Fermat's equations and Fermat's last theorem:

We call the family of Diophantine equations

$$X^n + Y^n = Z^n \qquad (n \geq 2)$$

(n = 1 is really easy.)

Fermat's equations.

Theorem (Pythagorean triples)

For $n = 2$, a triple $(x,y,z) \in \mathbb{Z}^3$ is a non-trivial (e.g. (1,0,1)) primitive solution to Fermat's equation (i.e. a primitive Pythagorean triple) iff there are $u, v \in \mathbb{Z}$ coprime s.t. $u + v \equiv 1 \bmod 2$ and

$$(x,y,z) = \pm(u^2 - v^2, -2uv, u^2 + v^2).$$

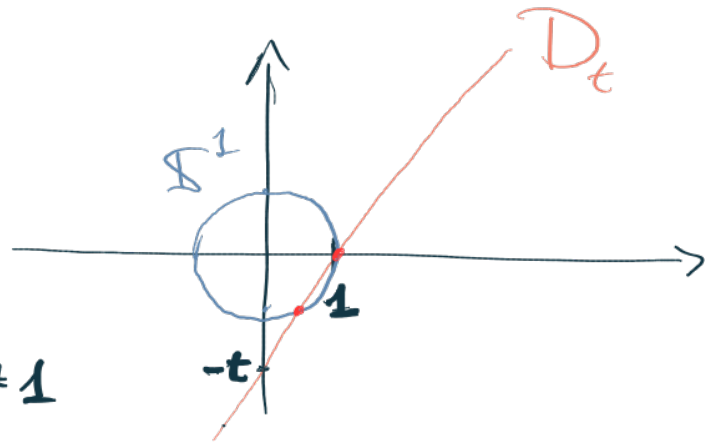
In particular, there are infinitely many primitive solutions.

Proof: We first show a procedure to construct a solution.

(i) Let $t \in \mathbb{Q}$ and let $u, v \in \mathbb{Z}$ s.t. $t = \frac{u}{v}$ is reduced.

Let $D_t = \{(A,B) \in \mathbb{R}^2 : B = tA - t\}$

$= \{B = t(A-1)\}$



(ii) Note that $D_t \cap \mathbb{S}^1 = \{(1,0), (A,B)\}$ with $A \neq 1$ and $A^2 + B^2 = 1$.

(iii) A calculation shows

$$(A,B) = \left(\frac{t^2-1}{t^2+1}, -\frac{2t}{t^2+1}\right) = \left(\frac{u^2-v^2}{u^2+v^2}, -\frac{2uv}{u^2+v^2}\right)$$

(iv) One checks that

$(u^2-v^2, -2uv, u^2+v^2)$

is a primitive Pythagorean triple.

Now, given a non-trivial primitive solution (x,y,z) (w.l.o.g. $z > 0$), let $(A,B) = \left(\frac{x}{z}, \frac{y}{z}\right)$ and and note that $A^2 + B^2 = 1, |A| < 1$. One checks that the line

$$D_{\frac{y}{x-z}} = \left\{(U,V) \in \mathbb{R}^2 : V = \frac{y}{x-z}(U-1)\right\}$$

passes through (A,B) and $(1,0)$.

This shows that up to sign every non-trivial primitive solution is obtained via the initial procedure.

The situation is very different for $n \geq 3$!

Fermat's last theorem (Wiles '95)

For $n \geq 3$, Fermat's equation does not admit any non-trivial integral solutions.

We will see: suffices to prove for $n = 4$ and n prime.

Famous special cases are due to Fermat ($n=4$), Euler ($n=3$), Legendre and Dirichlet ($n=5$), Lamé ($n=7$), Kummer (for all regular primes p, i.e. pth $\mathbb{Q}(e^{2\pi i/p})$).

conjecturally many ($\sim 60\%$)
NOT known

Remark: Case $n=4$ is done in the exercises.

Reduction to the cases $n=4$ and $n=p$ for odd primes p.

first a priori unknown case.

Assume FLT is known for 4 and p an odd prime. Let $n \geq 6$ not an odd prime. Then

$$n = k \cdot \ell$$

for either $k=4$ or k an odd prime and $\ell \geq 2$ an integer (by prime factorization in $\mathbb{Z}$).

Let (x,y,z) be a primitive solution, i.e.

$$x^n + y^n = z^n = (z^\ell)^k = (x^\ell)^k + (y^\ell)^k.$$

Note that (x^ℓ, y^ℓ, z^ℓ) is primitive, therefore FLT for $k \Rightarrow (x^\ell, y^\ell, z^\ell)$ is a trivial solution and thus so is (x,y,z). Hence FLT for n follows.

↑ that is why $k=2$ does not help.

FLT for $n=3$ (some details in the exercises):

Note that $(-1)^3 = -1$ implies that FLT for 3 is equivalent to triviality of all primitive solutions to

$$X^3 + Y^3 + Z^3 = 0.$$

In what follows we assume that $(x,y,z) \in \mathbb{Z}^3$ is a non-trivial primitive solution.

Case I: $3 \nmid xyz \Rightarrow x, y, z \equiv \pm 1 \pmod 3$ (as $\mathbb{F}_3$ has only two non-zero elts. ± 1).

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \Rightarrow x^3, y^3, z^3 \equiv \pm 1 \pmod 9.$$

($a = \pm 1$, $3 \mid b$)

Therefore $0 = x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \pmod 9$ ↯

Case II: $3 \mid z$ (w.l.o.g.).

Note that $3 \nmid xy$ (as otherwise $3 \mid x^3+y^2+z^2 \Rightarrow 3 \mid x \wedge 3 \mid y$ ↯)

Let $v \geq 1$ s.t. $3^v \mid z$ and $3^{v+1} \nmid z$. Replacing z by $-z$ and factoring by 3 we assume that

$$x^3 + y^3 = 3^{3v} z^3$$

with (x,y,z) primitive.

Goal: we construct, using (x,y,z) a primitive vector (ξ, υ, ζ) such that

$$\xi^3 + \upsilon^3 = 3^{3(v-1)} \zeta^3,$$

is a non-trivial primitive solution. FLT for 3 then follows by induction on v. (Fermat's method of infinite descent)

Tool: Factorization of the prime 3 in the Eisenstein integers

$$\mathbb{Z}[j] \subset \mathbb{C},$$

where $j = \frac{-1+i\sqrt{3}}{2} = e^{2\pi i/3}$ is one of the two roots of X^2+X+1.

Why? Because

$$x^3 + y^3 = (x+y)(x+jy)(x+j^2y).$$

Theorem: (1) $\mathbb{Z}[j] = \mathbb{Z} + \mathbb{Z}j$

(2) $\mathbb{Z}[j] = \overline{\mathbb{Z}[j]}$

(3) Let $Nr(q) = q\bar{q}$ $(q \in \mathbb{Z}[j])$. Then $Nr(\mathbb{Z}[j]) \subseteq \mathbb{N} \cup \{0\}$ and

$$\mathbb{Z}[j]^\times = \{q \in \mathbb{Z}[j] : Nr(q) = 1\} = \{\pm 1, \pm j, \pm j^2\}$$

(4) If $q \in \mathbb{Z}[j] - \{0\}$, then

$$\left| \mathbb{Z}[j] / (q) \right| = Nr(q).$$

(5) $\mathbb{Z}[j]$ is a PID

Remarks: (1) follows from Ex. 2.

(2) $\bar{j} = j^2 \Rightarrow \bar{j} \in \mathbb{Z}[j] \Rightarrow \overline{\mathbb{Z}[j]} = \mathbb{Z}[\bar{j}] \subseteq \mathbb{Z}[j]$

$j = -1 - j^2 = -1 - \bar{j} \Rightarrow j \in \mathbb{Z}[\bar{j}] \Rightarrow \mathbb{Z}[j] \subseteq \mathbb{Z}[\bar{j}] = \overline{\mathbb{Z}[j]}$

(3) First, note that for $a, b \in \mathbb{Z}$ we have

$$Nr(a+jb) = \underbrace{a^2 - ab + b}_{\in \mathbb{Z}} = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2 \geq 0$$

Characterization of units via norm as for Gaussian integers. For identification, one solves

$$1 = Nr(a+jb) \qquad (a, b \in \mathbb{Z}).$$

(4) follows from Ex. 1.b)

(5) Domain is clear. Principality: $\mathbb{Z}[j]$ is also Euclidean (Ex. 1a).

Proposition: Let $\pi_3 = 1 - j$. Then

- π_3 is irreducible, i.e. (π_3) is a prime ideal.
- $3 = -j^2\pi_3^2$, i.e. $(3) = (\pi_3)^2$.

Proof: $Nr(\pi_3) = 3 \Rightarrow \pi_3$ is irreducible by multiplicativity of norm.

$\Rightarrow (\pi_3) \lhd \mathbb{Z}[j]$ is prime.

$1 = j^3 = j^2 \cdot j$

$3 = Nr(\pi_3) = \pi_3\overline{\pi_3} = -j^2\pi_3^2$ $\quad (\overline{\pi_3} = 1 - \bar{j} = 1 - j^2 = -j^2(1-j) = -j^2\pi_3).$

$\Rightarrow (3) = (\pi_3^2) = (\pi_3)^2.$ ∎

Starting the descent: Let $A=x+y$, $B=x+jy$, $C=x+j^2y=\overline{B}$ $\qquad ABC=3^{3v}z^3$

Lemma: $\exists\, z_0,z_1,z_2\in\mathbb{Z}[j]$ pairwise coprime and coprime to π_3 s.t.

$$A=3^{3v-1}z_0,\quad B=\pi_3 z_1,\quad C=\pi_3 z_2 \qquad (z_2=-j^2\overline{z}_1)$$

Proof: $\pi_3\mid 3\mid ABC$ (as $v\geq 1$) $\Rightarrow \pi_3\mid A \vee \pi_3\mid B \vee \pi_3\mid C$.

O.t.o.h. $A-B=\pi_3 y$, $A-C=(1-j^2)y=-j^2\pi_3 y$

$$\Rightarrow \boxed{\pi_3\mid A \wedge \pi_3\mid B \wedge \pi_3\mid C}$$

$C=\overline{B} \Rightarrow \pi_3^k\mid B \Leftrightarrow (-j^2)^k\pi_3^k=\overline{\pi_3}^k\mid C$, i.e. $\boxed{v_{\pi_3}(B)=v_{\pi_3}(C).}$

Also, $\boxed{\pi_3\nmid xyz}$ Assume $\pi_3\mid x \Rightarrow 3=Nr(\pi_3)=\pi_3\overline{\pi_3}\mid x\overline{x}=x^2 \Rightarrow 3\mid x$ ↯

Thus $B-C=j\pi_3 y$ and $\pi_3\nmid y \Rightarrow \boxed{v_{\pi_3}(B)=1}$

$\Rightarrow B=\pi_3 z_1$ w/ $\pi_3\nmid z_1$ and $C=\overline{B}=-j^2\pi_3\overline{z}_1=\pi_3 z_2$ w/ $\pi_3\nmid z_2$.

$$v_{\pi_3}(A)+2=v_{\pi_3}(ABC)=v_{\pi_3}(3^{3v}z^3)=6v$$

$\Rightarrow A=\pi_3^{6v-2}y_0=3^{3v-1}z_0$ w/ $\pi_3\nmid z_0$.

Remains to show that z_0,z_1,z_2 are coprime.

Assume that $\pi \in \mathbb{Z}[j]$ is an irreducible divisor of z_0 and z_1.

$$\Rightarrow \pi \mid A \wedge \pi \mid B$$

$$\Rightarrow \pi \mid A - B = \pi_3 y \qquad \wedge \pi \mid jA - B = -\pi_3 x$$

$$\Rightarrow \pi \mid y \qquad \Rightarrow \pi \mid x$$

$$\Rightarrow 1 < Nr(\pi) \mid Nr(y) = y^2 \wedge Nr(\pi) \mid x^2$$

$$\Rightarrow (x,y) \neq 1 \overset{3 \nmid Nr(\pi)}{\Longrightarrow} (x,y,z) \neq 1 \lightning$$

Let $p \mid Nr(\pi)$, then $p \neq 3$ and $p \mid x^3 + y^3 = 3^{3v} z^3 \Rightarrow p \mid z^3$.

Remaining cases are similar.

- $A - C = -j^2 \pi_3 y$ and $j^2 A - C = j^2 \pi_3 x$
- $B - C = j \pi_3 y$ and $jB - C = -\pi_3 x$.

∎

Remark: • $z_1 \notin \mathbb{Z}[j]^\times : z_1 \in \mathbb{Z}[j]^\times \Rightarrow 1 = Nr(z_1) = \frac{1}{3} Nr(B) \Rightarrow Nr(B) = 3$

$$\Rightarrow x, y = \pm 1 \Rightarrow \pm 1 + \pm 1 = x^3 + y^3 = 3^{3v} z^3 \lightning$$

• $z_2 \notin \mathbb{Z}[j]^\times : Nr(z_2) = Nr(-j^2 \bar{z}_1) = Nr(z_1) \neq 1$

Lemma: Up to multiplication by a third root of unity, z_i is a cube in $\mathbb{Z}[j]$, i.e. there are $u_i \in \{1, j, j^2\}$ and $\varrho_i \in \mathbb{Z}[j]$ s.t. $z_i = u_i \varrho_i^3$.

Proof: $\beta^{3v} z^3 = (\beta^{3v-1} z_0)(\pi_3 z_1)(\pi_3 z_2)$ and $\pi_3 \nmid z_i$

$$\Rightarrow (z^3) = (z_0 \cdot z_1 \cdot z_2) = (z_0) \cdot (z_1) \cdot (z_2).$$

As $\mathbb{Z}[j]$ is a UFD, we have

$$z = u \cdot \overline{\prod_{r \in \mathbb{Z}[j]/\mathbb{Z}[j]^\times}} r^{v_r(z)}$$

$\left(v_r(z) = \max\{v \in \mathbb{N} \cup \{0\} : r^v \mid z\}\right)$

for some $u \in \mathbb{Z}[j]^\times$.

$$\Rightarrow z_0 \cdot z_1 \cdot z_2 = z^3 = \overline{\prod_{r \in \mathbb{Z}[j]/\mathbb{Z}[j]^\times}} r^{3v_r(z)}$$

and therefore coprimality implies that $z_i = \xi_i \varrho_i^3 = (-\xi_i)(-\varrho_i)^3$ ∎

Lemma: $u_0 = 1$ and w.l.o.g. $\varrho_0 \in \mathcal{H}$

Proof: $z_0 = \frac{A}{3^{3v-1}} = \frac{x+y}{3^{3v-1}} \in \mathbb{Q}^\times \therefore 1 = \frac{z_0}{\overline{z_0}} \Rightarrow \mathcal{H}[j]^\times \ni \frac{u_0}{\overline{u_0}} = \left(\frac{\overline{\varrho_0}}{\varrho_0}\right)^3 \in \mathbb{Q}(j)^{\times 3} \overset{(*)}{\Rightarrow} \frac{\overline{\varrho_0}}{\varrho_0} \in \mathcal{H}[j]^\times$

($x = -y \Rightarrow z^3 = x^3 + y^3 = x^3 + (-x)^3 = 0 \Rightarrow (x,y,z)$ is a trivial solution)

(*): Let $u = \frac{u_0}{\overline{u_0}}$, then $\varrho_0^3 = u\overline{\varrho_0}^3$. If $r \in \mathcal{H}[j]$ is irred., then $r \mid \varrho_0 \leftrightarrow r \mid \overline{\varrho_0}$. (Now cancel common divisors)

$\Rightarrow \frac{u_0}{\overline{u_0}}$ is a cube in $\mathcal{H}[j]^\times \Rightarrow \frac{u_0}{\overline{u_0}} \in \{\pm 1\}$ $(1 = 1^3 = j^3 = (j^2)^3,\ -1 = (-1)^3 = (-j)^3 = (-j^2)^3)$

$\boxed{\Rightarrow u_0 = 1}$ (as $u_0 \in \{1, j, j^2\}$ and $\frac{j}{\overline{j}}, \frac{j^2}{\overline{j^2}} \notin \{\pm 1\}$)

In particular, $\boxed{\varrho_0^3 = z_0 \in \mathbb{Q}^\times}$, i.e. ϱ_0 is a root of $X^3 - z_0 \in \mathbb{Q}[X]$, at least one of which is real. Moreover, for any root ϱ_0, the set of all roots is given by $\{\varrho_0, j\varrho_0, j^2\varrho_0\}$, thus w.l.o.g. $\boxed{\varrho_0 \in \mathbb{R}}$

$\Rightarrow \varrho_0 \in \mathbb{R} \cap \mathcal{H}[j] = \mathcal{H}$ $(a + bj \in \mathbb{R} \Rightarrow b = 0)$

Lemma: Let $z_0 = \xi_0^3$ w/ $\xi_0 \in \mathbb{Z}$, then $u_1 = 1$.

Proof (skipped): $9 \mid 3^{3v-1} z_0 \Rightarrow x+y \equiv 0 \mod \pi_3^4$ $\quad (\pi_3^4 \sim 9)$

$$\Rightarrow \pi_3 y = A - B \equiv -B = -\pi_3 z_1 = -\pi_3 u_1 \xi_1^3 \mod \pi_3^4$$

$$\Rightarrow y \equiv -u_1 \xi_1^3 \mod \pi_3^3$$

As $\pi_3^3 \in (3)$, we have

$$\mathbb{Z}[j]/(\pi_3^3) \longrightarrow \mathbb{Z}[j]/(3)$$

and $y \equiv \pm 1 \pmod 3$ implies

$$u_1^{-1} \equiv \pm \xi_1^3 \mod (3). \qquad (*)$$

Note: $\mathbb{Z}[j]/(\pi_3)$ is a domain of cardinality $Nr(\pi_3) = 3$. Therefore

$$\pi_3 \nmid z_1 \Rightarrow \pi_3 \nmid \xi_1 \Rightarrow \xi_1 \equiv \pm 1 \mod \pi_3,$$

i.e. $\xi_1 = \pm 1 + \pi_3 r$ for some $r \in \mathbb{Z}[j]$.

$\Rightarrow \xi_1^3 \equiv \pm 1 \mod 3$ $\quad \xi_1^3 = (\pm 1)^3 + 3(\pm 1)^2 \pi_3 r + \cdots$ and $3 \mid \pi_3^3$.

$(*)$ $\Rightarrow u_1 \equiv \pm 1 \mod 3 \overset{u_1 \in \{1, j, j^2\}}{\Rightarrow} u_1 = 1$.

- $-\pi_3 = j - 1 \not\equiv 0 \mod 3$ as $\pi_3 \notin (3)$ — otherwise $(\pi_3) = (3) \Rightarrow 3 = Nr(\pi_3) = Nr(3) = 9$ ↯
- $-j^2 = j + 1$ is a unit mod 3 and similarly $-j = j^2 + 1$ is a unit mod 3.
- $j^2 \pi_3 = j^2 - 1 \equiv 0 \mod 3$ as j^2 is a unit mod (3) and $\pi_3 \notin (3)$.

∎

Conclusion (proof of FLT for $n=3$):

We know $x+y=3^{3v-1}\varsigma_0^3$, $x+j y=\pi_3\varsigma_1^3$, $x+j^2y=-j^2\pi_3\overline{\varsigma_1}^3$

wl $\varsigma_0\in\mathbb{Z}$, $\varsigma_1=a+bj\in\mathbb{Z}[j]$.

Plug $\pi_3=1-j$ and $\varsigma_1^3=(a+bj)^3$ expanded into $x+jy$ to obtain

$$\left.\begin{aligned} x&=a^3+b^3-6ab^2+3a^2b\\ y&=-a^3-b^3-3ab^2+6a^2b\end{aligned}\right\}\Rightarrow \quad 9ab(a-b)=x+y=9(3^{v-1}\varsigma_0)^3=9\cdot 3^{3(v-1)}\varsigma^3\neq 0$$

$\varsigma_0\in(\mathbb{Z}^\times)^3$

Claim: $a^2b+(-ab^2)$ is a sum of two cubes

Note: $(x,y)=1\Rightarrow(a,b)=1$ (any common divisor of a and b is a divisor of x and y)

$$\Rightarrow \boxed{1=(a,b)(a,a-b)(b,a-b)}$$

$(r,r-s)=(r,s-r)=(r,s)$

Therefore $3^{3(v-1)}\varsigma^3$ a cube $\Rightarrow$ $\boxed{a,b,a-b \text{ are cubes}}$

Case 1: $3\nmid ab$, then $p\mid a^2b \Leftrightarrow p\mid ba^2 \Leftrightarrow p\mid\varsigma^3$ $\Rightarrow$ we obtain primitive, non-trivial solution.

$\Updownarrow$ $\Updownarrow$ $\Updownarrow$

$p^3\mid a^2b$ $\quad p^3\mid ba^2$ $\quad p^3\mid\varsigma^3$

$a^2b=0\Leftrightarrow ab^2=0$

Case 2: $3\mid ab$. w.l.o.g. $3\mid a\Rightarrow 3\nmid b(a-b)$ and

$$a^2b-ab^2=b(a-b)((a-b)+b)=b(a-b)^2+b^2(a-b)$$

reduces to case 1.