WORKSHEET 3 for the session on 24th October 2025

Summary of the 10th October session and Plan for 24th October session:

So far we have discussed necessary conditions for existence of non trivial rational solutions of a homogeneous quadratic form in 3 variables (but the discussion can be easily extended to n variables). Such a rational solutions can put in one to one correspondence with integer solutions of a homogeneous equation which can then be diagonalised to get to a form $\Sigma a_i x_i^2 = 0$.

A. Obviously for a solution to exist we must have $\Sigma a_i x_i^2 = 0 \; mod \; n$ for all positive integer n. By Chinese Remainder Theorem it is necessary and sufficient to have $\Sigma a_i x_i^2 = 0 \; mod \; p^k$ for all integer k >0.
B. By Hensel's lemma shows, solutions to $\Sigma a_i x_i^2 = 0 \; mod \; p^k$ can be obtained by lifting the solution of $\Sigma a_i x_i^2 = 0 \; mod \; p$ provided that it is a simple zero. We have seen the lifting process in simple specific cases.
C. Therefore, the problem of finding non trivial solution to $\Sigma a_i x_i^2 = 0$ boils down to finding solutions to $\Sigma a_i x_i^2 = 0 \; mod \; p$. Even that is difficult to check for all primes. That is where Chevalley Warning theorem comes in to help. When $n > d$, the theorem says there are non trivial solutions for all good primes. Good primes are primes other than 2 and prime factors of the coefficients a_i.
D. Hasse-Minkowski theorem then says rational solutions exist for $\Sigma a_i x_i^2 = 0$. If (and only if) a real solution exists AND $\Sigma a_i x_i^2 = 0 \; mod \; p^k$ for all k >0. LOCAL TO GLOABAL PRINCIPLE: a local global solution exits if all local solutions exist. The principle is not universally true.
E. Today we will sketch how to prove the Chevalley Warning theorem. Doing that will introduce a few important techniques in number theory.
F. Then we will see reexamine Hasse Mikowski theorem for n=3 and d=2 and understand how it relates concretely to checking Legendre conditions
G. That will complete our discussion on rational solutions of quadratic forms of n variables. In the last remaining lecture, we will discuss some aspects of rational points on elliptic curves.

Problem 1A. (Many parts)

Goal of this problem is to explore and discover the proof of Chevalley Warning Theorem. The theorem says that $\Sigma a_i x_i^2 = 0 \; mod \; p$ has nontrivial solutions for every good prime p if $n > d$. Good primes are primes other than 2 and prime factors of the coefficients a_i.

Our strategy to prove this is to count the solutions of the equation $\Sigma a_i x_i^2 = 0 \; mod \; p$. In particular we area interested to check if the number of solutions is divisible by p. If it is then we are done. (Why?)

a.) Count the number of solutions for $X + Y + Z + W \equiv 0 \pmod 5$

b.) Count the number of solutions of $x^3 + y^3 + z^3 + w^3 \equiv 0 \pmod 5$.
Note that you can get the answer for b.) by making use of what you get in a.) and without any major recalculation. Why?

c.) Let's take a non-diagonal polynomial and check this again. Find he zeroes mod 5 of
$f(x, y, z, w) = xy^2 - z^3 + w^3$
This requires a careful counting.

d.) From the above results, it seems like the number of solutions are (0 mod 5) !!! We will sketch the proof of that without explicit counting using residue class of p=5, but the arguments will be very general. Also we will use the above quadratic function though again the discussion will be very general.

The FIRST STEP in counting zeroes by constructing a function P(x,y,z) that is 1 when f(x,y,z) =0 and P = 0 otherwise. THIS IS A STANDARD TECHNIQUE.

Show that the following P is such a function.

$$P(x, y, z, w) = 1 - f(x, y, z, w)^4$$

Note that for general solution for mod p, we will have $f(x,yz,w)^{p-1}$ in stead of $f(x,y,z,w)^4$.

Hint: Take a look at the following table:

Exponentiation Table Modulo 5

This table shows the values of a^i, where both 'a' and 'i' are in the set $\{0, 1, 2, 3, 4\}$. The calculation uses the condition $0^0 = 1$. The final row is the sum of the values in each column.

a\i	0	1	2	3	4
0	1	0	0	0	0
1	1	1	1	1	1
2	1	2	4	3	1
3	1	3	4	2	1
4	1	4	1	4	1
Sum	**5**	**10**	**10**	**10**	**4**

Problem 1e.) Therefore we can count the number of zeroes by summing P(x,y,z...) over all possible values of the argument. N below counts zeroes of the above function mod 5.

$$N = \sum_{\mathbb{F}_5^4} 1 - \sum_{\mathbb{F}_5^4} (xy^2 - z^3 + w^3)^4$$

Explain why it counts the number of zeroes.

The first term is obviously a multiple of 5 (or of p in general), What about the second term.

1f.) Show that the general expansion of the above will generate Factorizable monomials

$$M = C \cdot x^a y^b z^c w^d \quad , \quad \sum_{\mathbb{F}_5^4} (C \cdot x^a y^b z^c w^d) = C \cdot \left(\sum_{x \in \mathbb{F}_5} x^a \right) \left(\sum_{y \in \mathbb{F}_5} y^b \right) \left(\sum_{z \in \mathbb{F}_5} z^c \right) \left(\sum_{w \in \mathbb{F}_5} w^d \right)$$

Now show that at least one of the index, a,b,c,d MUST BE less than 5 (p-1 in the general case) and that factor is 0 mod5 (or 0 mod p) HINT: Take a look at the exponentiation table given above.

1g.) we already have a trivial zero. Since the number of zeroes is divisible by 5 (or by p) there must be other non trivial zeroes.

THAT COMPLETES OUR DISCUSSION on Chevalley Warning theorem.

Problem 2. There are many INTERLINKED parts to this problem. UNDERSTAND THESE and try proving as many parts as you can.

2.a.)

For 3 variables, the existence of solution rational solutions for $(ax^2 + by^2 + cz^2) = 0$ (with a, b, c, non-zero, square-free, pairwise coprime and (abc) square free), the following two statements are equivalent:

- **Statement A (Local Solvability):** The equation has a non-trivial solution in the real numbers $(ax^2 + by^2 + cz^2) = 0$ AND solutions of $(ax^2 + by^2 + cz^2) = 0 \mod p^k$ for every prime for every positive integer k.
- **Statement B (Legendre's Conditions):**
    1. a, b, c do not all have the same sign.
    2. (-bc) is a quadratic residue modulo a, i.e. that $t^2 = -(bc) \mod a$ for some t.
    3. (-ac) is a quadratic residue modulo |b|.
    4. (-ab) is a quadratic residue modulo |c|.

Prove one direction of the equivalence: A implies B (necessity).

2b.) Now show that the totality of Legendre conditions is sufficient to prove and construct non trivial solutions. Try to prove this result using the following hints.

i.) $(ax^2 + by^2 + cz^2)$ = (two factors linear in y and z mod a, and similarly for mod b and mod c.)

ii.) Using Chinese Remainder Theorem show that $(ax^2 + by^2 + cz^2)$ = (two factors linear in x, y, z) mod (abc).

iii.) Count the number of solutions in x, y and z satisfying

$$|x| < \sqrt{|bc|}$$
$$|y| < \sqrt{|ca|}$$
$$|z| < \sqrt{|ab|}$$

and show that it leads to non trivial solution for the $ax^2 + by^2 + cz^2 = 0$. THIS PART IS HARD. Try it and we will discuss in the class.

THIS COMPLETES OUR DISCUSSION ON existence and finding of non trivial rational solutions for quadratic equation in 3 variables.