12. Sums of squares via Geometry of Numbers (02 August 2019).

1. **Minkowski Convex Body Theorem.** *Let Λ be a lattice in $\mathbb{R}^n$ and $\Omega \subset \mathbb{R}^n$ be a bounded convex 0-symmetric set of volume* $\operatorname{vol}\Omega \geq 2^n \det\Lambda$. *Then* $\Omega \cap (\Lambda \setminus \{0\}) \neq \varnothing$.

2. **Two squares** (Fermat-Euler).

Theorem 1. *$n \in \mathbb{Z}_+$ can be written as a sum of two squares if and only if* $n \not\equiv 0 \pmod 4$ *and in its canonical representation $n = p_1^{\nu_1} \cdots p_t^{\nu_t}$ for all primes p_j of the form $p_j = 4k_j - 1$ one has* $\nu_j \equiv 0 \pmod 2$.

To give a geometrical proof of Theorem 1 we need the following.

a. For any $m \in \mathbb{Z}_+, a \in \mathbb{Z}$ the set

$$\Lambda(m,a) = \{(x,y) \in \mathbb{Z}^2 : \ x \equiv ay \pmod m\}$$

is a two-dimensional lattice. What is the determinant of this lattice?
b. There is a non-zero point of the lattice $\Lambda(m,a)$ in the circle $x^2 + y^2 < 2m$.
c. If $\exists\, z \in \mathbb{Z}$ such that $z^2 \equiv -1 \pmod m$ then m can be represented as $m = x^2 + y^2$.
d. There exists $z \in \mathbb{Z}$ such that $z^2 \equiv -1 \pmod m$ if and only if $m \not\equiv 0 \pmod 4$ and in the canonical representation $m = p_1^{\nu_1} \cdots p_t^{\nu_t}$ all primes p_j are of the form $p_j = 4k_j + 1$.

3. **Four squares** (Largange).

Theorem 2. *Every $n \in \mathbb{Z}_+$ can be represented as a sum of four squares.*

To give a geometrical proof of Theorem 2 we need the following.

a. For any prime p there exist x and y such that $x^2 + y^2 + 1 \equiv 0 \pmod p$.
b. There exist x and y such that $x^2 + y^2 + 1 \equiv 0 \pmod m$ if and only if $m \not\equiv 0 \pmod 4$.
c. Volume of four-dimensional unit ball is equal to $\frac{\pi^2}{2}$.
d. Let $m \in \mathbb{Z}_+, a, b \in \mathbb{Z}$. Then

$$\Lambda(m;a,b) = \left\{ (x_1,x_2,x_3,x_4) \in \mathbb{Z}^4 : \ \begin{cases} x_3 = ax_1 - bx_2 \pmod m \\ x_4 = bx_1 + ax_2 \pmod m \end{cases} \right\}$$

is a lattice which has a non-zero point in the ball $x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2m$.

4. **From Basic Number Theory**.

a. Euler's Criteria.

$x^2 \equiv a \pmod p$ is solvable $\iff$ $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

b. Chinese Remainder Theorem.

Let $m = m_1 \cdots m_t$ and $(m_i, m_j) = 1, i \neq j$. Then the solution of the system

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \dots \\ x \equiv b_t \pmod{m_t} \end{cases}$$

is a residue class $\mod m$.

b. Hensel's Lemma.

Let $f \in \mathbb{Z}[x]$ be a polynomial,
$f(x_1) \equiv 0 \pmod{p}$ and $f'(x_1) \not\equiv 0 \pmod{p}$.
Then for any $k \in \mathbb{Z}_+$ there exists unique $x_k \pmod{p^k}$ such that

1) $x_k \equiv x_1 \pmod{p}$;
2) $f(x_k) \equiv 0 \pmod{p^k}$.