

Me and Anthony were talking about it and we came up with some conditions on the existence of non-degenerate (bilinear) semi-inner products (where a semi-inner product is defined as an inner product minus the condition of non-negativity because it makes no sense) in  $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$  for prime  $p$ .

Let  $V$  be a vector space over  $\mathbb{F}_p$  with  $n := \dim(V)$ .

Assume there exists semi-inner product  $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{F}$

We can still construct an orthonormal basis of the vector space  $\mathcal{L}$  without nonnegativity.

Then consider  $\langle x, x \rangle$  for  $x = \sum_{i=1}^n \alpha_i \mathcal{L}_i$

$$\begin{aligned} \langle x, x \rangle &= \sum_{i=1}^n \sum_{j=1}^n \alpha_i \alpha_j \langle \mathcal{L}_i, \mathcal{L}_j \rangle \\ &= \sum_{i=1}^n \alpha_i^2 \end{aligned}$$

Thus it's degenerate if (letting  $S$  be the set of quadratic residues in the field) there exists a list  $\mathcal{J} \subseteq S$  with  $|\mathcal{J}| \leq d$  and  $\sum_{i=1}^{|\mathcal{J}|} \mathcal{J}_i \equiv 0 \pmod{p}$ .

In any dimension greater than or equal to the modulus it is trivially degenerate, let all coefficients be the additive identity.

Additionally in  $\dim(V) = 1$  it is never degenerate, because this would mean  $\exists a \neq 0, a^2 = 0$ , which contradicts the existence of modular multiplicative inverses.

Using Lagrange's four square theorem we see that  $\forall p \in \mathbb{N}, \exists a, b, c, d \in \mathbb{N}$

$$p = a^2 + b^2 + c^2 + d^2$$

Thus,  $0 \equiv a^2 + b^2 + c^2 + d^2 \pmod{p}$ , and it's degenerate in  $\deg(V) \geq 4$

Thus we can only be nondegenerate if our dimension is less than or equal to 3, we now look at Legendre's three square theorem, which states that  $\neg \exists a, b \in \mathbb{N}, p = 4^a(8b + 7) \Leftrightarrow p = \exists x, y, z \in \mathbb{N}, x^2 + y^2 + z^2$ , this condition is equivalent by irreducibility of  $p$  to  $p \equiv 7 \pmod{8}$ , so if that is the case then it becomes degenerate in  $\dim(V) \geq 3$ .

In  $\dim(V) = 2$ , we have that they are degenerate if and only if the modulus is a pythagoren triple.

Its trivial to see that the latter implies the former.

We have by Fermat's theorem on sums of squares that the latter for a prime is equivalent to  $p \equiv 1 \pmod{4}$ .

Thus we only need to prove  $p \not\equiv 1 \pmod{4}$ , obviously the only possibility is  $p \equiv 3 \pmod{4}$ .

Consider, using Euler's criterion

$$a^{(p-1)/2} - (p-a)^{(p-1)/2}$$

This will be congruent to 0 if  $a$  and  $p-a$  are both quadratic residues, but we have that

$$(p-a)^{(p-1)/2} \equiv (-a)^{(p-1)/2} \equiv -a^{(p-1)/2}$$

Thus they cannot both be quadratic residues and it's nondegenerate.