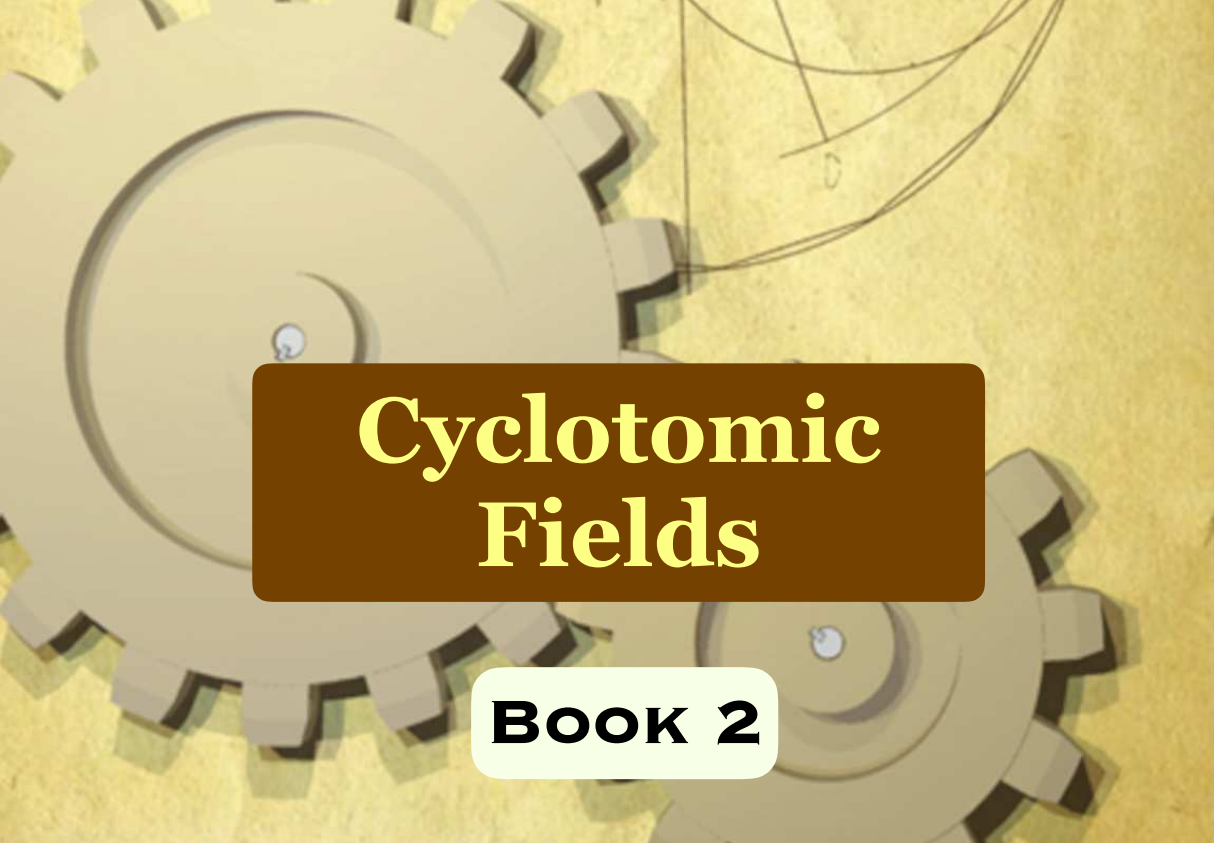

Cyclotomic
Fields
Book 2

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

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

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 $n \equiv 0 \bmod 4$.

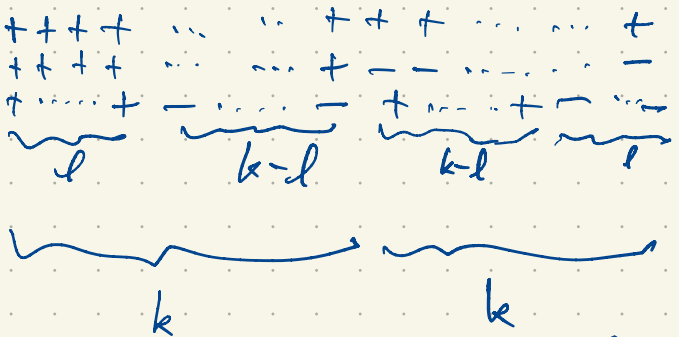
Question: If $n = 4k$ for $k \geq 1$, does there necessarily exist a Hadamard matrix of order n?

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 $n \equiv 0 \bmod 4$.

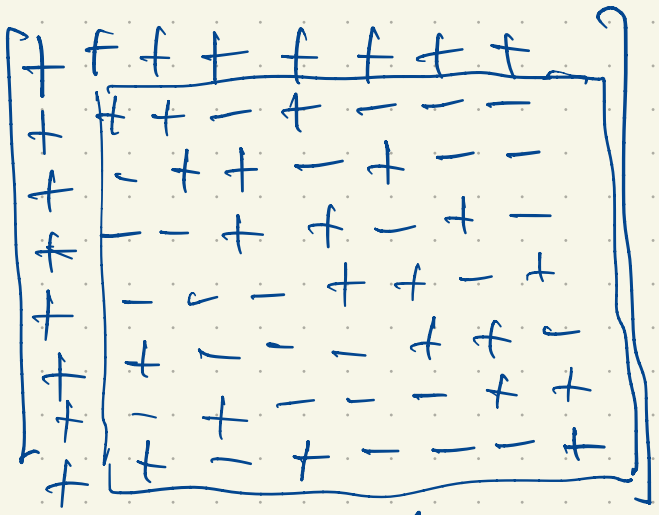
Let H be a Hadamard matrix of order $n \geq 3$. First three rows:



$n = 2k$

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

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



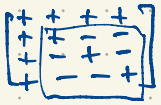
$+ \simeq 1$

$- \simeq -1$

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

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

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

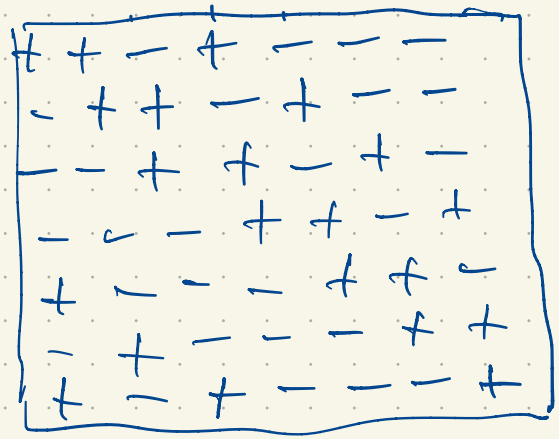
A, B, C, D commute with each other
A, B, C, D symmetric

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 $\chi \in \hat{G}$.

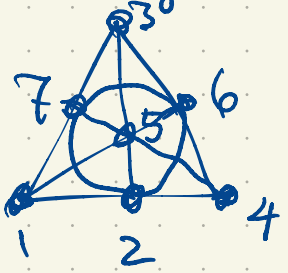
(v,k,r) difference set in group G $\longrightarrow$ (v,k,r) design (combinatorial structure)

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

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

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

$\vdots$

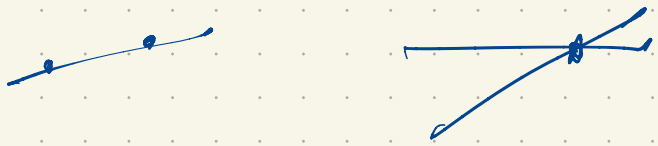
$Dg^6 = \{g^6, 1, g^2\}$

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

$D^{[p]} = D$

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

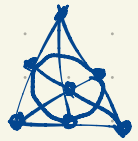
$D^{[p]} = \{g^{pe_1}, \cdots, g^{pe_k}\}$

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



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

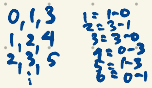
$n = 2$



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

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

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



$n=2$, 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

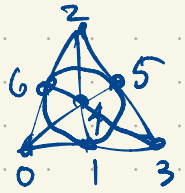
Multiplication by 2 in $G = \mathbb{Z}/7\mathbb{Z}$:

$0 \mapsto 0$
$1 \mapsto 2 \mapsto 4 \mapsto 1$
$3 \mapsto 6 \mapsto 5 \mapsto 3$

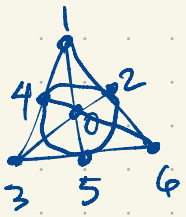
So $D = \{1, 2, 4\}$ or $\{3, 5, 6\}$

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



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

$0 \mapsto 0$
$1 \mapsto 3 \mapsto 9 \mapsto 1$
$2 \mapsto 6 \mapsto 5 \mapsto 2$
$4 \mapsto 12 \mapsto 10 \mapsto 4$
$7 \mapsto 8 \mapsto 11 \mapsto 7$

$|D| = k = n+1$