Math 361 lecture for Friday, Week 10

Four squares theorem

Today, we will give some first application's of Minkowski's theorem.

Theorem 1 (Two squares theorem)**.** Let $p \in \mathbb{Z}$ be a prime number, and suppose that $p = 1 \bmod 4$. Then

$$p = x^2 + y^2$$

for some $x, y \in \mathbb{Z}$.

Exercise 2. Try some examples.

Proof of two square theorem.

Step 1. Pick $u \in \{1, \dots, p-1\}$ such that $u^2 = -1 \bmod p$. To see that this is always possible, consider $(\mathbb{Z}/p\mathbb{Z})^*$, the multiplicative group of non-zero elements of $\mathbb{Z}/p\mathbb{Z}$. By the structure theorem for finite abelian groups,

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1|n_2|\cdots|n_k$ and some $k \geq 0$. It follows that $a^{n_k} = 1$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^*$. (Note that we have an isomorphism between a multiplicative group and an additive group.) Thus, all $p-1$ elements of $(\mathbb{Z}/p\mathbb{Z})^*$ are roots of the polynomial $x^{n_k} - 1 \in K[x]$ where K is the field $\mathbb{Z}/p\mathbb{Z}$. Using the division algorithm, we know that $x^{n_k} - 1$ has at most n_k roots, and thus $n_k \geq p - 1$. In the other hand, we know $n_1 \cdots n_k = p - 1$, and so, $n_k \leq p - 1$. Therefore, $k = 1$, and $n_1 = p - 1$.

So far we have shown that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$ just based on the fact that p is prime. In our case, $p - 1 = 4k$ for some integer k. Let v be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, and define $u = v^k$. It follows that $u^4 = v^{4k} = v^{p-1} = 1 \bmod p$, and $u^2 \neq 1 \bmod p$ (since v has order 4). Since

$$u^4 - 1 = (u^2 - 1)(u^2 + 1) = 0 \bmod p,$$

it follows that $u^2 = -1 \bmod p$.

Step 2. Having fixed $u \in \{1, \dots, p-1\}$ such that $u^2 = -1 \bmod p$, define

$$L = \mathrm{Span}_{\mathbb{Z}}\{(0, p), (1, u)\} \subset \mathbb{Z}^2 \subset \mathbb{R}^2$$

Then L is a rank 2 lattice in $\mathbb{R}^2$, and the area of a fundamental domain F for L is

$$\left| \begin{pmatrix} 0 & 1 \\ p & u \end{pmatrix} \right| = p.$$

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\mathrm{vol}(X) = \pi r^2 = \frac{3}{2}\pi p > 4p = 2^2 \,\mathrm{vol}(F).$$

By Minkowski's theorem, there exists a nonzero lattice point $(x, y) \in L \cap X$. Since $(x, y) \in X$, we have

$$x^2 + y^2 \leq r^2 = \frac{3}{2}p < 2p.$$

We now show that $x^2 + y^2$ is divisible by p. Since $(x, y) \in L$, we have

$$(x, y) = a(0, p) + b(1, u) = (b, ap + bu)$$

for some $a, b \in \mathbb{Z}$. Since $u^2 = -1 \bmod p$, calculating modulo p, we have

$$x^2 + y^2 = b^2 + (ap + bu)^2 = b^2 + (bu)^2 = b^2 + b^2u^2 = b^2 - b^2 = 0 \bmod p.$$

So $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}_{>0}$. However, we have seen that $x^2 + y^2 < 2p$. It follows that $x^2 + y^2 = p$, as desired. □

Theorem 3 (Four squares theorem)**.** Every positive integer is the sum of four integer squares. In other words, if $n \in \mathbb{Z}$, then there exist $a, b, c, d \in \mathbb{Z}$ such that

$$n = a^2 + b^2 + c^2 + d^2.$$

Proof.

Step 1. It suffices to prove the result for primes p since

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = \\ (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 \\ + (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2\end{aligned}$$

for all $a, b, c, d, A, B, C, D \in \mathbb{Z}$.

Step 2. The result holds for $p = 2$ since $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

To see this, note that the elements of $\mathbb{Z}/p\mathbb{Z}$ may be written

$$0, \pm 1, \pm 2, \ldots, \pm(p - 1).$$

Further,

$$a^2 = b^2 \bmod p \quad \Rightarrow \quad (a + b)(a - b) \bmod p \quad \Rightarrow \quad a = \pm b \bmod p.$$

Since, $p \neq 2$, we have $a \neq -a \bmod p$. Therefore,

$$\begin{aligned}
|\{u^2 \bmod p : u \in \{0, 1, \ldots, p-1\}\}| &= |\{-1 - v^2 \bmod p : v \in \{0, 1, \ldots, p-1\}\}| \\
&= 1 + \frac{p-1}{2} = \frac{p+1}{2}.
\end{aligned}$$

The two sets above are not disjoint since

$$\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p.$$

So there exist $u, v \in \mathbb{Z}$ such that $u^2 = -1 - v^2 \bmod p$.

Step 4. Consider the rank 4 lattice

$$L = \operatorname{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

The volume of a fundamental domain for L is $|\mathbb{Z}^4/L| = p^2$. Apply Minkowski's theorem with X being a ball of radius $r = \sqrt{1.9p}$. Since X is a 4-dimensional ball,

$$\operatorname{vol}(X) = \frac{\pi^2 r^4}{2} > 2^4 p^2 = 2^4 \operatorname{vol}(F)$$

where F is a fundamental domain for L. Hence, by Minkowski's theorem, there exists a nonzero $\ell = (a, b, c, d) \in L \cap X$. Since $\ell \in X$,

$$a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p,$$

Since $\ell \in L$,

$$\begin{aligned}
(a, b, c, d) &= x(1, 0, u, -v) + y(0, 1, v, u) + z(0, 0, p, 0) + w(0, 0, 0, p) \\
&= (x, y, xu + yv + zp, -xv + yu + wp).
\end{aligned}$$

Working modulo p, we have

$$\begin{aligned}
a^2 + b^2 + c^2 + d^2 &= x^2 + y^2 + (xu + yv + zp)^2 + (-vx + yu + wp)^2 \\
&= x^2 + y^2 + (xu + yv)^2 + (-xv + uy)^2 \\
&= x^2 + y^2 + x^2u^2 + 2xyuv + y^2v^2 + x^2v^2 - 2xyuv + y^2u^2 \\
&= x^2 + y^2 + x^2u^2 + y^2v^2 + x^2v^2 + y^2u^2 \\
&= x^2 + y^2 + x^2(u^2 + v^2) + y^2(v^2 + u^2) \\
&= 0 \bmod p.
\end{aligned}$$

So $a^2 + b^2 + c^2 + d^2 = kp$ is a positive multiple of p that is less then $2p$. Therefore,

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

$\square$