Multiplier Theorem: ((G, +) Abelian group)
If $D \subseteq G$ is a (v,k,λ)-difference ~~set~~ set and p is a prime s.t. $p > \lambda$ and $p \mid n$ $(n = k - \lambda)$, then p is a multiplier for D.

We consider matrices whose rows and columns are indexed by elements of G.

Note that the points of the design associated to D are the elements of G.
The blocks $\mathcal{B} = \{g + D \mid g \in G\}$ are also indexed by elements of G.
$\therefore$ The incidence matrix is most naturally viewed as ~~a~~ a matrix with rows/cols indexed by G.

Notation and Facts:
For $g \in G$, let X^g be the matrix

$$(X^g)_{ab} = \begin{cases} 1 & \text{if } a-b = g \\ 0 & \text{o/w} \end{cases}$$

$(a, b \in G)$
This construction have the following properties:

- X^g is a permutation matrix.
  (Every row/col has exactly one 1)
- $(X^g)^{-1} = (X^g)^T$ (Since it is a permutation matrix)
  and further, $(X^g)^T = X^{-g}$ $(-g \in G)$

- If $g, h \in G$, then
  $X^g X^h = X^{g+h}$

Let $\mathbb{G} = \text{Span}\{X^g \mid g \in G\}$
- $\mathbb{G}$ is closed under multiplication

($\mathbb{G}$ is isomorphic to the group algebra of G)
- X^g are the only permutation matrices in $\mathbb{G}$

For $S \subseteq G$, write $X^S = \sum_{g \in S} X^g \in \mathbb{G}$

(Caution: $X^{-S} \neq (X^S)^{-1}$)

Take all the elements in S and negate them.

Instead, $X^{-S} = (X^S)^T$.

- $X^0 = I$
- $X^G = J$
- $X^D = N \Leftrightarrow$ Proof: ~~[illegible]~~ $(X^D)_{ab} = \sum_{\substack{g \in D \\ a-b=g}} 1 = \begin{cases} 1 & \text{if } a-b \in D \\ 0 & \text{o/w} \end{cases}$

  Incidence matrix

$a \in b+D \Leftrightarrow a-b \in D$

Proof (Multiplier Theorem)

p is a multiplier

$\Leftrightarrow pD = g + D$ for some $g \in G$

$\Leftrightarrow X^{pD} = X^{g+D} \left(= \sum_{h \in D} X^{g+h} = X^g \sum_{h \in D} X^h.\right)$

$\Leftrightarrow X^{pD} = X^g X^D$

$\Leftrightarrow X^{pD} X^{-D} = X^g \underbrace{X^D X^{-D}}_{= N \cdot N^T}$ (Since $X^{-D} = N^T$ is invertible)

$= nI + \lambda J.$

$\Leftrightarrow X^{pD} X^{-D} = X^g(nI + \lambda J)$

$X^g \lambda J = \lambda J$ since X^g is a permutation matrix

$\Leftrightarrow X^{pD} X^{-D} = nX^g + \lambda J.$ ← fo

$\boxed{\Leftrightarrow X^{pD} X^{-D} - \lambda J = nX^g}$ ← We want to prove this!

We will show that $\frac{1}{n}(X^{pD}X^{-D} - \lambda J)$ gives a permutation matrix (Since X^g is a permutation matrix)

Let $M = X^{pD} X^{-D} - \lambda J$.

We will show that if $p > \lambda$ and $p \mid n$, then:

① M has nonnegative entries, and ($\Rightarrow \frac{1}{n}M$ has ~~positive~~ nonnegative entries)

② $MM^T = n^2 I$ ($\Rightarrow \frac{1}{n}M$ is orthogonal).

Together, ① and ② $\Rightarrow \frac{1}{n}M$ is a permutation matrix.

and since $\frac{1}{n}M \in G$, it must be X^g for some $g \in G$.

Proof: (Con't)

Proof of ①:

Consider M modulo p.

Although it is not true that $X^{pD} = (X^D)^p$, it is true that $X^{pD} \equiv (X^D)^p \bmod p$.

Recall: that $(\sum x_i)^p \equiv \sum x_i^p \pmod p$

(Example:

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$$
$$\equiv x^5 + y^5 \pmod 5))$$

Here:

$$(X^D)^p = \left(\sum_{s\in D} X^s\right)^p$$
$$\equiv \sum_{s\in D} (X^s)^p \pmod p$$
$$\equiv \sum_{s\in D} \underbrace{X^s \cdots X^s}_{p \text{ times}} \pmod p$$
$$= \sum_{s\in D} X^{ps} = X^{pD}.$$

So,

$$M \equiv (X^D)^p X^{-D} - \lambda J \pmod p$$
$$\equiv (X^D)^{p-1} \underbrace{X^D X^{-D}}_{NN^T} - \lambda J \pmod p$$
$$\equiv (X^D)^{p-1} (\underbrace{nI}_{=0,\text{ since } p \mid n} + \lambda J) - \lambda J \pmod p$$
$$\equiv (X^D)^{p-1} \lambda J - \lambda J.$$

Proof: Con'td

$\equiv \lambda((X^D)^{p-1}J - J)$ (mod p)

$\hookrightarrow X^D J = \Delta N J = kJ = (n+\lambda)J$

$\equiv \lambda((n+\lambda)^{p-1}J - J)$ (mod p)

$\equiv \lambda(\underbrace{\lambda^{p-1}}_{\equiv 1 \text{ (By FLT)}} - 1)J$ (mod p)

$\equiv 0$ (mod p)

$\uparrow$ zero matrix.

So, every entry of M is divisible by p.

And also:

$M = \underbrace{X^{pD} X^{-D}}_{\text{has nonnegative entries}} - \lambda J$

All entries of M are $\geq -\lambda$.

Since $p > \lambda$, there are no negative ~~~~ multiples of p that are $\geq -\lambda$

$\therefore$ Every entry of M is ≥ 0.

Proof of ②:

Recall $v = 1 + \frac{k(k-1)}{\lambda} = 1 + \frac{(n+\lambda)(n+\lambda-1)}{\lambda}$

$\equiv 1 + \frac{\lambda(\lambda-1)}{\lambda}$ (mod p) $\quad$ λ invertible mod p since $p > \lambda$ and p prime.

$\equiv \lambda$ (mod p)

$\therefore \gcd(v, p) = 1$.

--

Proof: (Con't).

It follows that pD is a difference set

(key point! $\exists q \in \mathbb{Z}$ such $pq \equiv 1 \pmod v$ and $\Rightarrow$

$$pg_1 - pg_2 = x \text{ iff } g_1 - g_2 = qx$$

$\Rightarrow$ # of ways to write x as a difference in pD

$\Rightarrow$ # ——— " ——— qx as a difference in D)

$\therefore X^{pD}$ is the incidence matrix of a symmetric (v,k,λ)-BIBD.

Also, X^{-D} is the incidence matrix of a symmetric (v,k,λ)-BIBD

Exercise: If N_1, N_2 are the incidence matrices of 2 (possibly different) symmetric (v,k,λ)-designs, then $M = N_1 N_2 - \lambda J$ must satisfy $MM^T = n^2 I$.

(and so ② follows)

$$MM^T = (N_1N_2 - \lambda J)(N_1N_2 - \lambda J)^T$$
$$= (N_1N_2 - \lambda J)(N_1^TN_2^T - \lambda J)$$
$$= \ldots \text{ (crunch it out)}$$

☒

Open (?) Problem: We used that $p > \lambda$ to deduce $\gcd(v,p)=1$. Can we replace $p > \lambda$ by the weaker condition $\gcd(v,p)=1$. Clearly, the proof doesn't work, but there are no known counterexamples!