Jan 27th

The story so far: (not-λ)

(1) If a symmetric (v,k,λ)-design exists then $I_v \simeq nJ_v + \lambda I_v$.

(2) With Bruckelection:

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \simeq \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}, \quad A_1 \simeq B_1 \Rightarrow A_2 \simeq B_2$$

(and some invertibility condition)

(3) $J_u \simeq nJ_u$ $(n \in \mathbb{Z}_{>0})$.. ← Proof next time

Lemma:

If a symmetric (v,k,λ)-design exists, then

$$\begin{pmatrix} J_v & 0 \\ 0 & -\lambda \end{pmatrix} \simeq n \cdot \begin{pmatrix} J_v & 0 \\ 0 & -\lambda \end{pmatrix}$$

$(v+1)\times(v+1)$ matrix

Proof: (Outline)

We already know that if the design exists, then $J_v \simeq nJ_v + \lambda J_v$.

$$\Rightarrow \begin{pmatrix} J_v & 0 \\ 0 & -\lambda \end{pmatrix} \simeq \begin{pmatrix} nJ_v + \lambda J_v & 0 \\ 0 & -\lambda \end{pmatrix}$$

Using

$$P = \begin{pmatrix} J_v & \frac{1}{k} J_v \\ J_v^T & k \end{pmatrix}$$

we can check that

$$\begin{pmatrix} nJ_v + \lambda J_v & 0 \\ 0 & -\lambda \end{pmatrix} \simeq \begin{pmatrix} nJ_v & 0 \\ 0 & -n\lambda \end{pmatrix}.$$

□

Theorem (Bruck-Ryser-Chowla (BRC))
Suppose a symmetric (v,k,λ)-design exists and let $n=k-\lambda$.
(a) If v is even, then n is a square
(b) If $v\equiv 1 \pmod 4$ then the equation $n=a^2-\lambda b^2$ has a solution $(a,b)\in\mathbb{Q}$.
(c) If $v\equiv 3 \pmod 4$ then the equation $n=a^2+\lambda b^2$ has a solution $(a,b)\in\mathbb{Q}$.

Proof:

Remark: Often, (b) and (c) are combined into a single statement:

If v is odd, then the equation:
$n=a^2+(-1)^{\frac{v-1}{2}}\lambda b^2$ has a solution $(a,b)\in\mathbb{Q}$

(Both the proofs are completely different)

Proof:

(a) There exists a matrix $P\in M_{(v+1)\times(v+1)}(\mathbb{Q})$ such that

$$P^T\left(\begin{array}{c|c} I_v & 0 \\ \hline 0 & -\lambda \end{array}\right)P = \left(\begin{array}{c|c} nI_v & 0 \\ \hline 0 & -n\lambda \end{array}\right)$$

Taking determinants of both sides

$$\det(P^T)\det\left(\left(\begin{array}{c|c} I_v & 0 \\ \hline 0 & -\lambda \end{array}\right)\right)\det(P) = \det\left(\left(\begin{array}{c|c} nI_v & 0 \\ \hline 0 & -n\lambda \end{array}\right)\right).$$

$$\Rightarrow \det(P)^2\cdot(-\lambda) = n^v(-n\lambda).$$

$$\Rightarrow \det(P)^2\cdot n^v = n^{v+1}.$$ ← LHS is a square since v is even.

$$\frac{\det(P)^2}{n^v} = \left(\frac{\det(P)}{n^k}\right)^2$$ ← $v=2k$

Proof (cont.)

(b) $CV = I \pmod 4$

Starting with $\left(\begin{array}{c|c} I_V & 0 \\ \hline 0 & -\lambda \end{array}\right) \tilde{\sim} \left(\begin{array}{c|c} nI_V & 0 \\ \hline 0 & -n\lambda \end{array}\right)$

Using with Cancellation to cancel as many I_V and nI_V's pairs as possible! ($\frac{V-1}{4}$ such blocks)

This gives:

$$\begin{pmatrix} I & 0 \\ 0 & -\lambda \end{pmatrix} \tilde{\sim} \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix}$$

Therefore, $\exists$ invertible matrix $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Q})$ s.t.

$$\begin{pmatrix} a & b \\ b & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -\lambda \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} a^2 - \lambda b^2 & \square \\ \square & \square \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix}$$

(other entries don't matter)

$\Rightarrow a^2 - \lambda b^2 = n$ has a solution with $a, b \in \mathbb{Q}$.

(c) Since $\left(\begin{array}{c|c} I_V & 0 \\ \hline 0 & -\lambda \end{array}\right) \tilde{\sim} \left(\begin{array}{c|c} nI_V & 0 \\ \hline 0 & -n\lambda \end{array}\right)$, then

$$\left(\begin{array}{c|c} I_V & 0 \\ \hline 0 & \begin{matrix} -\lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & n \end{matrix} \end{array}\right) \tilde{\sim} \left(\begin{array}{c|c} nI_V & 0 \\ \hline 0 & \begin{matrix} -n\lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & n \end{matrix} \end{array}\right)$$

$(V+3)\times(V+3)$-matrix

$$\tilde{\sim} \left(\begin{array}{c|c} nI_{V+1} & 0 \\ \hline 0 & \begin{matrix} 1 & 0 \\ 0 & -\lambda n \end{matrix} \end{array}\right)$$

$$\left(\begin{array}{c|c} I_{V+1} & 0 \\ \hline 0 & \begin{matrix} n & 0 \\ 0 & -\lambda \end{matrix} \end{array}\right)$$

$\longleftrightarrow$ By reordering diagonal elements

$\hookrightarrow$

and $I_{v+1} \simeq nI_{v+1}$ since $v+1$ is a multiple of 4.

$$\Rightarrow \begin{pmatrix} n & 0 \\ 0 & -\lambda \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 \\ 0 & -\lambda n \end{pmatrix}$$

Therefore, $\exists$ an invertible matrix $\begin{pmatrix} p & r \\ q & s \end{pmatrix} \in M_{2\times2}(\mathbb{Q})$ s.t.

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -n\lambda \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & -\lambda \end{pmatrix}$$

$$\Rightarrow \left(\begin{array}{c|c} p^2-n\lambda q^2 & \\ \hline & \end{array}\right) = \left(\begin{array}{c|c} n & \\ \hline & \end{array}\right)$$

So $p^2 - n\lambda q^2 = n$.

Claim: $p \neq 0$, since in $p^2 - n\lambda q^2 = n$ ($\lambda, q^2 \geq 0$, so $-n\lambda q < 0$ AND $n > 0$, so $p \neq 0$)

(annotations: $n\lambda q^2$ +ve, $-n\lambda q^2$ −ve, n +ve)

Let $a = n/p$ and $b = nq/p$.

Then:

$$n = a^2 + \lambda b^2$$

$\square$

Example: Prove that there is no projective plane of order 6.

Recall:

Projective plane = symmetric $(v, k, 1)$-design.

And order 6 $\Rightarrow$ $k = 7$ and $v = \frac{k(k-1)}{\lambda} + 1 = 43$

So, we want to show that no $(43, 7, 1)$-design exists.

By BRC, if such a design exists then $a^2 + b^2 = 6$ has a solution $a, b \in \mathbb{Q}$ (since $43 \equiv 3 \pmod 4$). But, we've showed that $3 = a^2 + b^2$ has no solution for $a, b \in \mathbb{Q}$, and by same reasoning (Fermat's SOS thm), this equation also has no rational solutions. $\therefore$ Design does not exist

But the Fermat SOS Thm only helps if λ is a square. For other values of λ, we use Legendre's theorem.

Defn (Quadratic Residue)
If $GF(q)$ is a finite field, then

$$QR(q) = \{a^2 \mid a \in GF(q), a \neq 0\}$$

$a \in GF(q)^\times := a \in GF(q) \setminus \{0\}$.

$QR(q)$ is called the set of quadratic residues in $GF(q)$.

Example:
$q=5$, $GF(5) = \mathbb{Z}_5$, $QR(5) = \{1, 4\}$ ← considered modulo 5

Theorem (Legendre)
Suppose A, B, C are nonzero integers such that ABC is square-free (i.e. Not divisible by any perfect square other than 1).
Then TFAE:
(1) $Ax^2 + By^2 + Cz^2 = 0$ has a non-trivial integer solution $(x,y,z) \in \mathbb{Z}^3 \setminus \{0,0,0\}$.
(2) The following conditions hold:
  (i) A, B, C do not all have the same sign
  (ii) For every odd prime p:
    If $p \mid A$, then $-BC \in QR(q)$ and symmetrically for B and C.

Proof:

($\Leftarrow$) May discuss this direction later.

($\Rightarrow$) Suppose that $Ax^2+By^2+Cz^2=0$ have a non-trivial integer sol'n. Then:

(i) is clear,

For (ii), we may assume $\gcd(x,y,z)=1$ (If they have a common factor we can divide through by it).

Suppose $p \mid A$, then working modulo p, we have:

$$By^2+Cz^2 \equiv 0 \pmod{p}$$

Claim $p \nmid z$.

Proof: Suppose it does, then $By^2 \equiv 0 \pmod{p}$. and since ABC is squarefree, $p \nmid B$ (otherwise $p^2 \mid ABC$) $\Rightarrow y^2 \equiv 0 \pmod{p}$

$\Rightarrow p \mid y$.

Then, $\underbrace{Ax^2}_{\text{divisible by } p} + \underbrace{By^2 + Cz^2}_{\text{divisible by } p^2} = 0$,

So, Ax^2 must have an extra factor of p. A is squarefree so $p \nmid A$ and $\gcd(x,y,z)=1$, so $p \nmid x$.

$\therefore p^2 \nmid Ax^2$, which is impossible

So, $z \neq 0$ in $GF(p)$ and so it is invertible.

$\Rightarrow -BC \equiv (Byz^{-1})^2 \pmod{p}$

$\Rightarrow -BC \in QR(p)$.