58 87 116

Have the handout.

X^2+1:

	2	3	5	7	11	13	17	19	23	29	31	37	41
#sols:	1	0	2	0	0	2	2	0	0	2	0	2	2
mod 4	0	3	1	3	3	1	1	3	3	1	3	1	1

weird

$29 \times 5 = 145$, hence $12^2 = -1 \bmod 29$.

Here we can give an elementary explanation:

1) seems for $p \neq 2$:

solutions $= 2 \iff p \equiv 1 \bmod 4$.

X^2+1 has a solution mod p $\iff$ -1 is a square mod p

$$\boxed{\{\text{squares}\} \hookrightarrow \mathbb{F}_p^\times \longrightarrow \{\pm 1\}, \quad x \longmapsto x^{(p-1)/2}}$$

$$\overset{p\neq 2}{\iff} (-1)^{(p-1)/2} = 1$$

$$\overset{p\neq 2}{\iff} (p-1)/2 \text{ is even} \iff p-1 \equiv 0 \bmod 4$$

$$\iff p \equiv 1 \bmod 4. \qquad \square$$

Next example:

X^2-3:

	2	3	5	7	11	13	17	19	23	29	31	37	41
#sol'ns:	1	1	0	0	2	2	0	0	2	0	0	2	0
p mod 12:	2	3	5	7	-1	1	5	7	-1	5	7	1	5

weird

$$\left(\frac{x}{p}\right) = (-1)^{p-1/2} = \begin{cases} 1 & \text{if } x \text{ is a quad. residue} \\ -1 & \text{otherwise.} \end{cases}$$

Need to introduce Legendre symbols.

This is explained via Gauß's law of quadratic reciprocity.

$p \neq 2$: $\quad \varepsilon(p) := \begin{cases} 0 & \text{if } p \equiv 1 \bmod 4 \\ 1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$ $\qquad \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$

Thm: if l, p are primes $\neq 2$. $\quad \left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\varepsilon(p)\varepsilon(l)}$.

$l \neq p$

We have

$X^2 - 3$ has a solution modulo p $\iff \left(\frac{3}{p}\right) = 1$

$$\overset{\text{Group'hm}}{\iff} \left(\frac{p}{3}\right) (-1)^{\varepsilon(p)\varepsilon(3)} = 1$$

$$\iff \left(\frac{p}{3}\right)(-1)^{\varepsilon(p)} = 1$$

$$\overset{p \neq 2,3}{\iff} \begin{cases} p \equiv 1 \bmod 3 \text{ and } p \equiv 1 \bmod 4 & 1 \quad 1 \\ p \equiv 2 \bmod 3 \text{ and } p \equiv 3 \bmod 4 & -1 \quad -1 \end{cases}$$

$(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, -1\}$.

$$\iff p \equiv 1, -1 \bmod 12. \qquad \square$$

A few more examples that don't precisely fall under the umbrella of quadratic reciprocity.

Examples of elliptic curves $\longrightarrow$ Sato-Tate.

Explain example of $f(x) = x^2 - 3$ from this perspective, to highlight the relevance of abelian Galois groups.

What is going on here? And what does this have to do with rep. theory?

$f(x) \in \mathbb{Z}[x]$ $\rightsquigarrow$ $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)/\mathbb{Q}$ splitting field of f.

our polynomial (assumed irreducible)

here roots will satisfy many relations, we seek the group of permutations which preserves them.

$\rightsquigarrow$ $\Gamma = \text{Galois group}(K/\mathbb{Q}) \circlearrowright \{\alpha_1, \dots, \alpha_n\}$

$\rightsquigarrow$ (permutation) representation $\Gamma \circlearrowright \bigoplus \mathbb{Q}\alpha_i$

Alternatively, we can consider $\bar{f}(x) \in \mathbb{F}_p[x]$ (Note that $\bar{f}(x)$ will often be reducible.)

If $p \nmid \Delta(f)$ then $\bar{f}(x)$ still has n roots $\bar{\alpha}_1, \dots, \bar{\alpha}_n \in \mathbb{F}_{p^n}$.

Recall that the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ is generated by the Frobenius, $\overline{\text{Frob}}_p : x \mapsto x^p$.

Hence: # solutions of $\bar{f}(x)$ in $\mathbb{F}_p$ = # fixed points of $\overline{\text{Frob}}_p$ on $\{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$.

DO THIS EXAMPLE

E.g. $f(x) = x^2+1$ $\rightsquigarrow$ $K = \mathbb{Q}(\pm i)$

$\Gamma = \mathbb{Z}/2\mathbb{Z} = \{s, 1\}$

In this case, $\bar{f}(x) = \begin{cases} (x+\lambda)(x-\lambda) & \text{if } \bar{f}(x) \text{ has a root in } \mathbb{F}_p \\ \text{irreducible} & \text{otherwise.} \end{cases}$

Here $\forall p \nmid 2$ $\text{Frob}_p : i \mapsto i^p$, $\text{Frob}_p \mapsto \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ s & \text{if } p \equiv 3 \bmod 4. \end{cases}$

For such a p, and

After a choice ("choose a prime in $\mathcal{O}$ over p")

we get: ① bijection $\{\bar{\alpha}_1, \dots, \bar{\alpha}_n\} \xleftarrow{\sim} \{\alpha_1, \dots, \alpha_n\}$ $(*)$

② an elt $\mathrm{Frob}_p \in \Gamma$ which agrees with $\overline{\mathrm{Frob}_p}$ under $(*)$.

<u>Remark:</u> For unramified primes (i.e. $p \nmid \Delta(f)$) a different choice of prime over p leads to a conjugate Frob_p. Hence what we really get is a <u>conjugacy class</u>.

The above discussion shows that

$$\#\ \text{fixed points of } \mathrm{Frob}_p \text{ on } \{\alpha_1, \dots, \alpha_n\} = \#\ \text{roots of } f(x) \text{ over } \mathbb{F}_p.$$

$$\parallel$$

$$\mathrm{Tr}(\mathrm{Frob}_p, H)$$

DON'T WORRY IF YOU DON'T UNDERSTAND THESE LINES NOW!

BACK TO EXAMPLES

We are aiming for a more representation theoretic understanding of this problem. Our aim is the following picture:

"geometric" representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ $\rightsquigarrow$ "character" built out of (i.e. $\mathrm{Tr}(\mathrm{Frob}_p, H)$ $\forall$ unramified p) $\leftsquigarrow$ automorphic forms.

E.g.

trivial rep $\rightsquigarrow$ Riemann ζ-function $\leftsquigarrow$ trivial rep of $GL_1(\mathbb{A})$

2 dim reps (elliptic curves) $\rightsquigarrow$ "Hecke L-functions" $\leftsquigarrow$ modular forms

If we talk of $\mathrm{Tr}(\mathrm{Frob}_p, H)$ as the character of a representation, we'd better know that the $\{\mathrm{Frob}_p\}$ exhaust all elements in Galois groups.

This is a deep theorem:

<u>Chebotarev density theorem:</u> Let Γ be as above, and fix a conjugacy class C. Then

$$\{ p \text{ unramified} \mid \mathrm{Frob}_p \in C \}$$

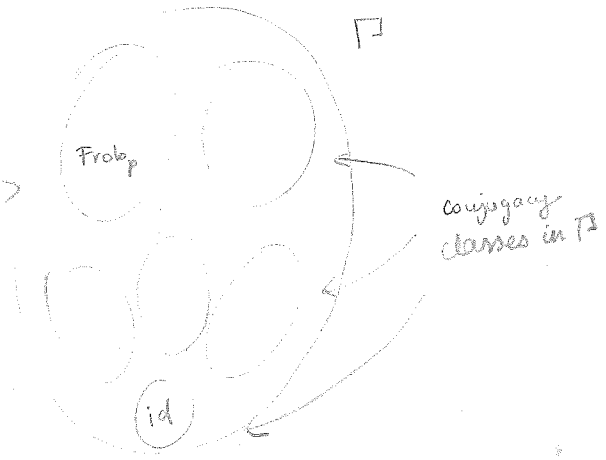
has density $|C|/|\Gamma|$ amongst all unramified primes.

(either analytic density or natural density).

<u>Exercise:</u> By considering a suitable cyclotomic extension of $\mathbb{Q}$, show that Chebotarev's density theorem implies Dirichlet's theorem on primes in arithmetic progressions.

<u>Picture:</u>

$$\left\{ \begin{matrix} (\text{unramified}) \\ \text{primes} \end{matrix} \right\} \longrightarrow$$



Where does Frob_p land?

In simple examples (e.g. $\Gamma = \mathbb{Z}/2\mathbb{Z}$) we saw that where Frob_p lands is given by a simple rule based on congruences.

Class field theory is a description of these rules when Γ is abelian. When Γ is non-abelian (and even worse non-solvable) we need a much more sophisticated theory, this is what the Langlands program provides.

Another example: $X^2 - X - 1$ on handout ... why modulo 10?

$$\phi = \frac{1+\sqrt{5}}{2} = 2\cos(\pi/5) = \zeta + \bar{\zeta} \quad \text{where } \zeta = e^{i\pi/5}.$$

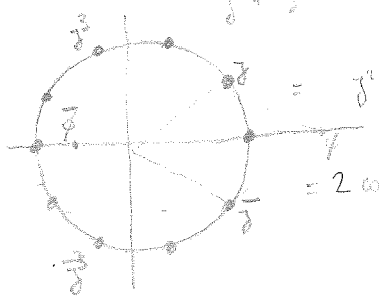
primitive 10th root of unity.

$(\zeta + \bar{\zeta})^2 - (\zeta + \bar{\zeta}) - 1$

$= \zeta^2 + \bar{\zeta}^2 + 2 - \zeta - \bar{\zeta} - 1$

$= \zeta^2 + \bar{\zeta}^2 - \zeta - \bar{\zeta} + 1$

$= 2\cos(2\pi/5) - 2\cos(\pi/5) + 1.$



This determines an embedding: $\mathbb{Q}(\phi) \hookrightarrow \mathbb{Q}(\zeta)$ (cyclotomic field).

On $\mathbb{Q}(\zeta)$ we have $\mathrm{Frob}_p : \zeta \longmapsto \zeta^p$. $p \nmid 10$

Now: $\mathrm{Frob}_p(\phi) = \begin{cases} \phi & \text{if } p \equiv 1 \text{ or } 9 \bmod 10, \\ \bar{\phi} & \text{if } p \equiv 3 \text{ or } 7 \bmod 10. \end{cases}$