An introduction to "elliptic curves" or "mod. fns"

(Not) A ring (always comm), $A^\times = \{$inv elts of $A\}$

(Not) p prime, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{p-1}\}$ field [$\neq \mathbb{Z}_p$ reserved for smth else]

$\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \dots, \overline{p-1}\} = \mathbb{F}_p \setminus \{0\}$ gr (*)

$n \in \mathbb{N}$ $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{m-1}\}$ ring [$\neq \mathbb{F}_m$ reserved if $m = p^k$ for smth else]

$(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{k} \in \mathbb{Z}/m\mathbb{Z} \mid (k,m) = 1\}$ gr

ex $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\} \xrightarrow{\chi} \{-1, 1\} = \mathbb{Z}^\times$, $\chi(\bar{3}) = -1$.

(Not) For $f \in \mathbb{Z}[x_1, \dots, x_n]$ set $N_p(f) = \#\{\alpha \in \mathbb{F}_p^n \mid f(\alpha) = 0\} = \#Z_f(\mathbb{F}_p)$ where $Z_f(\mathbb{F}_p) = \{\alpha \in \mathbb{F}_p^n \mid f(\alpha) = 0\}$

For $f, g \in$ —"— set $N_p(f=g) = N_p(f-g)$; same not for $f \in \mathbb{F}_p[\dots]$

(Pbl) Compute $N_p(x^2+y^2=1)$ [$= N_p(C)$, $C = x^2+y^2-1$ "circle" ⊕]

$\#$ pts on circle in ch. p

obs: if $p=2$ double line!

next $p \neq 2$

(Prop 1) (Fermat) $N_p(C) = p - (-1)^{\frac{p-1}{2}} = \begin{cases} p-1 & \text{if } p \equiv 1 \ (4) \\ p+1 & \text{if } p \equiv 3 \ (4) \end{cases}$ (**)

Need preparation

(Def) (p odd, $a \in \mathbb{Z}$) $\left(\frac{a}{p}\right) = \left(\frac{\bar{a}}{p}\right) = N_p(x^2 = a) - 1 = \begin{cases} 1 & \text{if } \bar{a} \in \mathbb{F}_p^{*2} \\ 0 & \text{if } \bar{a} = 0 \\ -1 & \text{if } \bar{a} \notin \mathbb{F}_p^{*2} \end{cases}$

(Prop 2) (Euler) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (p)$

Pf. $\alpha \mapsto \left(\frac{\alpha}{p}\right)$ & $\alpha \mapsto \alpha^{\frac{p-1}{2}}$ gr homo $\mathbb{F}_p^* \to \{\pm 1\}$

Enough to show they are -1 on $\bar{g}$ where $\mathbb{F}_p^* = \langle \bar{g} \rangle$ i.e. that both non-trivial. Clear.

Obs: Ker of gr homo above $= \mathbb{F}_p^{\times 2}$

$\mathbb{F}_p^\times \hookrightarrow \mathbb{Z}^\times$

(Cor) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \ (4) \\ -1 & \text{if } p \equiv 3 \ (4) \end{cases} = \chi(p \bmod 4) = \chi(p)$. ← notation

(Prop 3) $\sum_{\alpha \in \mathbb{F}_p^\times} \left(\frac{\alpha}{p}\right) = 0$ [clear]

(**) $a \equiv b \ (m)$ iff $m \mid b-a$ iff $\pi(a) = \pi(b)$, $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

$a \equiv b \bmod (m)$

(*) (Th) (Gauss) $\mathbb{F}_p^\times$ cyclic

Earliest form of "quadr rec" (a periodicity)

Proof of Prop 1

$$N_p(x^2+y^2=1) = \sum_{\substack{\alpha+\beta=1 \\ \alpha,\beta\in\mathbb{F}_p}} N_p(x^2=\alpha)\,N_p(y^2=\beta) = \sum_{\alpha+\beta=1} \left(1+\left(\frac{\alpha}{p}\right)\right)\left(1+\left(\frac{\beta}{p}\right)\right)$$

$$= p + \underbrace{\sum \left(\frac{\alpha}{p}\right)}_{0} + \underbrace{\sum \left(\frac{\beta}{p}\right)}_{0} + \underbrace{\sum_{\alpha+\beta=1} \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right)}_{S}$$

$$S = \sum_{\alpha} \left(\frac{\alpha(1-\alpha)}{p}\right) = \sum_{\alpha\neq 1} \left(\frac{\alpha/(1-\alpha)}{p}\right) = \sum_{\gamma\neq -1} \left(\frac{\gamma}{p}\right) = -\left(\frac{-1}{p}\right) \quad \square$$

$\uparrow$ $\left(\frac{x^2}{p}\right)=1$

$\uparrow$ if α runs thr. $\mathbb{F}_p\setminus\{1\}$, $\gamma=\frac{\alpha}{1-\alpha}$ runs thr $\mathbb{F}_p\setminus\{-1\}$

Not $a_p = a_p(C) := p - N_p(C) \left(= (-1)^{\frac{p-1}{2}} = \chi_{\blacksquare}(p)\right)$

Def $L(C,s) := \underbrace{\prod_{p\neq 2} (1-a_p p^{-s})^{-1}}_{\text{called Hasse-Weil fcn}} \left(= \prod_{p\neq 2} \frac{1}{\left(1-\frac{a_p}{p^s}\right)}\right)$ hol in s for $\mathrm{Re}\, s > 0$ (we'll see)

Miracle (1)

Cor $L(C,s) = \sum_{n \text{ odd}} \frac{\chi_{\blacksquare}(n)}{n^s} =: \underset{\text{def}}{L(\chi_{\blacksquare}, s)}$ called Dirichlet L fcn

Pf of $\prod_{p\neq 2} \frac{1}{\left(1-\frac{a_p}{p^s}\right)} = \prod_{p\neq 2} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right) = \sum_{2\nmid n} \frac{\chi(n)}{n^s}$.

~~Facts not to be proved~~

Cor $L(C,1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots = \frac{\pi}{4} = \frac{1}{8}\,\text{length}(C)$

$= 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \cdots$

$L(C,1)$: defined arithmetically (mod p's)

$\frac{\pi}{4}$: known from "calculus" $\tan^{-1} x = \int \frac{dx}{1+x^2} = \int (1-x^2+x^4-\cdots)\,dx$, $x=1$ + Abel

$\frac{1}{8}\,\text{length}(C)$: belongs to real analysis.

miraculous link (2)

Fact (not to be proved for $L(\chi_{\blacksquare}, s)$ but in easier case $\zeta(s) = "L(\chi_0, s)"$)

If $\Lambda(s) = \left(\frac{4}{\pi}\right)^{s/2} \Gamma\left(\frac{s+1}{2}\right) L(C,s)$ then $\Lambda \in \mathcal{E}$, hence L, have analyt cont to $\mathbb{C}$

& $\Lambda(s) = \Lambda(1-s)$ [fcnal equ : a "hidden symmetry"] miracle (3)

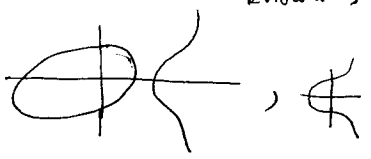
Main question : Are there analogues of miracles (1) & (2) & (3) for other curves than $C = x^2+y^2-1$? (circle.)

Answers 1) yes for other conics $Q = ax^2+by^2-c$ (Hasse)
(need more general reciprocity of Gauss $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$) all miracles 1,2,3 OK.

2) (partial) yes for cubics $E = y^2-(x^3+ax+b)$ (Wiles, Taylor, ...)
(need modular forms etc)

3) (completely) open for higher degree curves. (none of miracles 1,2,3 known)

Description of 2) $E = y^2-(x^3+ax+b)$



$a_p := p - N_p(E)$ if $p \nmid \Delta = 4a^3+27b^2$

$L(E,s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$

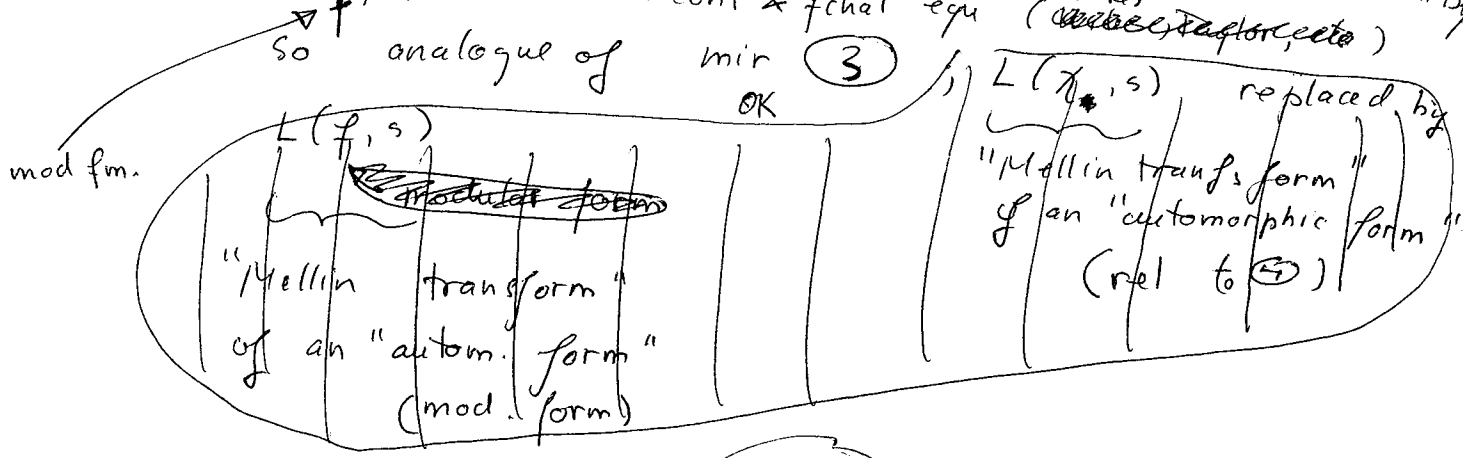
Euler factor for p

miracle (1) OK due to Wiles, Taylor, etc. $L(E,s) = L(f,s)$, "f mod fm." (*)

Then — no analogue of miracle (2) known. $\exists$ BIG conj "Birch-Swinnerton Dyer"

— $L(E,s)$ has an. cont & fcnal eqn (Hecke)

So analogue of mir (3) OK



In our course show 2) for (SOME) E's according to old work of Eichler-Shimura. Wiles et al. did it for (ALL) E's.

(*) needs "correction" by ∞ in many "Euler factors". $L(E,s)$