)}, \quad \eta = \zeta_p^k} \qquad (*)$$

The rest is easy: (a) If $\eta = 1 \Rightarrow p(1-\zeta_p) \mid (\zeta_p - \zeta_p^{-1}) y \Rightarrow p \mid y$ impossible

(b) If $\eta = \zeta_p \Rightarrow p(1-\zeta_p) \mid (\zeta_p - \zeta_p^{-1}) x \Rightarrow p \mid x$ impossible

(c) If $p = 3$, we have already proved the result by looking at $x^3 + y^3 \equiv z^3 \pmod 9$. So we can assume $p \geq 5$.

(d) $\sum_{j=1}^{p-1} a_j \zeta_p^j \in p\mathbb{Z}[\zeta_p] \Leftrightarrow \forall j \quad a_j \in p\mathbb{Z}$. Therefore $(*) \Rightarrow p \mid x$, $p \mid y$ whenever the four elements $\eta, \eta^{-1}, \eta\zeta_p^{-1}, \eta^{-1}\zeta_p$ of μ_p are distinct.

(e) The only remaining case: ($p \geq 5$), $\eta^{-1} = \eta \zeta_p^{-1} \Rightarrow p(1-\zeta_p) \mid (\eta^{-1} - \eta)(x-y)$

$\Rightarrow p \mid (x-y)$. Applying the same arguments to $y^p + (-z)^p = (-x)^p$

$\Rightarrow p \mid (y+z) \Rightarrow y^p + y^p \equiv -y^p \pmod p \overset{p \neq 3}{\Longrightarrow} p \mid y$ contradiction.

Thm 2 is proved!

Which prime numbers are regular ?

Thm (Kummer's criterion) $p \nmid h_p \iff p \nmid B_2, B_4, \dots, B_{p-3}$ $\in \mathbb{Z}_{(p)}$

Above, B_n are the **Bernoulli numbers**, defined by the generating series

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \qquad (B_1 = -\tfrac{1}{2},\ B_{2k+1} = 0 \text{ for } k \geq 1)$$

n	0	2	4	6	8	10	12	14	16
B_n	1	$\frac{1}{2\cdot 3}$	$-\frac{1}{2\cdot 3\cdot 5}$	$\frac{1}{2\cdot 3\cdot 7}$	$-\frac{1}{2\cdot 3\cdot 5}$	$\frac{5}{2\cdot 3\cdot 11}$	$-\frac{691}{2\cdot 3\cdot 5\cdot 7\cdot 13}$	$\frac{7}{6}$	$-\frac{3617}{2\cdot 3\cdot 5\cdot 17}$

Explanation: (1) $h_p = h_p^+ h_p^-$, $h_p^+ = |Cl_{K^+}|$

(2) $p \nmid h_p^- \Rightarrow p \nmid h_p^+$ (special case of Leopoldt's mirror principle)

(3) Kummer proved class number formulas for h_p and h_p^+ that generalise Dirichlet's —— " —— quadratic fields.

In particular, h_p^- = product of $\frac{p-1}{2}$ rational numbers $\in \mathbb{Z}_{(p)}$ one of them $\equiv 1 \pmod p$, the remaining ones are $\equiv -\frac{1}{2}\frac{B_{2i}}{2i} \pmod p$ $\left(1 \leq i \leq \frac{p-3}{2}\right)$.

Rmk. It is known that $|\{p;\ p \mid h_p\}| = \infty$.

It is not known whether $\{p;\ p \nmid h_p\}$ is infinite.