One can say that the root of number theory is to study solutions of polynomial equations over the integers. We will concentrate our discussion today to quadratic forms, i.e. of the form $f(x) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ (with $a_{ij} \in \mathbb{Z}$). A natural question one can ask is: what integers do $f(x)$ admit? Although we do not know the answer to this fully, we can still say quite a bit.

Classical example: Sum of squares We probably all know the results in this case.

- x^2 admits all square integers. In fact, there is quadratic reciprocity: let $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is not a quadratic residue mod } p \\ 0 & \text{else} \end{cases}$ be the Legendre symbol (which is completely multiplicative in the top). Then, for p, q primes, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

  Prove using Gauss sums, say.

- Fermat's 2-squares: x^2+y^2 admits all positive integers $n = p_1^{e_1} \cdots p_r^{e_r}$ such that, if e_i is odd, then necessarily $p_i \equiv 1 \pmod 4$.

  Prove using Gaussian integers, say

- Legendre's 3-squares: $x^2+y^2+z^2$ admits all positive integers not of form $4^a(8b+7)$.

- Fermat's 4-squares: $x^2+y^2+z^2+w^2$ admits all positive integers.

  see below.

⌜ This only tells us existence of solutions. There are, in fact, formulas that enumerates the number of integer solutions to $x_1^2 + \cdots + x_{2k}^2 = m$ for low k, and for higher k we can get asymptotes via the theory of modular forms (using Hecke's estimate that Eisenstein series's coefficients grows much faster than cusp form coefficients). ⌟

For the purpose of explaining our main theorem later, let us review how to prove the

3-squares and 4-squares results.

The p-adic numbers A famous theorem of Ostrowski tells us that all valuations, or absolute value, of $\mathbb{Q}$ are:

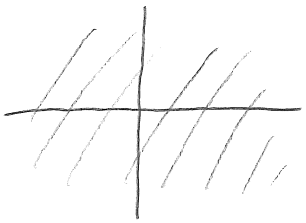
- the usual norm $|\ |_\infty$, (also called archimedean)
- the p-adic norm $|\ |_p$ for primes p, defined by $|p^k \frac{m}{n}|_p = p^{-k}$ if $p \nmid m$ and $p \nmid n$. (also called nonarchimedean)

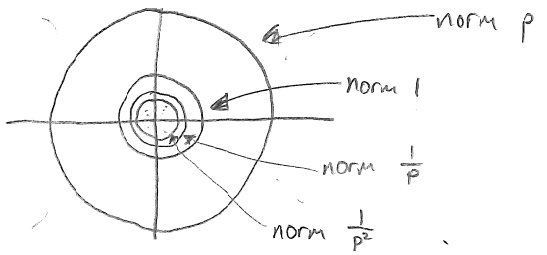
A first course in analysis tells us $\mathbb{Q}$ completed with respect to $|\ |_\infty$ is $\mathbb{Q}_\infty = \mathbb{R}$. A moments' thought tells us $\mathbb{Q}$ completed with respect to $|\ |_p$ is

$$\mathbb{Q}_p = \left\{ \text{Laurent series } \sum_{n=k}^{\infty} a_n p^n \text{ with } k \in \mathbb{Z} \text{ and } 0 \le a_n < p-1 \right\}$$

with addition and multiplication base p. Clearly $\mathbb{Q}_p$ has valuation $|\sum_{n=k}^{\infty} a_n p^n| = p^{-k}$ extended from $|\ |_p$ on $\mathbb{Q}$, and it satisfies the basic properties that $|n|_p \le 1$ for $n \in \mathbb{Z}$, and $|\alpha+\beta|_p \le \max\{|\alpha|_p, |\beta|_p\}$, with $|\alpha+\beta|_p = |\beta|_p$ if $|\alpha|_p < |\beta|_p$ and $|\alpha+\beta|_p < |\beta|_p$ implies $|\alpha|_p = |\beta|_p$. We call $\mathbb{Q}_p$, $p \neq \infty$, the p-adic numbers

Notice a fundamental difference when "visualizing" $\mathbb{Q}_p$ versus $\mathbb{R}$:

$\mathbb{R}$: 

$\mathbb{Q}_p$: 

We call $\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \le 1\} = \left\{ \sum_{n=k}^{\infty} a_n p^n \text{ with } k \in \mathbb{Z}_{\ge 0} \text{ and } 0 \le a_n < p-1 \right\}$ the ring of integers. It is a local ring with maximal ideal $p\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p < 1\}$, and clearly $\mathbb{Z}_p / p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. (Certainly the definition implies $\mathbb{Z}_p \subset \mathbb{Q}_p$ is the completion of $\mathbb{Z}$ at p.)

The most important tool in p-adic numbers, more generally valuation theory, is

Hensel's Lemma: Let R be a DVR with $K = \mathrm{Frac}(R)$ complete in its valuation. Let $g(x) \in R[x]$ be a monic polynomial such that $\bar{g}(x) \in R[x]$ admits a simple root $\alpha_0 \in R/m$ (so $\bar{g}'(\alpha_0) \neq 0$). Then there is a unique $\alpha \in R$ that is a lifting of α_0 and satisfies $g(\alpha) = 0$.

[Assumptions are essential. For example x^3+x+1 has no roots in $\mathbb{Q}$, but has a root 1 in $\mathbb{Z}/3\mathbb{Z}$.]

An important example: Over $\mathbb{Z}_2$, the polynomial x^2 admits all 2-adic integers that are, in base 10, of the form $4^a(8b+1)$. To see this, note that x^2+x-2b admits simple roots over $\mathbb{Z}/2\mathbb{Z}$, so by Hensel's Lemma $\alpha^2+\alpha-2b=0$ for some $\alpha \in \mathbb{Z}_2$. Thus $(2^a)^2(2\alpha+1)^2 = 4^a(8b+1)$. This is important for the 3-squares result.

Hasse's Principles Let us come back to an integral quadratic form $f(x) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$. We can associate to f the matrix $M_f = \begin{bmatrix} a_{11} & & \frac{a_{ij}}{2} \\ & \ddots & \\ \frac{a_{ij}}{2} & & a_{nn} \end{bmatrix}$, so that $f(x) = x^t M_f x$.

We will work in case f is classically integral, i.e. $a_{ii} \in \mathbb{Z}$ and $a_{ij} \in 2\mathbb{Z}$, so that $M_f \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$. All of what we say will work for general f by considering $2f$ instead.

We say that two quadratic forms f, g are equivalent if $B^t M_f B = M_g$ for some integer $n \times n$ matrix B. This can be interpreted more geometrically as we see later.

A weaker equivalence we need is the following. Two quadratic forms f, g are in the same genus if, for every $p \in \{\text{primes}, \infty\}$, there is a matrix $B_p \in \mathrm{Mat}_{n\times n}(\mathbb{Z}_p)$ such

that $B_p^t M_f B_p = M_g$ (here $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$).

⌜Equivalent quadratic forms are in the same genus, but the converse is false. A counterexample is x^2+82y^2 and $2x^2+41y^2$. Use the fact that, if $u_1,..,u_n \in \mathbb{Z}_p^*$, $p \neq \infty$, then $u_1x_1^2+\dots+u_nx_n^2$ is $\mathbb{Z}$-equivalent to $x_1^2+\dots+x_{n-1}^2+(u_1\cdots u_n)x_n^2$.⌟

Hasse's "Local-Global" principle, in its useful form, holds in case of unique genus.

Hasse's Principle: Let f be a classically integral quadratic form in n variables, which is unique in its genus and $d := \det M_f \neq 0$. Suppose $a \in \mathbb{Z}\setminus\{0\}$ is an integer represented by f over $\mathbb{R}$, and (primitively) represented by f over $\mathbb{Z}_p$ for all p (in fact, if $p \mid 2d$ for $n \geq 3$, and $p \mid 2ad$ for $n=2$). Then a is (primitively) represented by f over $\mathbb{Z}$. [In general, if genus is not unique, then a is represented by f^* over $\mathbb{Z}$, where f^* is in the genus of f.]

⌜There is a general algorithm that computes the genus of a quadratic form; see the habilitation thesis of Markus Kirschmer (Algorithm 5.4.11) for instance.⌟

With this, we can sketch the proof of Legendre's 3-squares theorem. By Hasse's principle it suffices to consider over $\mathbb{R}$ and $\mathbb{Z}_2$. The case for $\mathbb{R}$ is trivial, and the case for $\mathbb{Z}_2$ is by case checking using fact that x^2 admits $4^a(8b+1)$ over $\mathbb{Z}_2$.

Fermat's 4-squares theorem follows immediately, for we just need to consider $4^a(8b+7)$ case, but $4^a(8b+7) = (2^a)^2 +$ (sum of 3-squares equalling $4^a(8b+6)$).

Classical example: Forms over $\mathbb{F}_p$ and $\mathbb{Q}$ This is a short discussion of the well-known criteria that determines if a quadratic form over $\mathbb{F}_p$ or $\mathbb{Q}$ admits all elements in its field.

Simple Fact: The form $a_1x_1^2 + a_2x_2^2$, $a_i \in \mathbb{F}_{p^k} \setminus \{0\}$, admits all elements in $\mathbb{F}_{p^k}$.

↳ Let $b \in \mathbb{F}_{p^k}$. Then both $a_1x_1^2$ and $b - a_2x_2^2$ admits $\frac{p^k+1}{2}$ different values.

Another Hasse Principle. Let f be a nondegenerate quadratic form over $\mathbb{Q}$ (or number field).

- If $f(x) = 0$ for some $x \in \mathbb{Q}^n \setminus \{0\}$, then f represents all elements in $\mathbb{Q}$.
- If $f(x_p) = 0$ for some $x \in \mathbb{Q}_p^n \setminus \{0\}$ and each p (including $p = \infty$), then $f(x) = 0$ for some $x \in \mathbb{Q}^n \setminus \{0\}$.

[In fact, as $\mathbb{Q}$ is a field, by a change of variables we can always assume f is diagonal, i.e. of the form $\sum_{i=1}^{n} a_i x_i$. The first part is easy too by $f(tx+y) = t^2 f(x) + f(y) + t B_{x,y}$.]

Quadratic Forms over $\mathbb{Z}$ So far we have been discussing very classical results. Here is a surprising recent result (that is proven using very classical methods!!).

15-theorem: If a classically integral positive definite quadratic form represents $1, 2, 3, 5, 6, 7, 10, 14, 15$, then it represents every positive integer. Further,

- if t is any one of the nine numbers above, then there is a (quaternary diagonal) form that represents <u>every</u> positive integer <u>but</u> t.
- There are exactly 204 quaternary forms with above assumptions that satisfies the 15 theorem (up to equivalence).

[History: John Conway thought this might be true after giving a class, and "proved" this theorem with William Schneeberger without a written proof. Manjul Bhargava then wrote down an independent proof that is available since 2000.] → Want to mention Margaret Willerding?

290-theorem: If an integral positive definite quadratic form represents

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37,$$
$$42, 58, 93, 110, 145, 203, 290,$$

then it represents every positive integer. Further:

- if t is any one of the twenty-nine numbers above, then there is a form that represents every positive integer but t.
- there are exactly 6436 quaternary forms with above assumptions that satisfies the 290 theorem (up to equivalence).

[History: John Conway conjectured this with some of his students after computational evidence. Manjul Bhargava and Jonathan Hanke claimed to have proven it in 2005, but only the written up proof was available last year 2016.]

The rest of the talk sketch the ideas that goes into this amazing result. We focus on the 15-theorem, commenting on the 290-theorem whenever appropriate.

The first thing to do is to reinterpret f, a classically integral positive definite quadratic form for the remainder of the talk (unless said otherwise), as <u>lattices</u>. We have

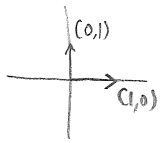
$$\left\{\begin{array}{l}\text{classically integral positive definite}\\ \text{quadratic form with } n\text{-variables}\end{array}\right\}/_{\text{equiv.}} \longleftrightarrow \left\{\begin{array}{l}\text{lattices in } \mathbb{R}^n \text{ having}\\ \text{integral inner products}\end{array}\right\}/_{\text{isom.}}$$

[For 290-theorem, use similar, except remove "classical" in left hand side, and change "inner product" to "norm with inner product in $\frac{1}{2}\mathbb{Z}$" in right hand side.]

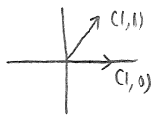
The correspondence is the obvious one:

$$\sum_{1\le i\le j\le n} a_{ij} x_i x_j \longleftrightarrow \mathbb{Z}\text{-basis } x_1, \dots x_n \text{ such that}$$
$$x_i \cdot x_i = \|x_i\|^2 = a_{ii}$$
$$x_i \cdot x_j = \frac{a_{ij}}{2} \qquad (i \neq j).$$

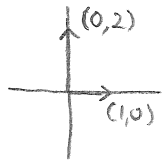
For example.

x^2+y^2 $\begin{bmatrix}1&0\\0&1\end{bmatrix}$ $\longleftrightarrow$ 

using $\begin{bmatrix}1&0\\1&1\end{bmatrix}$ $\lbrace\lbrace$ equivalent to

$x^2+2xy+2y^2$ $\begin{bmatrix}1&1\\1&2\end{bmatrix}$ $\longleftrightarrow$ 

$\lbrace\lbrace$ isometric to

x^2+2y^2 $\begin{bmatrix}1&0\\0&2\end{bmatrix}$ $\longleftrightarrow$ 

A form f is <u>universal</u> if it represent every positive integer. If f is not universal, define its <u>traunt</u> to be the smallest positive integer not represented by f.

The <u>most important idea</u> in the proof of the 15 and 290 theorems is

Escalation. An <u>escalation</u> of a nonuniversal lattice ($\leftrightarrow$ quadratic form) L is any lattice generated by L and a vector with norm equals to the traunt of L.

An <u>escalator lattice</u> is a lattice obtained by escalations from the 0-dimensional lattice.

We now consider escalations for the 15-theorem, and comment on 290-theorem after.

<u>1-dimensional escalation</u>. This is clearly just x^2 (or $[1]$), of traunt 2.

<u>2-dimensional escalation</u>. We must have $\begin{bmatrix}1&a\\a&2\end{bmatrix}$ for some $a\in\mathbb{Z}$. By the Cauchy-Schwarz inequality, necessarily $a^2\leq 2$, so $a\in\{0,1,-1\}$. Up to isometry we only have $\begin{bmatrix}1&0\\0&2\end{bmatrix}$ and $\begin{bmatrix}1&0\\0&1\end{bmatrix}$ $\left(\overset{\text{isom.}}{\underset{\text{to}}{\approx}} \begin{bmatrix}1&1\\1&2\end{bmatrix} \text{ and } \begin{bmatrix}1&-1\\-1&2\end{bmatrix}\right)$.

<u>3-dimensional escalation</u>. By Cauchy-Schwarz and considering isometries, we have 9 of them:

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}, \begin{bmatrix}1&0&0\\0&1&0\\0&0&2\end{bmatrix}, \begin{bmatrix}1&0&0\\0&1&0\\0&0&3\end{bmatrix}, \begin{bmatrix}1&0&0\\0&2&0\\0&0&2\end{bmatrix}, \begin{bmatrix}1&0&0\\0&2&0\\0&0&3\end{bmatrix}, \begin{bmatrix}1&0&0\\0&2&1\\0&1&4\end{bmatrix}, \begin{bmatrix}1&0&0\\0&2&0\\0&0&4\end{bmatrix},$$

$$\begin{bmatrix}1&0&0\\0&2&1\\0&1&5\end{bmatrix}, \begin{bmatrix}1&0&0\\0&2&0\\0&0&5\end{bmatrix}.$$

4-dimensional escalation: We now have 207 of them. However, on the list one will find out that a lot of them (201 in fact) are universal, such as $x_1^2+x_2^2+x_3^2+x_4^2$! We would like to say why this is the case. Say L_4 is such a 4-dimensional escalation, that comes from a 3-dimensional lattice L_3. We write $L_3^{\perp}=[m]$, so $L_3 \oplus [m] \subset L_4$. If L_3 is unique in genus, show L_4 will represent all sufficiently large integers, and then one can check for the small integers manually.

For example, consider escalations of $L_3 = x^2+2y^2+2z^2$ $\left(\leftrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}\right)$. This is unique in genus, and by Hasse's principle represents all integers $\neq 4^a(8b+7)$.

- Say $L_4 (\supset L_3 \oplus [m])$ is not universal, with traunt u. Then u is not represented by L_3, so $u \neq 4^a(8b+7)$. Minimality implies $a=0$.
- If $m \equiv 1,2,4,5,6 \pmod 8$, then $u-m \neq 4^{a'}(8b'+7)$.
- If $m \equiv 3,7 \pmod 8$, then $4m \equiv 4 \pmod 8$, so $u-4m \neq 4^{a'}(8b'+7)$
- Thus for $m \not\equiv 0 \pmod 8$, if L_4 is not universal we require $u < 4m$.

Here we explicitly calculate $m \leq 28$, and for $m \not\equiv 0 \pmod 8$ every escalation of L_3 represents positive integers up to 112. Hence all such escalations are universal in this case.

- If $m \equiv 0 \pmod 8$, the only two possible ones are

$$\begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 2 & 1 & 1 & 7 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 7 \end{bmatrix}.$$

Apply same argument after changing L_3 to $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 3 \end{bmatrix}$ and $\begin{bmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 7 \end{bmatrix}$, still unique genus!

This kind of argument works for all but one of the 3-dimensional escalator as they are unique in genus. The exception is

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{bmatrix}.$$

In this case we simply find genus of sublattices in this lattice to find what integers this lattice does not possibly represent, and use the same yoga.

5-dimensional escalators: They must come from the following 6 4-dimensional ones:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 4 \end{bmatrix} \text{ traunt } 10, \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 4 & 1 \\ 0 & 0 & 1 & 5 \end{bmatrix} \text{ traunt } 10,$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 1 & 5 \end{bmatrix} \text{ traunt } 15, \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix} \text{ traunt } 15,$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 5 & 2 \\ 0 & 1 & 2 & 8 \end{bmatrix} \text{ traunt } 15, \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 5 & 1 \\ 0 & 1 & 1 & 9 \end{bmatrix} \text{ traunt } 15.$$

Use the same technique as in the other 4-dimensional on these to see that, actually, the traunt is the unique number they don't represent. So in fact, all 5-dimensional escalators are universal!

This immediately proves the 15-theorem, for the numbers 1,2,3,5,6,7,10,14,15 are the only possible traunts of escalator lattices! (Obviously every universal lattice must contain a sequence of escalator sublattices, in fact of length at most six including the zero-dimensional lattice.)

What difficulties arise in proving the 290-theorem? The main problem is that there

are a lot more 4-dimensional escalators to consider (millions instead of just < 2000), and for a lot of these there is not a good, if any, choice of a unique genus sublattice to use. By computational techniques described in their paper, one gets three types of escalations of 4-dimensions:

- I: universal
- II: misses at most 3 positive integers

} all but 5 escalators

- III: (some technical conditions plus) represents all positive integers $\neq 4^a(16k+14)$.
  - ↳ all of these 5 escalators have traunt 14 and arises from a 3-dimensional escalator of traunt 10. (Specifically, $L_3 = \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1 \\ 1/2 & 1 & 5 \end{bmatrix}$). Remarkably all 5-dimensional escalators arising from those of type III are achieved if we escalate L_3 by 14 first, and then 10. By escalating L_3 by 14, one finds they are either of type I, type II, or the following type
- IV: represents all integers but perhaps those of form $10n^2$ or $13n^2$.

Hence, in the 290-theorem case, escalators have dimensions at most 7, with all possible traunts the twenty-nine listed in the theorem.

Final thoughts In some sense the 15 and 290 theorems can be thought of as another attempt to understand the many curious number theoretical assertions of Srinivasa Ramanujan, for he actually listed the 54 universal quaternary diagonal integral quadratic forms up to isometry (thought he unfortunately wrote down $x^2+2y^2+5z^2+5w^2$ as well, which does not represent 15).

References :

(1) Manjul Bhargava, "On the Conway-Schneeberger Fifteen Theorem".

(2) Manjul Bhargava and Jonathan Hanke, "Universal Quadratic Forms and the 290 Theorem".

(3) John William Scott Cassels, "Rational Quadratic Forms".

(4) Markus Kirschmer, "Definite Quadratic and Hermitian Forms with Small Class Number".

Supplement to Pizza Seminar 2017-04-07

Proving Fermat's 2-square theorem

We first prove the version for prime numbers.

Thm*: A prime number p can be expressed as $p = x^2+y^2$, $x, y \in \mathbb{Z}$, iff

$$p = 2 \quad \text{or} \quad p \equiv 1 \pmod 4.$$

Proof. The case $p=2$ is clear, so assume p is odd. If $p = x^2+y^2$, then obviously $p \equiv 1 \pmod 4$. So let us assume $p \equiv 1 \pmod 4$. Recall $\mathbb{Z}[i]$ is an Euclidean domain (for $x, y \in \mathbb{Z}[i]$, need to choose $q, r \in \mathbb{Z}[i]$ so that $x = qy + r$. Simply choose q closest to $\frac{x}{y}$ (so $\left|\frac{x}{y} - q\right| \le \frac{\sqrt{2}}{2} < 1$) and so $r = y\left(\frac{x}{y} - q\right)$ with $|r| < |y|$). Hence $\mathbb{Z}[i]$ is a PID and UFD. Thus:

- $p = x^2+y^2 \Rightarrow p = (x+iy)(x-iy)$ in $\mathbb{Z}[i]$ is factorizable,
- If $p = \alpha\beta$ is a nontrivial factorization, then $p^2 = N(\alpha)N(\beta)$ so that $N(\alpha) = N(\beta) = p$, hence $p = N(\alpha) = N(\alpha_1 + i\alpha_2) = \alpha_1^2 + \alpha_2^2$.

Suppose p cannot be expressed as sum of two squares. Then p is a prime in $\mathbb{Z}[i]$, so that $p \cdot \mathbb{Z}[i]$ is a maximal ideal in $\mathbb{Z}[i]$, and $\mathbb{Z}[i]/(p)$ is a field. Recall Euler's Criterion: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. As $p \equiv 1 \pmod 4$, $\left(\frac{-1}{p}\right) = 1$, so there is an element $\gamma \in \mathbb{Z}$ such that $\gamma^2 \equiv -1 \pmod p$. But this means $\pm i, \pm\gamma$ are solutions to x^2+1 in $\mathbb{Z}[i]/(p)$, a contradiction to the factor theorem.

Using this we can easily prove the general Fermat's Two Square Theorem

2-square Theorem. x^2+y^2 admits all positive integers $n = p_r^{e_1} \cdots p_r^{e_r}$ such that, if e_i is odd, then necessarily $p_i \equiv 1 \pmod 4$.

Lemma 1: If p divides n with $p \equiv 3 \pmod 4$, then n has no primitive representation (i.e. if $n = x^2+y^2$, then $\gcd(x,y) > 1$ necessarily).

Proof. Suppose $n = x^2+y^2$ is a primitive representation. Then $p \nmid x$ and $p \nmid y$ with $x^2+y^2 \equiv 0 \pmod p$. Thus y is invertible in $\mathbb{Z}/p\mathbb{Z}$, and $\left(\frac{x}{y}\right)^2 \equiv -1 \pmod p$, and $\left(\frac{-1}{p}\right) = 1$. However, Euler's criterion gives $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4m+3-1}{2}} = -1$. ∎

Lemma 2 (Brahmagupta-Fibonacci Identity) For integers a,b,c,d,

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= (ac-bd)^2 + (ad+bc)^2 \\ &= (ac+bd)^2 + (ad-bc)^2.\end{aligned}$$ ∎

Proof of 2-square theorem. Suppose $p^r \| n$ with r odd, and $n = x^2+y^2$. Then, letting $d = \gcd(x,y)$, we have $\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{n}{d^2}$ a primitive representation of $\frac{n}{d^2}$ with p dividing n, a contradiction to Lemma 1.

Suppose the condition of n in 2-squares theorem. Without loss of generality we can assume $n = p_1 \cdots p_r$ with $p_j \equiv 1 \pmod 4$ for all j. Then just apply Thm* and Lemma 2. ∎