Fermat's Christmas Theorem

Jay Zhao

I'm going to present what I think is a really cool proof of the following theorem:

☐ **Theorem 0.1**: An odd prime p can be expressed as:

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

with x, y integers if $p \equiv 1 \bmod 4$.

Example: $5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2.$

☐ **Lemma 0.2**: For every a where $p \nmid a$ there exists b such that $ab \equiv 1 \bmod p$.

Example: For $a = 2$ and $p = 5$ we may choose $b = 3$.

Proof by Bézout's theorem: Since a and p are coprime there exists integer n and M such that $an + pm = 1$ hence $an \equiv 1 \bmod p$. 😀 ∎

☐ **Lemma 0.3**: For all prime numbers p $(p-1)! \equiv -1 \bmod p$.

Example: $1 * 2 * 3 * 4 \equiv 1 \cdot (2 \cdot 3) \cdot (-1) \bmod 5$. Remember from the previous example that $2 * 3 \equiv 1 \bmod 5$. So $4! \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \bmod 5$.

Example:

$$\begin{aligned} & 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \\ \equiv\; & 1 \cdot (2 \cdot 7) \cdot (3 \cdot 9) \cdot (4 \cdot 10) \cdot (5 \cdot 8) \cdot (6 \cdot 11) \cdot (-1). \end{aligned}$$

Something fishy is going on, every pair of numbers I put in brackets multiplies to something $1 \bmod p$. We can pair everything up with something else and have those multiply to 1. Leaving $1 * 1 * \cdots \cdot 1 \cdot (-1)$. So $12! \equiv -1 \bmod 13$.

Proof by pairing: Every number from 1 to $p-1$ is coprime to p and hence pairs uniquely to some other number from 1 to $p-1$ to multiply to 1. Unique because $ab \equiv 1 \equiv ac$ implies $a(b-c) \equiv 0$ and hence $p \mid 0$ or $p \mid b-c$ neither of which can be true. The only two numbers which pair with themselves are x where $x^2 \equiv 1$ hence $(x-1)(x+1) \equiv 0$ and so $x \equiv \pm 1 \bmod p$. The rest is trivial, you can do it yourself. ∎

☐ **Lemma 0.4**: For a prime number $p \equiv 1 \bmod 4$, there exists n such that

$$n^2 \equiv 1 \bmod p$$

Proof: Let $p = 4k + 1$ and consider $n = 1 * 2 * \cdots * 2k$.

$$
\begin{aligned}
n^2 &\equiv 1 \cdot 2 \cdot \cdots \cdot 2k \cdot (-1)^{2k} \cdot (-2k) \cdot (-2k+1) \cdot \cdots \cdot (-1) \\
&\equiv (-1)^{2k} 1 \cdot 2 \cdot \cdots \cdot (2k)(2k+1) \cdot \cdots \cdot (4k-2) \cdot (4k-1) \\
&\equiv (-1)^{2k} (p-1)! \\
&\equiv (p-1)! \\
&\equiv -1
\end{aligned}
$$

∎

○ **Definition 0.1** (Lattice): A lattice of points generated by n linearly independent vectors $v_1, v_2, ..., v_n$ is the set of all points of the form

$$a_1 v_1 + a_2 v_2 + ... + a_n v_n$$

where $a_1, a_2, ..., a_n$ are integers.

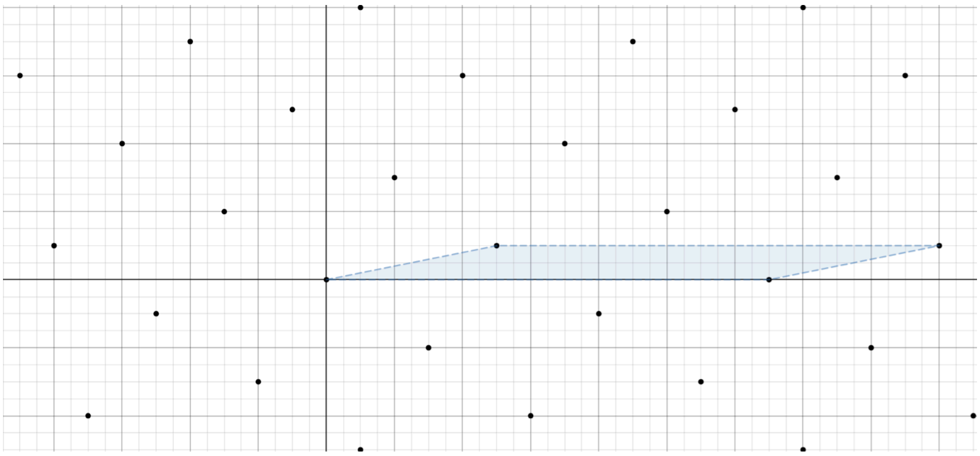
The parallelepiped spanned by the vectors $v_1, v_2, ..., v_n$ is called the **fundamental parallelepiped** of the lattice. That is the set of points of the form $r_1 v_1 + r_2 v_2 + \cdots + r_n v_n$ where $0 \leq r_i \leq 1$ for all i.

☐ **Theorem 0.5** (Minkowski's Theorem): If a convex set in $\mathbb{R}^n$ is symmetric about the origin and has volume 2^n times the volume of the fundamental parallelepiped of a lattice Λ in $\mathbb{R}^n$, then the set contains a non-zero point of the lattice Λ.

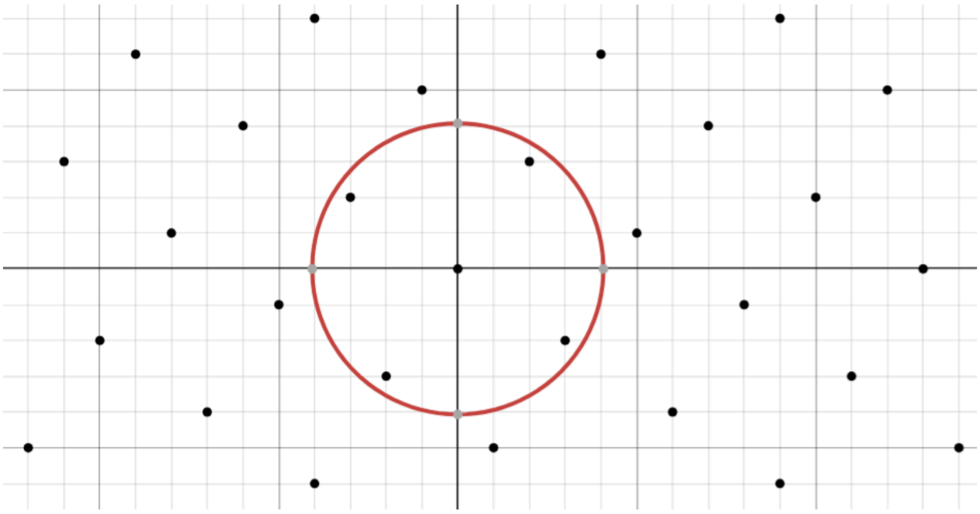
What this is really saying is that if you have a lattice of points in $\mathbb{R}^n$ and you blow a big enough balloon about the origin, you will eventually hit a lattice point.

More specifically in the case of $\mathbb{R}^2$, if you have a lattice of points generated by two vectors v_1 and v_2 and you draw a circle with area $4 * \text{area}(v_1, v_2)$ centered at the origin, then there must be a lattice point other than the origin inside that circle.

Proof of ☐ *Theorem 0.1*: Consider the lattice of points generated by the two vectors $\binom{n}{1}$ and $\binom{0}{p}$. The area of the parallelogram spanned by these two vectors is p. What's important is that every lattice point (x, y) is such that $x^2 + y^2 \equiv 0 \bmod p$.



Now draw a circle of radius $\sqrt{\frac{4p}{\pi}}$ centered at the origin. The area of this circle is $4p$ and so by Minkowski's theorem there must be a lattice point (x, y) inside this circle other than the origin.



$p \mid x^2 + y^2$ and $x^2 + y^2 < \frac{4p}{\pi} < 2p$. So $x^2 + y^2 = p$. So there must exists integers x and y such that $p = x^2 + y^2$.

∎