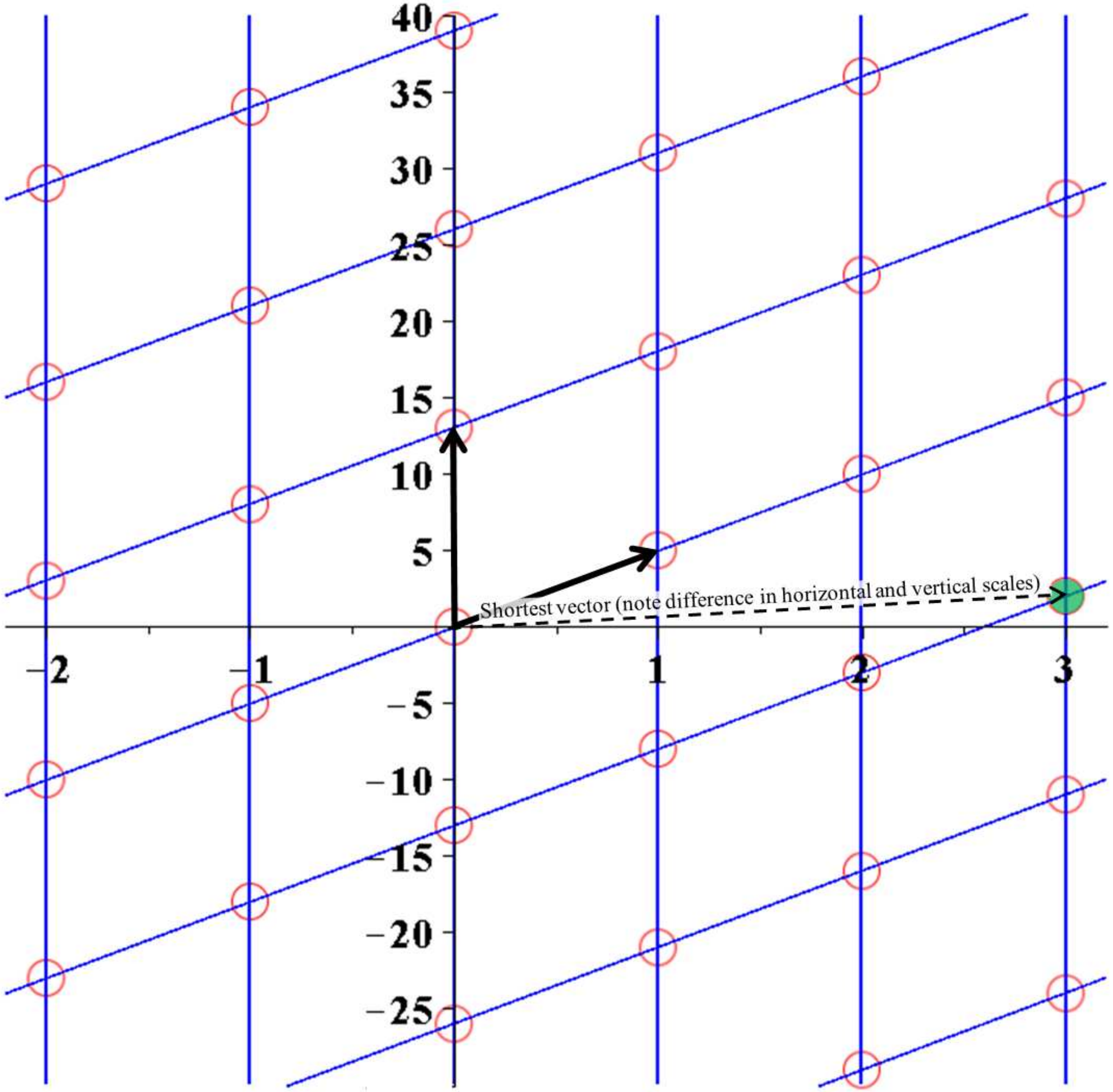
THEOREM OF THE DAY

Fermat's Two-Squares Theorem *An odd prime number p may be expressed as a sum of two squares if and only if $p \equiv 1 \pmod 4$.*



Lagrange's Lemma: *-1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$.* E.g. $r^2 \equiv -1 \pmod{13}$ is solved by $r = \pm 5$, since $(\pm 5)^2 = -1 + 2 \times 13$. But $r^2 \equiv -1 \pmod{11}$ has no solutions. This confirms almost directly that primes of the form $4n+3$ cannot be written as a sum of two squares. For if $p = a^2 + b^2$ then p can divide neither a nor b, otherwise it will divide both (if it divides a then it must also divide b^2 and hence b) implying that p^2 divides $a^2 + b^2 = p$ which is impossible. Then $\gcd(a, p) = 1$ and consequently $aa' \equiv 1 \pmod p$ for some a'. Multiplying $a^2 + b^2 - p = 0$ by $(a')^2$ gives $(aa')^2 + (ba')^2 - p\,(a')^2 = 0 \equiv 1 + (ba')^2 - 0 \pmod p$: we discover that -1 is a quadratic residue mod p and Lagrange's Lemma says that p has remainder 1 mod 4.

So the 'only if' part of the theorem is established. Now we must produce a two-squares representation when $p = 5, 13, 17, 29, 37, \ldots$. The theory of integer lattices supplies a beautiful general purpose construction. Use Lagrange's Lemma again to take a positive integer r satisfying $r^2 \equiv -1 \pmod p$, and define the integer lattice

$$\left\{ Bx,\ B = \begin{pmatrix} 1 & 0 \\ r & p \end{pmatrix} \middle|\ x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

On the left this lattice is depicted for $p = 13$, with $r = 5$: it consists of all integer points in two dimensions which are integer-weighted sums of the two basis vectors $(1, 5)$ and $(0, 13)$. A corollary of Minkowski's Convex Body Theorem says that there is some vector in this lattice whose Euclidean length is strictly less than $\sqrt{2\det(B)}$. In our construction this gives

$$|Bx| = \sqrt{x_1^2 + (rx_1 + px_2)^2} < \sqrt{2\det(B)} = \sqrt{2p}.$$

Squaring, expanding out and factorising:

$$x_1^2 + (rx_1 + px_2)^2 = (px_2^2 + 2rx_1x_2)p + x_1^2(r^2 + 1) < 2p.$$

Now $r^2 + 1 \equiv 0 \pmod p$ by our choice of r, so $(px_2^2 + 2rx_1x_2)p + x_1^2(r^2+1)$ is a nonzero multiple of p which is less than $2p$, and therefore is exactly p. Thus if $a = x_1$ and $b = rx_1 + px_2$ then $a^2 + b^2 = p$. In our illustration, left, $x_1 = 3$, $x_2 = -1$ and $a^2 = 9$, $b^2 = (5 \times 3 - 1 \times 13)^2 = 4$, with $a^2 + b^2 = 13$.

This theorem was discovered by Fermat in 1640 and by Albert Girard in 1632, the year of his death. The first published proof is due to Euler in 1754; that given here is an example of Hermann Minkowski's 'Geometry of Numbers', developed in the 1890s.

Web link: cseweb.ucsd.edu/classes/wi10/cse206a/lec1.pdf; Don Zagier's famous 'one-sentence' proof: math.berkeley.edu/~mcivor/math115su12/schedule.html, Lec. 6.

Further reading: *From Fermat to Minkowski: Lectures on the Theory of Numbers and its Historical Development* by Winfried Scharlau and Hans Opolka, Springer, 2010.