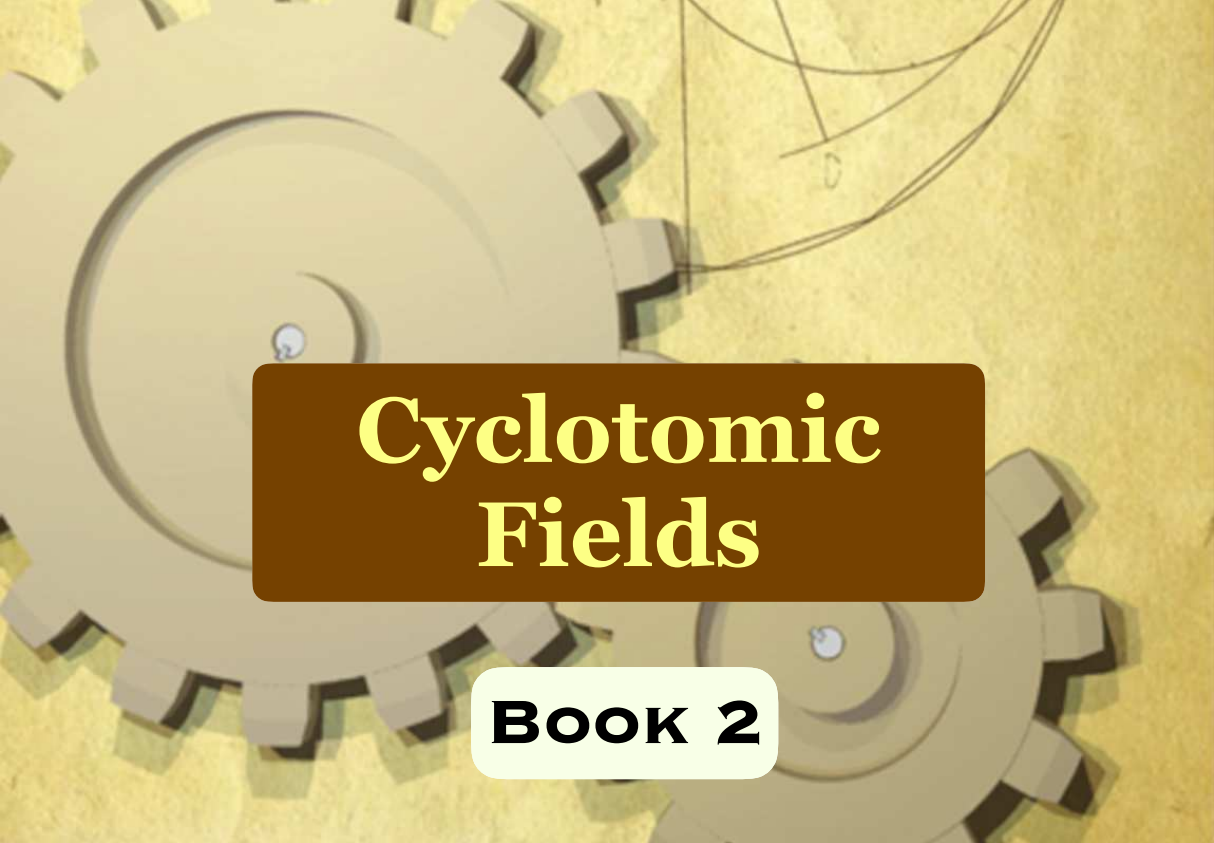

Cyclotomic Fields
Book 2

$$\frac{x}{e^x-1} = 1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4 + \frac{1}{30240}x^6 - \cdots - \frac{691}{1307\cdots 0}x^{12} + \cdots = \sum_{n=0}^{\infty} \frac{B_n}{n!}x^n, \quad B_n = n^{\text{th}} \text{ Bernoulli number}$$

$$g(x) = \frac{x}{e^x-1} + \frac{1}{2}x \qquad g(-x) = \frac{-x}{e^{-x}-1} - \frac{1}{2}x = \frac{-xe^x}{1-e^x} - \frac{1}{2}x = \frac{xe^x}{e^x-1} - x = \frac{xe^x}{e^x-1} - x\frac{e^x-1}{e^x-1} = \frac{x}{e^x-1} = g(x)$$

even function

B_n: $1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, -\frac{1}{42}, \cdots$

We say a (odd) prime p is regular if $B_2, B_4, \cdots, B_{p-3}$ have no numerators divisible by p.

Otherwise p is irregular. ↙ $e^{-1/2}$

Heuristically, about 61% of the primes are regular

37 is the smallest irregular prime

Hilbert Irreducibility Theorem (one form)

If $f(x,y) \in \mathbb{Q}[x,y]$ is irreducible then there exists $b \in \mathbb{Q}$ such that $f(x,b) \in \mathbb{Q}[x]$ is irreducible.

$(x^2+y^2)(x^2+3y^2) = x^4 + 4x^2y^2 + 3y^4$ reducible in $\mathbb{Q}[x,y]$

$E \supseteq \mathbb{Q}$, $[E:\mathbb{Q}] = n$ Galois. $E = \mathbb{Q}[\alpha]$, α root of $m(x) \in \mathbb{Q}[x]$ irreducible of degree n.

$G = \operatorname{Aut} E$ = Galois group of E. G transitively permutes the n roots of $m(x)$.

If $n=3$ then $G \cong C_3$. $m(x) = x^3 + x^2 - 2x - 1$, $E \subset \mathbb{Q}[\zeta_7]$.

Usually if $m(x) \in \mathbb{Q}[x]$ is irreducible of degree 3 then $\mathbb{Q}[\alpha] \supset \mathbb{Q}$ is not Galois; its Galois closure has degree 6 over $\mathbb{Q}$ with Galois group S_3 permuting the three roots of $m(x)$ in all $3! = 6$ ways.

Inverse problem of Galois theory: Given G, find an extension $E \supseteq \mathbb{Q}$ having G as its group of automorphisms.

Try to realize $G \leq S_n$ (transitive subgroup) as the Galois group of $E \supset \mathbb{Q}$, $E = \mathbb{Q}[\alpha_1, \cdots, \alpha_n]$, $m(x) \in \mathbb{Q}[x]$ of degree n, $m(x) = (x-\alpha_1)\cdots(x-\alpha_n)$

If we can find an extension $E \supset \mathbb{Q}(t)$ then specialize t to some rational number
(t indeterminate i.e. transcendental)
hope to get a finite extension of $\mathbb{Q}$ with given Galois group.

A Hadamard matrix of order n is an $n \times n$ matrix H with entries ± 1 such that $HH^T = nI$ (i.e. $H^{-1} = \frac{1}{n}H^T$ i.e. $\frac{1}{\sqrt{n}}H$ is real orthogonal).

$[1]$, $[-1]$, $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$, ...

For $n \geq 1$, if there exists a Hadamard matrix of order n, then $n = 1$ or 2 or $n \equiv 0 \bmod 4$.

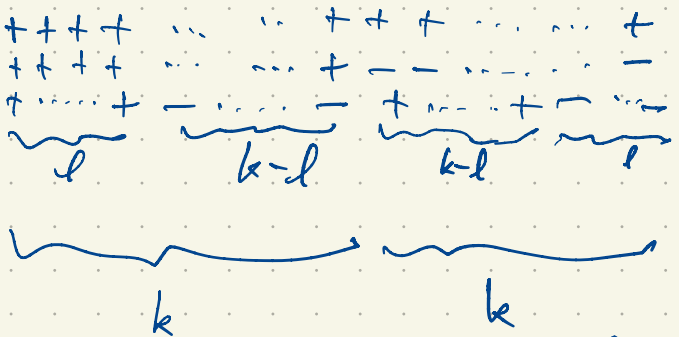
Question: If $n = 4k$ for $k \geq 1$, does there necessarily exist a Hadamard matrix of order n?

The smallest open case was for $n = 668$ until 2026.

If $n \geq 2$ then order n Hadamard requires n even since the dot product of the first two rows is $\equiv n \bmod 2$.

If $n \geq 3$ then we actually require $n \equiv 0 \bmod 4$.

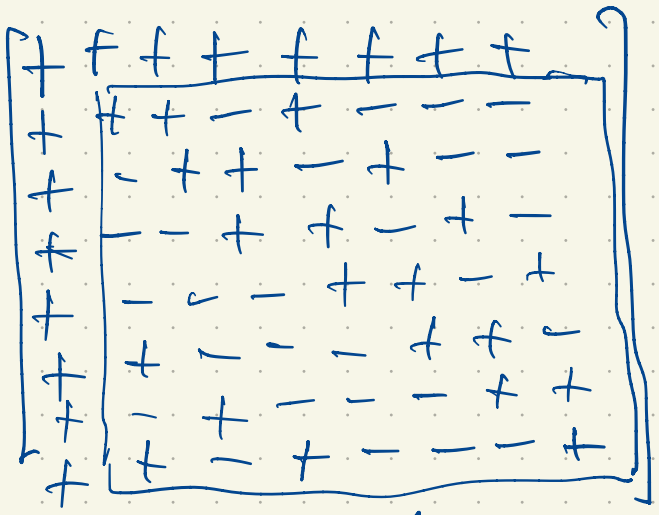
Let H be a Hadamard matrix of order $n \geq 3$. First three rows:



$n = 2k$

$l - (k-l) - (k-l) + l = 4l - 2k = 0$
$\Rightarrow n = 2k = 4l$

Circulant matrix: $\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & \cdots & a_1 \\ \vdots & & & \end{bmatrix}$ each row is a cyclic shift of the previous row



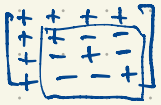
$+ \simeq 1$

$- \simeq -1$

Terry Tao
Mathematics in the Age of AI
preprint: arXiv
YouTube

7×7 circulant matrix

Can replace 7 by any prime $p \equiv 3 \bmod 4$ or any $q \equiv 3 \bmod 4$, prime power eg.

 or  [+]

There are many invalid claims to have proved the Hadamard Matrix Conjecture.

Bernard Schmidt is the expert.

$n = 4k$ A, B, C, D are $k \times k$ circulant matrices with entries ± 1

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

$$HH^T = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} \begin{bmatrix} A & -B & -C & -D \\ B & A & D & -C \\ C & -D & A & B \\ D & C & -B & A \end{bmatrix} = \begin{bmatrix} A^2+B^2+C^2+D^2 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & & \\ 0 & & & \end{bmatrix}$$

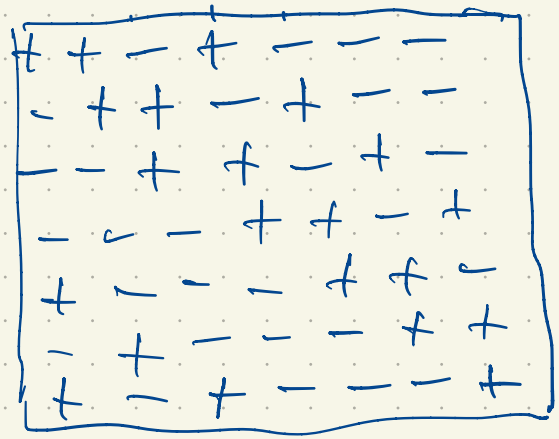
A, B, C, D commute with each other
A, B, C, D symmetric

Need $A^2+B^2+C^2+D^2 = nI = 4kI$

Complex Hadamard matrix of order n: $n \times n$ matrix H with entries h_{ij}, $|h_{ij}| = 1$.
such that $HH^* = H^*H = nI$. These exist for all $n \geq 1$.

eg. $\xi = \xi_n$, $h_{ij} = \xi^{ij}$ $0 \leq i, j \leq n-1$

Using blocks of circulant matrices to construct new Hadamard matrices: why?



$= I + C - C^2 + C^3 - C^4 - C^5 - C^6 \in \mathbb{Q}[C]$

where $I = I_7$, $C = \begin{bmatrix} 0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ \vdots & & & & & & \vdots \\ 0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0 \end{bmatrix}$, $C^7 = I$

$\mathbb{Q}[x]$ = algebra of polynomials in x with rational (number) coefficients

algebra = ring + vector space over $\mathbb{Q}$

$\mathbb{Q}[x] \xrightarrow{\phi} \mathbb{Q}[C]$ algebra homomorphism; surjective

infinite-dimensional 7-dimensional

$\ker\phi \subseteq \mathbb{Q}[x]$ is an ideal. It is a subspace such that $f(x)g(x) \in \ker\phi$ for all $g(x) \in \ker\phi$ and $f(x) \in \mathbb{Q}[x]$.

$\ker\phi = (x^7-1)$ = principal ideal generated by x^7-1

$= \{ f(x)(x^7-1) : f(x) \in \mathbb{Q}[x] \}$.

First Isomorphism Theory: $\mathbb{Q}[C] \cong \mathbb{Q}[x]/(x^7-1) = \{ a_0 + a_1 x + \cdots + a_6 x^6 : a_i \in \mathbb{Q} \}$ with "wrap-around" $x^7 = 1$

If G is cyclic of order 7, say multiplicative, $G = \langle g : g^7 = 1 \rangle = \{1, g, g^2, \cdots, g^6\}$

$\mathbb{Q}[G] = \{ a_0 + a_1 g + a_2 g^2 + \cdots + a_6 g^6 : a_i \in \mathbb{Q} \}$ $\quad g^i g^j = g^{i+j}$ exponents mod 7.

the group algebra of G over $\mathbb{Q}$

i.e. the rational group algebra of G

Because $\mathbb{Q}[G]$ is a commutative algebra, it can be "simultaneously diagonalized"

C has n eigenvalues $1, \xi, \xi^2, \dots, \xi^6$ in $\mathbb{Q}[\xi] = E \supseteq \mathbb{Q}$

with eigenvectors $v_i = \begin{bmatrix} 1 \\ \xi^i \\ \vdots \\ \xi^{6i} \end{bmatrix}$, $Cv_i = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \xi^i \\ \vdots \\ \xi^{6i} \end{bmatrix} = \begin{bmatrix} \xi^i \\ \xi^{2i} \\ \vdots \\ 1 \end{bmatrix} = \xi^i v_i$

$v_0 = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$, $v_1 = \begin{bmatrix} 1 \\ \xi \\ \xi^2 \\ \vdots \\ \xi^6 \end{bmatrix}$, $\dots$ basis of eigenvectors of C.

After conjugating by H (complex Hadamard of order 7) $C \rightsquigarrow \begin{bmatrix} 1 & & & 0 \\ & \xi & & \\ & & \xi^2 & \\ 0 & & & \ddots \\ & & & & \xi^6 \end{bmatrix}$

$$\mathbb{Q}[G] \underset{\mathbb{Q}}{\cong} \bigoplus_{i=0}^{6} \mathbb{Q} \cong \mathbb{Q}^7.$$

Cyclic of order 7

$G = \langle g \rangle = \{1, g, g^2, \dots, g^6\}$, $g^7 = 1$

In $\mathbb{Q}[G]$, the element $\delta = 1 + g + g^3$ satisfies a nice identity: $D = \{1, g, g^3\} \subset G$ is a difference set: every $x \in G$, $x \neq 1$, is uniquely expressible as $x = d_1 d_2^{-1}$, $d_1, d_2 \in D$.

$$\begin{aligned} g \cdot 1^{-1} &= g & 1 \cdot 1^{-1} &= 1 \\ g^3 \cdot 1^{-1} &= g^3 & g \cdot g^{-1} &= 1 \\ 1 \cdot g^{-1} &= g^6 & g^3 \cdot (g^3)^{-1} &= 1 \\ 1 \cdot (g^3)^{-1} &= g^4 & & \\ g \cdot (g^3)^{-1} &= g^5 & & \\ g^3 \cdot g^{-1} &= g^2 & & \end{aligned}$$

9 ways to take $d_1 d_2^{-1}$, $d_1, d_2 \in D$

$$\delta\delta^* = (1 + g + g^3)(1 + g^{-1} + g^{-3}) = 2 + \gamma, \qquad \gamma = \sum_{g \in G} g$$

$\mathbb{Z}G = \mathbb{Z}[G]$ ← integral group algebra

$\mathbb{Q}G = \mathbb{Q}[G]$ ← rational group algebra.

is an algebra with basis G

If $\alpha = \sum_{g \in G} a_g g$, $a_g \in \mathbb{Q}$

then $\alpha^* = \sum_{g \in G} a_g g^{-1}$

If G is any finite group of order $v = |G|$,

a (v, k, λ)-difference set in G is a subset $D \subset G$ of size $|D| = k$ such that every nonidentity element of G can be expressed as $d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$, in λ ways.

In a finite group G, $|G|=v$, a (v,k,r)-difference set is a subset $D \subset G$ such that $|D|=k$ and every nonidentity element $x \in G$ can be expressed as $x = d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$ in exactly r ways.

In order for a difference set to exist, the parameters (v,k,λ) must satisfy certain necessary conditions.

Count in two different ways the number of pairs $(d_1, d_2) \in D^2$:

$$k^2 = k + r(v-1) \Rightarrow k^2 - k = k(k-1) = r(v-1).$$

The condition for $D \subset G$ to be a difference set is expressible in the language of group rings/algebras.

Consider $\delta = \sum_{d \in D} d \in \mathbb{Z}G$ and $\gamma = \sum_{g} g \in \mathbb{Z}G$.

Example: $(7,3,1)$ - difference set in a cyclic group of order 7.

eg. in $G = \langle g : g^7 = 1 \rangle$, $D = \{1, g, g^3\}$, $\gamma = 1+g+g^2+g^3+g^4+g^5+g^6$,

$$\delta = 1+g+g^3, \quad \delta^* = 1+g^{-1}+g^{-3} = 1+g^4+g^6$$

$$\delta\delta^* = (1+g+g^3)(1+g^{-1}+g^{-3}) = 3 + g+g^2+g^3+g^4+g^5+g^6 = 2+\gamma$$

In the general case: $\delta\delta^* = n + r\gamma$ where $n = k - r$

$$= \underbrace{n+r}_{k} + r\sum_{1 \neq g \in G} g$$

If G were written additively as $G = \{0,1,2,3,4,5,6\}$ then $D = \{0,1,3\}$

Every nonidentity $x \in G$ is expressible as $x = d_1 - d_2$ for exactly one pair $(d_1, d_2) \in D^2$, $d_1 \neq d_2$.

How do we search for solutions of $\delta\delta^t = n + r\gamma$ in $\mathbb{Z}G$ or $\mathbb{Q}G$?

As a vector space, $\dim \mathbb{Q}G = |G| = v$

As an algebra over $\mathbb{Q}$, if G is abelian then $\mathbb{Q}G \cong \mathbb{Q}^v = \underbrace{\mathbb{Q} \oplus \mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{v \text{ times}}$

There are many algebra homomorphisms $\mathbb{Q}G \longrightarrow \mathbb{C}$ ("linear characters")

i.e. maps $\chi : \mathbb{Q}G \longrightarrow \mathbb{C}$

$$\chi(a\alpha + b\beta) = a\chi(\alpha) + b\chi(b) \qquad a, b \in \mathbb{Q},\ \alpha, \beta \in \mathbb{Q}G$$

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$$

$$\chi(1) = 1.$$

eg. $\chi_i : \mathbb{Q}^v \longrightarrow \mathbb{C}$

$(x_1, \ldots, x_v) \longmapsto x_i$

Assuming G is abelian, G has exactly $v = |G|$ algebra homomorphisms

$\chi_i : \mathbb{Q}G \longrightarrow \mathbb{C}$

For $\alpha, \beta \in \mathbb{Q}G$, $\alpha = \beta$ iff $\chi(\alpha) = \chi(\beta)$ for all $\chi \in \hat{G} = \{\text{algebra homomorphisms } \mathbb{Q}G \to \mathbb{C}\}$.

If $G = \{1, g\}$, $g^2 = 1$

$\chi_0(1) = \chi_0(g) = 1$ $\qquad$ $\chi_1(1) = 1$, $\chi_1(g) = -1$

$\chi_0(a + bg) = a + b$ $\qquad$ $\chi_1(a + bg) = a - b$.

Apply these homomorphisms to the equation $\delta\delta^t = n + r\gamma$

Theorem Let G be an abelian mult. gp. of order v and consider a nonempty subset $D \subset G$, $|D| = k < v$ and $\delta = \sum_{d \in D} d \in \mathbb{Z}G$. Then

D is a (v,k,r)-diff. set in G iff $k^2 - rv = n := k - r$ and

$$|\chi(\delta)| = \sqrt{n}$$

for every nontrivial $\chi \in \hat{G}$.

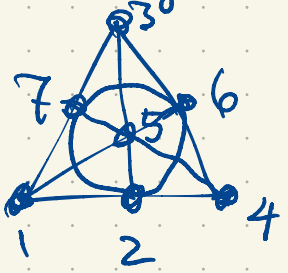
(v,k,r) difference set in group G $\longrightarrow$ (v,k,r) design (combinatorial structure)

Let V be a set of cardinality $|V| = v$ and let $1 < k < v$, $r \geq 1$.
A (v,k,r) **design** in V is a collection $\mathcal{B} = \{B_1, \dots, B_v\}$ of subsets of V (called blocks) of size $|B_1| = |B_2| = \cdots = |B_v| = k$ (block size) such that for all $v_1 \neq v_2$ in V (points) we have exactly r blocks containing both v_1 and v_2. Dually, we require any two blocks intersect in exactly $|B_i \cap B_j| = r$. $(i \neq j)$. Every point is in k blocks.

Eg. $V = \{1,2,3,4,5,6,7\}$

$\mathcal{B} = \{\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,7\}, \{5,6,1\}, \{6,7,2\}, \{7,1,3\}\}$.

This is a $(7,3,1)$-design. Any two (distinct) points are in exactly one block. Any two distinct blocks intersect in 1 point. Every point is in $k=3$ blocks and every block has exactly 3 points.



Point-block incidence matrix:

	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1	0	0	0	1	0	1
2	1	1	0	0	0	1	0
3	0	1	1	0	0	0	1
4	1	0	1	1	0	0	0
5	0	1	0	1	1	0	0
6	0	0	1	0	1	1	0
7	0	0	0	1	0	1	1

circulant matrix

A $(7,4,2)$-design

$V = \{1,2,3,4,5,6,7\}$

$\mathcal{B} = \{\{3,5,6,7\}, \{4,6,7,1\}, \{5,7,1,2\}, \{6,1,2,3\}, \{7,2,3,4\}, \{1,3,4,5\}, \{2,4,5,6\}\}$

7 points
7 blocks
each block has 4 points
each point is in 4 blocks
Two different points in 2 blocks

Incidence matrix:

$$\begin{bmatrix} 0&1&1&1&0&1&0 \\ 0&0&1&1&1&0&1 \\ 1&0&0&1&1&1&0 \\ 0&1&0&0&1&1&1 \\ 1&0&1&0&0&1&1 \\ 1&1&0&1&0&0&1 \\ 1&1&1&0&1&0&0 \end{bmatrix}$$

$k^2 - r\nu = n = k - r$

$(n+1)^2 - 1\cdot(n^2+n+1) = n$

A symmetric design with $r=1$ has parameters $(\underbrace{n^2+n+1}_{\nu}, \underbrace{n+1}_{k}, \underbrace{1}_{r})$ which is a projective plane of order n.
(a very special and important case of a symmetric design.)

One way to construct a symmetric design (in particular a projective plane) is using a difference set.

Let $D \subset G$ be a (v,k,r)-difference set in a group G, $|G| = v$.
This means: $|D| = k$, and every $1 \neq x \in G$ can be expressed as $x = d_1 d_2^{-1}$ for exactly r choices of $(d_1, d_2) \in D^2$, $d_1 \neq d_2$.

From this we construct a symmetric (v,k,r)-design in $V = G$ with blocks
$Dh = \{dh : d \in D\}$, $h \in G$.

$x \in Dh \cap Dh'$ $h \neq h'$ in G

$\iff x = d_1 h = d_2 h'$

$\Rightarrow d_1 = d_2 h' h^{-1}$

$d_2^{-1} d_1 = h' h^{-1}$

Eg. $G = \{1, g, g^2, \dots, g^6\}$, $g^7 = 1$: $D = \{1, g, g^3\}$

$Dg = \{g, g^2, g^4\}$

$Dg^2 = \{g^2, g^3, g^5\}$

$\vdots$

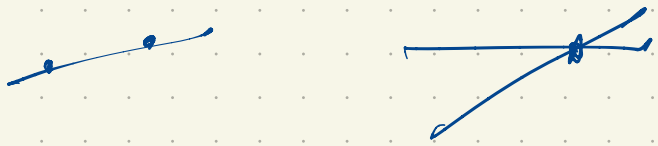
$Dg^6 = \{g^6, 1, g^2\}$

Big question: for which n does there exist a projective plane of order n?

If $q = p^e$, p prime, $e \geq 1$ (prime powers) then there exists a (unique) field $\mathbb{F}_q$ of order q

We have at least one projective plane of each prime power order q.

Let $F = \mathbb{F}_q$. $|F| = q$. Then F^3 has q^3 vectors, q^2+q+1 (points) one-dimensional subspaces, q^2+q+1 two-dimensional subspaces (lines)



A projective plane is a symmetric $(n^2+n+1, n+1, 1)$-design i.e. $n \geq 2$

n^2+n+1 points
n^2+n+1 lines
$n+1$ points on every line
$n+1$ lines through every point



Can we figure out the first row without constructing the entire plane?

Hall's Multiplier Theorem Let D be a (v,k,r)-difference set in an abelian group G of order $|G| = v$, i.e. $D \subset G$, $|D| = k$ and every $1 \neq x \in G$ can be expressed as $x = d_1 d_2^{-1}$ for $d_1 \neq d_2$ in D in exactly r ways. Let $n = k - r$ (the order of the difference set). Suppose p is a prime divisor of n with $p \nmid v$. Then

$$D^{[p]} := \{d^p : d \in D\} = gD := \{gd : d \in D\} \text{ for some } g \in G.$$

If $G = \mathbb{Z}/N\mathbb{Z}$, $G = \{0, 1, \cdots, N-1\} \bmod N$, $D \subset G$

in multiplicative notation $G = \{1, g, g^2, \cdots, g^{N-1}\}$, g generator of G

$d_1 = g^{e_1}$, $d_2 = g^{e_2}$

$d_1 d_2^{-1} = g^{e_1 - e_2}$

WLOG D is chosen such that

$D^{[p]} = D$

$D = \{g^{e_1}, \cdots, g^{e_k}\}$

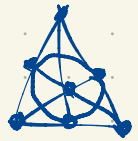
$D^{[p]} = \{g^{pe_1}, \cdots, g^{pe_k}\}$

$n = 1$ $(3, 2, 1)$



$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

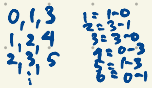
$n = 2$



$G = \{1, g, g^2, \cdots, g^6\}$, $g^7 = 1$

$D = \{1, g, g^3\}$

$gD = \{g, g^2, g^4\}$



$n=2$, take $p=2$ ✓

Look for $D \subset G = \{0,1,\cdots,6\}$ mod 7, $|D|=3$ such that $D^{[2]} = D$.

($D^{[2]}$ becomes $2D$)

Multiplication by 2 in $G = \mathbb{Z}/7\mathbb{Z}$:

$0 \mapsto 0$

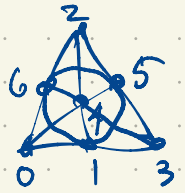
$1 \mapsto 2 \mapsto 4 \mapsto 1$

$3 \mapsto 6 \mapsto 5 \mapsto 3$

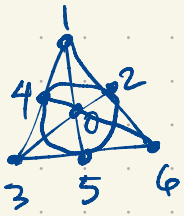
So $D = \{1,2,4\}$ or $\{3,5,6\}$

equivalent to $0,1,3$

0	1	3
1	2	4
2	3	5
3	4	6
4	5	0
5	6	1
6	0	2



3	5	6
4	6	0
5	0	1
6	1	2
0	2	3
1	3	4
2	4	5



Big open problem:

Is there any plane of non-prime-power order?

Now construct a projective plane of order $n=3$. $p=3$, $N = n^2+n+1 = 13$

$G = \mathbb{Z}/13\mathbb{Z} = \{0,1,2,\cdots,12\}$ mod 13

The multiplier 3: $G \to G$ permutation

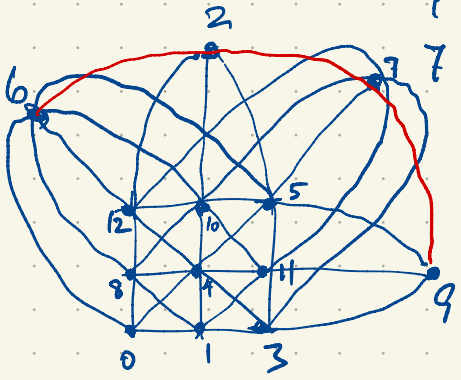
$0 \mapsto 0$

$1 \mapsto 3 \mapsto 9 \mapsto 1$

$2 \mapsto 6 \mapsto 5 \mapsto 2$

$4 \mapsto 12 \mapsto 10 \mapsto 4$

$7 \mapsto 8 \mapsto 11 \mapsto 7$



$n=3$

$n^2+n+1 = 13$ points/lines

$n+1 = 4$ points/line

$n+1 = 4$ lines/point

$|D| = k = n+1 = 4$

To form a set of size 4 as a union of orbits of the multiplier 3, we need $\{0\} \cup$ any orbit of size 3 e.g.

$D = \{0,1,3,9\}$

$0,1,3,9$

$1,2,4,10$

$2,3,5,11$

$3,4,6,12$

$4,5,7,0$

$5,6,8,1$

$6,7,9,2$

$7,8,10,3$

$8,9,11,4$

$9,10,12,5$

$10,11,0,6$

$11,12,1,7$

$12,0,2,8$

$1 = 1-0$

$2 = 3-1$

$3 = 3-0$

$4 = 0-9$

$5 = 1-9$

$6 = 9-3$

$7 = 3-9$

$8 = 9-1$

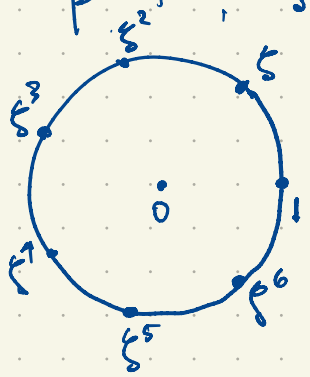
$9 = 9-0$

$10 = 0-3$

$11 = 1-3$

$12 = 0-1$

$p=7$, $\zeta=\zeta_7$ primitive 7th root of unity e.g. $\zeta = e^{2\pi i/7}$



$$\underbrace{1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6}_{\Phi_7(\zeta)} = 0$$

Inside $E = \mathbb{Q}[\zeta] = \{a_0+a_1\zeta+a_2\zeta^2+\cdots+a_5\zeta^5 : a_i\in\mathbb{Q}\}$, $[E:\mathbb{Q}]=6$

$1,\zeta,\zeta^2,\dots,\zeta^5$ basis

we take $\alpha = \zeta+\zeta^2+\zeta^4$ (Note: 1,2,4 difference set mod 7)

$$|\alpha|^2 = \alpha\bar{\alpha} = (\zeta+\zeta^2+\zeta^4)(\zeta^{-1}+\zeta^{-2}+\zeta^{-4}) = 3+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6$$
$$= 2+(1+\zeta+\zeta^2+\cdots+\zeta^6) = 2$$

$$|\alpha| = \sqrt{2}$$

Bernard Schmidt

Is $\sqrt{2}\in E=\mathbb{Q}[\zeta]$? No.

No; but $\sqrt{-7}\in E$. We saw this several weeks ago. The explanation will be revealed over the next couple of classes.

It is tempting to think that $\left|\frac{\alpha}{\sqrt{2}}\right|=1 \Rightarrow \frac{\alpha}{\sqrt{2}}$ is a root of unity.

Theorem If α is an algebraic integer (a root of a monic poly. with integer coefficients) such that $|\alpha^\sigma|=1$ for every $\sigma\in \mathrm{Aut}\,\mathbb{C}$ then α is a root of unity. (Chapter 1)

Note: $\alpha=\frac{3+4i}{5}$ is an algebraic number, $\bar{\alpha}=\frac{3-4i}{5}$, $|\alpha|^2=\alpha\bar{\alpha}=1 \Rightarrow |\alpha|=1$, $|\alpha^\sigma|=1$ for every $\sigma\in\mathrm{Aut}\,\mathbb{C}$

α is not a root of unity. But α is not an algebraic integer.

Its min. poly. over $\mathbb{Q}$ is $x^2-\frac{6}{5}x+1\in\mathbb{Q}[x]$, not in $\mathbb{Z}[x]$.

Eg. $\alpha = \sqrt{\sqrt{2}-1}+i\sqrt{2-\sqrt{2}}$ $|\alpha|^2 = \sqrt{2}-1+2-\sqrt{2}=1 \Rightarrow |\alpha|=1$.

Conjugate $\pm\sqrt{-\sqrt{2}-1}+i\sqrt{2+\sqrt{2}}$ has absolute value >1.

α is not a root of unity.

$\pm i\sqrt{\sqrt{2}+1}+i\sqrt{2+\sqrt{2}}$

$i\sqrt{\sqrt{2}+1}+i\sqrt{2+\sqrt{2}} = i\sqrt{\sqrt{2}+1}\,(1+\sqrt{2})$

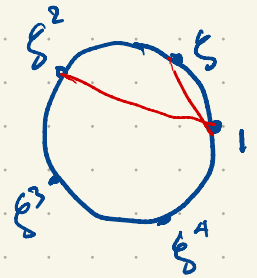
has absolute value $(\sqrt{2}+1)^{3/2}>1$.

Algebraic conjugation does not preserve absolute value.

eg. $3+\sqrt{2} \longmapsto 3-\sqrt{2}$ absolute value changes!

Even in cyclotomic fields, $\alpha \in \mathbb{Q}[\zeta]$, $\sigma \in \mathrm{Aut}\,\mathbb{Q}[\zeta]$, α^σ doesn't necessarily have the same absolute value as α eg.

(α^σ: algebraic conjugate of α)



$\zeta = \zeta_5$

$\zeta - 1 \longmapsto \zeta^2 - 1$ (algebraic conjugation)

$|\zeta - 1| < |\zeta^2 - 1|$

However if $\alpha \in \mathbb{Q}[\zeta]$, $|\alpha| = 1$ then $|\alpha^\sigma| = 1$ for all $\sigma \in \mathrm{Aut}\,\mathbb{Q}[\zeta]$

More generally if $|\alpha| = k$ then $|\alpha^\sigma| = k$ for all $\sigma \in \mathrm{Aut}\,\mathbb{Q}[\zeta]$ ($k \in \mathbb{Z}$)

($\mathrm{Aut}\,\mathbb{Q}[\zeta]$ Abelian)

Proof: $|\alpha^\sigma|^2 = \alpha^\sigma \overline{\alpha^\sigma} = \alpha^\sigma \bar{\alpha}^\sigma = (\alpha\bar{\alpha})^\sigma = (|\alpha|^2)^\sigma = (k^2)^\sigma = k^2 \Rightarrow |\alpha^\sigma| = k$. □

Back to example $\alpha = \zeta + \zeta^2 + \zeta^4 \in \mathbb{Q}[\zeta]$, $\zeta = e^{2\pi i/7}$

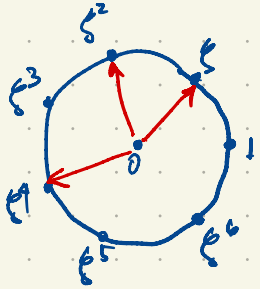
$\alpha^2 = (\zeta + \zeta^2 + \zeta^4)(\zeta + \zeta^2 + \zeta^4) = \underbrace{\zeta^2 + \zeta^4 + \zeta}_{\alpha} + \underbrace{2\zeta^3 + 2\zeta^5 + 2\zeta^6}_{2(-1-\alpha)}$

$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0$ ($-1-\alpha$ / α)

$= -2 - \alpha$

$\alpha^2 + \alpha + 2 = 0$

$\alpha = \frac{-1 \pm \sqrt{1-8}}{2} = \frac{-1 \pm \sqrt{-7}}{2}$ ($\sqrt{-7} = i\sqrt{7}$)



$\alpha = \frac{-1+\sqrt{-7}}{2} \in$ upper half-plane $\quad 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0$

$\sqrt{-7} = 1 + 2\alpha = 1 + 2\zeta + 2\zeta^2 + 2\zeta^4 = \zeta + \zeta^2 - \zeta^3 + \zeta^4 - \zeta^5 - \zeta^6$

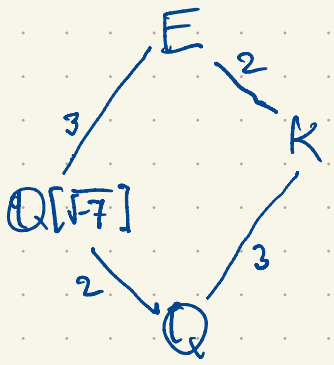
$\sqrt{-7} \in \mathbb{Q}[\zeta]$ but $i, \sqrt{7}, \sqrt{2} \notin \mathbb{Q}[\zeta]$ using Galois Theory

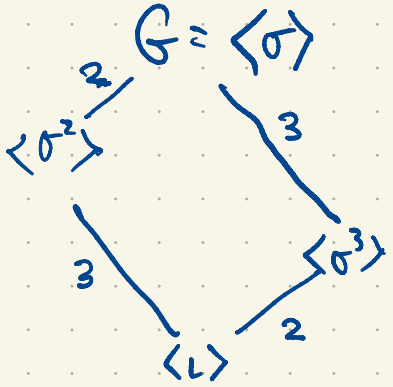
Galois theory gives a strong connection between the field $E = \mathbb{Q}[\xi]$ and its Galois group $G = \mathrm{Aut}\, E$:

$$|G| = [E:\mathbb{Q}] = 6$$

There is a one-to-one correspondence between subgroups of G and subfields of E.

G has exactly four subgroups (cyclic of order 1, 2, 3, 6) so E has exactly four subfields $E, \mathbb{Q}, \mathbb{Q}[\sqrt{-7}]$,





$\sigma(\xi) = \xi^3$

$\sigma^2(\xi) = (\xi^3)^3 = \xi^9 = \xi^2$

$\sigma^3(\xi) = (\xi^2)^3 = \xi^6 = \bar{\xi}$

$\sigma^4(\xi) = (\xi^6)^3 = \xi^{18} = \xi^4$

$\sigma^5(\xi) = (\xi^4)^3 = \xi^{12} = \xi^5$

$\sigma^6(\xi) = (\xi^5)^3 = \xi^{15} = \xi$; $\sigma^6 = 1$

$K = E \cap \mathbb{R} =$ maximal real subfield of E

I want to reuse the letter α to be $\alpha = \xi + \bar{\xi} \in K = \xi + \xi^6 \in \mathbb{Q}$ (by uniqueness of the minimal polynomial of ξ i.e. $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$). So $K = \mathbb{Q}[\alpha]$. Why? $K \supseteq \mathbb{Q}[\alpha] \supsetneq \mathbb{Q}$, $[K:\mathbb{Q}] = 3 = [K:\mathbb{Q}[\alpha]]\,[\mathbb{Q}[\alpha]:\mathbb{Q}]$ transitivity of degree of extensions

So α has min. poly. over $\mathbb{Q}$ of degree 3

$\alpha = \xi + \xi^{-1}$

$\alpha^2 = \xi^2 + 2 + \xi^{-2}$

$\alpha^3 = \xi^3 + 3\xi + 3\xi^{-1} + \xi^{-3}$

$\alpha^3 + \alpha^2 = \xi^3 + \xi^{-3} + 3(\xi + \xi^{-1}) + \xi^2 + \xi^{-2} + 2 = \underbrace{(\xi^3 + \xi^{-3} + \xi^2 + \xi^{-2} + \xi + \xi^{-1} + 1)}_{0} + 2(\xi + \xi^{-1}) + 1 = 2\alpha + 1$

$\xi^3 = \xi^9$, $\xi^{-2} = \xi^5$, $\xi^{-3} = \xi^4$

$\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$

So $m(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x] \subset \mathbb{C}[x]$ is the minimal poly. of α. What are the three roots α, β, γ of $m(x)$? Are they all real? Claim: $\beta = \alpha^2 - 2$ is another root.

$m(\beta) = (\alpha^2-2)^3 + (\alpha^2-2)^2 - 2(\alpha^2-2) - 1 = (\alpha^6 - 6\alpha^4 + 12\alpha^2 - 8) + (\alpha^4 - 4\alpha^2 + 4) - 2\alpha^2 + 4 - 1$

$= \alpha^6 - 5\alpha^4 + 6\alpha^2 - 1$

$= (9\alpha^2 - 5\alpha - 4) - 5(3\alpha^2 - \alpha - 1) + 6\alpha^2 - 1$

$= 0$

$\Rightarrow \gamma = \beta^2 - 2$ is a root and $\gamma^2 - 2$ is a root. How many of these roots are distinct?

$\gamma^2 - 2 = \alpha$

$\alpha^3 = -\alpha^2 + 2\alpha + 1$

$\alpha^4 = -\alpha^3 + 2\alpha^2 + \alpha = -(-\alpha^2 + 2\alpha + 1) + 2\alpha^2 + \alpha = 3\alpha^2 - \alpha - 1$

$\alpha^5 = 3\alpha^3 - \alpha^2 - \alpha = 3(-\alpha^2 + 2\alpha + 1) - \alpha^2 - \alpha = -4\alpha^2 + 5\alpha + 3$

$\alpha^6 = -4\alpha^3 + 5\alpha^2 + 3\alpha = -4(-\alpha^2 + 2\alpha + 1) + 5\alpha^2 + 3\alpha = 9\alpha^2 - 5\alpha - 4$

$\beta \in \mathbb{Q}[\alpha]$ since $\beta = \alpha^2 - 2$

$\Rightarrow \mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha]$

$\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha] \Rightarrow \mathbb{Q}[\alpha] = \mathbb{Q}[\beta] = \mathbb{Q}[\gamma] = K.$

So $m(x) = (x-\alpha)(x-\beta)(x-\gamma)$ and $\alpha, \beta, \gamma \in \mathbb{R}$

So K is the splitting field of $m(x) = x^3 + x^2 - 2x - 1$.

$\alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$ is the cyclic automorphism of K of order 3.

Let p be an odd prime. Fermat's Little Theorem: In $F = \mathbb{F}_p = \{0, 1, 2, \cdots, p-1\}$, $a^p = a$ for all $a \in F$. If $0 \neq a \in F$ then $a^{p-1} = 1$. (Proof: $F^\times$ is a multiplicative group of order $p-1$.) Use Lagrange's Theorem.

Moreover, $F^\times$ is cyclic. $F^\times = \{1, g, g^2, \cdots, g^{p-2}\}$, $g^{p-1} = 1$. $1, g^2, g^4, \cdots, g^{p-3}$ are squares; $g, g^3, g^5, \cdots, g^{p-2}$ are nonsquares.

(For $p = 7$, $g = 3$ gives 1, 2, 4 as squares; 3, 5, 6 are nonsquares.)

For any $a \in \mathbb{Z}$, write the Legendre symbol $\left(\frac{a}{p}\right) \in$ integer $= \begin{cases} 0 & \text{if } p \mid a \text{ i.e. } a \equiv 0 \bmod p; \\ 1 & \text{if } a \equiv \text{nonzero square} \bmod p; \\ -1 & \text{if } a \equiv \text{nonsquare} \bmod p. \end{cases}$

For $p = 7$:

a	$\left(\frac{a}{7}\right)$	$a^{\frac{7-1}{2}} \bmod 7$
0	0	0
1	1	1
2	1	1
3	-1	$6 \equiv -1$
4	1	1
5	-1	$6 \equiv -1$
6	-1	$6 \equiv -1$
7	0	
8	1	
9	1	
10	-1	
$\vdots$	$\vdots$	

Euler's Criterion: for all $a \in \mathbb{Z}$, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.

Proof: If $a \equiv 0 \bmod p$, we have $0 \equiv 0 \bmod p$.

If $a \equiv b^2 \bmod p$, $b \not\equiv 0 \bmod p$, then $a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p$.

The polynomial $x^2 - 1 = (x+1)(x-1)$ has exactly two roots in $F = \mathbb{F}_p$.

$x^{p-1} - 1 = (x^{\frac{p-1}{2}} + 1)(x^{\frac{p-1}{2}} - 1)$ has $p-1$ roots in F, all the nonzero elements $F^\times$.

$\frac{p-1}{2}$ roots: the nonsquares. $\frac{p-1}{2}$ roots in $F^\times$: the nonzero squares.

Corollary: for all $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof: $\left(\frac{ab}{p}\right) \in 0, \pm 1$; $\left(\frac{a}{p}\right) \in 0, \pm 1$; $\left(\frac{b}{p}\right) \in 0, \pm 1$.

Left side: $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \bmod p$.

Right side: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \bmod p$. $\square$

The quadratic Gauss sum for odd prime p: Let $\zeta = e^{2\pi i/p}$ (For this, we need this specific primitive p^{th} root of 1)

$$S = S_p = \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right)\zeta^a \in \mathbb{Z}[\zeta] \quad \text{(cyclotomic integer)}$$

Theorem $S^2 = \pm p$ so $S = \pm\sqrt{p}$ or $\pm i\sqrt{p} = \pm\sqrt{-p}$.

Precisely, $S^2 = \begin{cases} p & \text{if } p \equiv 1 \bmod 4 \\ -p & \text{if } p \equiv 3 \bmod 4 \end{cases} = (-1)^{\frac{p-1}{2}} p = \left(\frac{-1}{p}\right) p$

by Euler's criterion, -1 is a square mod p iff $p \equiv 1 \bmod 4$.

Note: $S = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^k = \sum_{l=0}^{p-1} \left(\frac{l}{p}\right)\zeta^l$

Proof of Theorem

$$S^2 = \left[\sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^k\right]\left[\sum_{l=0}^{p-1} \left(\frac{l}{p}\right)\zeta^l\right] = \sum_{k=1}^{p-1}\sum_{l=0}^{p-1} \left(\frac{k}{p}\right)\left(\frac{l}{p}\right)\zeta^{k+l} = \sum_{k\in\mathbb{F}^\times}\sum_{l=0}^{p-1} \left(\frac{kl}{p}\right)\zeta^{k+l} \qquad \begin{matrix} l = km \\ l \in F \Leftrightarrow m \in F \end{matrix}$$

$$= \sum_{k\in\mathbb{F}^\times}\sum_{m\in F} \left(\frac{k^2 m}{p}\right)\zeta^{k+km} = \sum_{k\in\mathbb{F}^\times}\sum_{m\in F} \left(\frac{m}{p}\right)\zeta^{(1+m)k}$$

$$\left(\frac{k^2}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{m}{p}\right)$$

$$= \sum_{m\in F}\left(\frac{m}{p}\right)\sum_{k\in\mathbb{F}^\times}\zeta^{(m+1)k} = \underbrace{\left(\frac{-1}{p}\right)(p-1)}_{m=-1} + \sum_{\substack{m\neq -1 \\ m\in F}}\left(\frac{m}{p}\right)(-1)$$

If $m = -1 = p-1$ in $\mathbb{F}$, the inner sum is $\sum_{k\in\mathbb{F}^\times} 1 = p-1$.

If $m \neq -1$ then the inner sum is

$\sum_{k\in F} \zeta^{(m+1)k} = 0$ since the exponent ranges over all integers mod p exactly once

$\sum_{k\in\mathbb{F}^\times} \zeta^{(m+1)k} = -1 \in \mathbb{C}$

$\sum_{m\in F}\left(\frac{m}{p}\right) = 0$ (one term 0, $\frac{p-1}{2}$ terms 1, $\frac{p-1}{2}$ terms -1)

$$\sum_{\substack{m\in F \\ m\neq -1}}\left(\frac{m}{p}\right) = -\left(\frac{-1}{p}\right)$$

$$S^2 = \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p = \begin{cases} p & \text{if } p \equiv 1 \bmod 4 \\ -p & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

$\Rightarrow$ The quadratic Gauss sum has value

$$S = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \bmod 4 \\ \pm\sqrt{-p} = \pm i\sqrt{p} & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

Gauss was able to prove both of these signs are '+':

$$S = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \bmod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Law of Quadratic Reciprocity

How do we compute the Legendre symbol $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is nonzero square mod } p \\ -1, & \text{" " " nonsquare " " } \\ 0, & \text{if } a \equiv 0 \bmod p. \end{cases}$

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

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

$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases} \} = (-1)^{\frac{p^2-1}{8}}$

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

If $p \neq q$ odd primes

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p, q \text{ are not both } 3 \bmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases} \} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Examples using the law of Quadratic Reciprocity to compute $\left(\frac{a}{p}\right)$ by hand for modest-size numbers a, p

eg. $p = 71$, $a = 14$. $\left(\frac{14}{71}\right) = \left(\frac{2}{71}\right)\left(\frac{7}{71}\right) = \left(\frac{7}{71}\right) = -\left(\frac{71}{7}\right) = -\left(\frac{1}{7}\right) = -1$ i.e. 14 is a nonsquare mod 71.

($71 \equiv -1 \bmod 8$ so $\left(\frac{2}{71}\right) = 1$; $7 \equiv 71 \equiv 3 \bmod 4$)

eg. $p = 101$, $a = 53$: $\left(\frac{53}{101}\right) = \left(\frac{101}{53}\right) = \left(\frac{-5}{53}\right) = \left(\frac{48}{53}\right) = \left(\frac{16\cdot 3}{53}\right) = \left(\frac{16}{53}\right)\left(\frac{3}{53}\right) = \left(\frac{3}{53}\right) = \left(\frac{53}{3}\right) = \left(\frac{2}{3}\right) = -1$.

($53 \equiv 1 \bmod 4$)

$= \left(\frac{-1}{53}\right)\left(\frac{5}{53}\right) = \left(\frac{5}{53}\right) = \left(\frac{53}{5}\right) = \left(\frac{3}{5}\right) = -1$

($53 \equiv 1 \bmod 4$, $\left(\frac{-1}{53}\right) = 1$)

How hard is it to find a nonsquare mod p (p odd prime is given)?

$\frac{14}{84} = \frac{1}{4}$

If $x, y \in \mathbb{Z}$ and p is prime then $(x+y)^p \equiv x^p + y^p \mod p$.

Proof of the law of Quadratic Reciprocity.

Let p and q be odd primes, $p \neq q$, and fix a primitive p^{th} root of unity $\zeta = \xi_p$.

Recall the quadratic Gauss sum $S = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta^k$ which as we proved satisfies

$$S^2 = (-1)^{\frac{p-1}{2}} p = \left(\frac{-1}{p}\right) p .$$

Take the $\frac{q-1}{2}$ power of both sides:

$$\left(S^2\right)^{\frac{q-1}{2}} \equiv \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} \mod q .$$

$(-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}}$; $p^{\frac{q-1}{2}}$ → Euler's criterion

$$\equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) \mod q .$$

$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \pm 1$

Now we just need to simplify the left side.