Mathematical Enrichment Jan 28th, 2023

Kevin Hutchinson: Number Theory

"Diophantine Equations"

Find integer solutions to a given equation.

Pell's equation: $x^2 - 2y^2 = 1$.

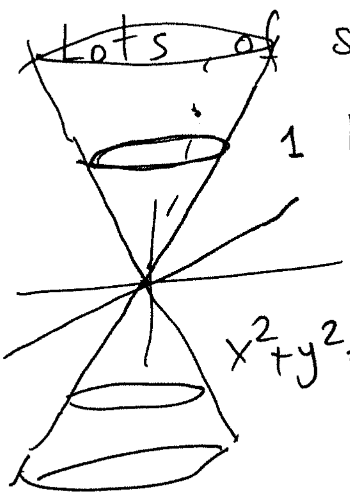
Fermat's Last Theorem

If $n \geq 3$, the equation $x^n + y^n = z^n$ has no (~~nonzero~~ positive) integer solutions

A classical example:

$$x^2 + y^2 = z^2$$

Lots of solutions: $1^2 + 1^2 = (\sqrt{2})^2$



1 but $\sqrt{2}$ not an integer. (not even rational)

$(x^0, y^0, z = \sqrt{x^2+y^2})$

Diophantine: We want integer solutions.

Example $(3,4,5)$ is one solution.

multiply by 2: $(6,8,10)$ . .

3. $(9,12,15)$

$(3m, 4m, 5m)$

m any integer

<u>Another solution</u>: $(20, 21, 29)$ . . .

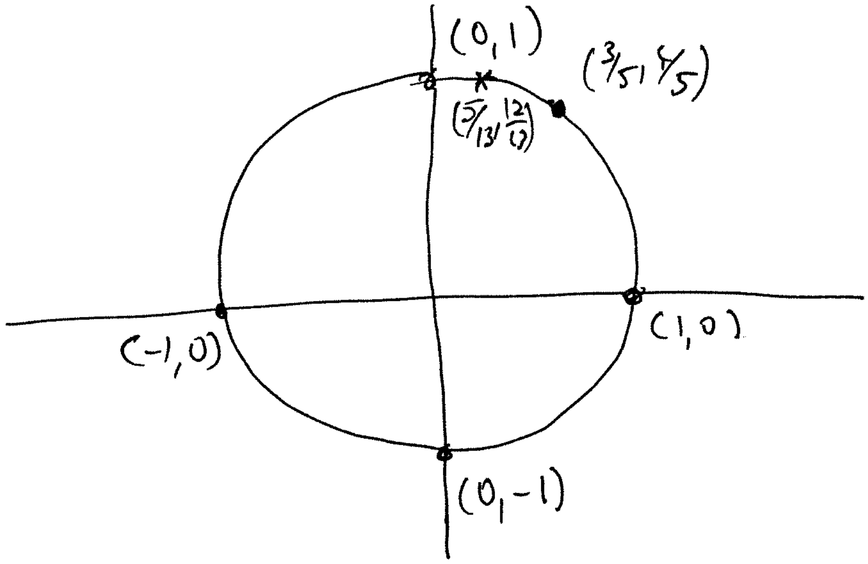
also: $(5, 12, 13)$ . . . "Pythagorean Triples"

Suppose (m, n, ℓ) is an integer solution:

$$m^2 + n^2 = \ell^2$$

$$\iff \left(\frac{m}{\ell}\right)^2 + \left(\frac{n}{\ell}\right)^2 = 1.$$

$\iff \left(\frac{m}{\ell}, \frac{n}{\ell}\right)$ lies on $x^2 + y^2 = 1$.
"unit circle"



$(3,4,5)$
$\updownarrow$
$\left(\frac{3}{5}, \frac{4}{5}\right)$

$(5, 12, 13)$
$\updownarrow$
$\left(\frac{5}{13}, \frac{12}{13}\right)$

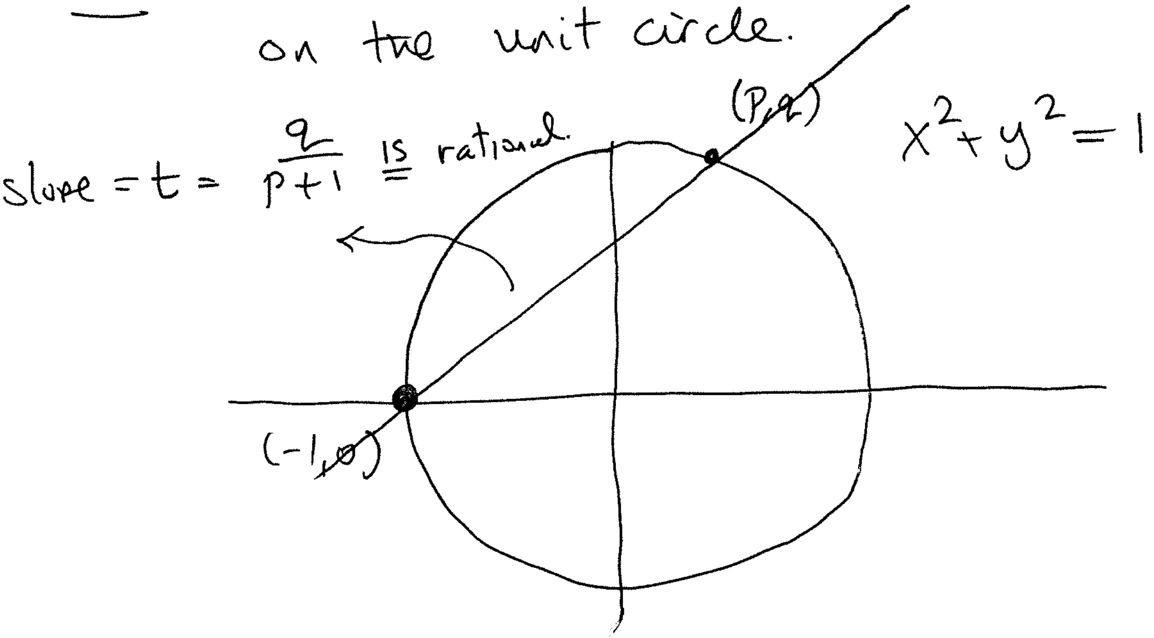
Conversely, suppose (p, q) is a <u>rational point</u> on the unit circle.

Then $p = \frac{m}{\ell} = \frac{tm}{t\ell}$, $q = \frac{n}{\ell} = \frac{tn}{t\ell}$ for some common denominator ℓ.

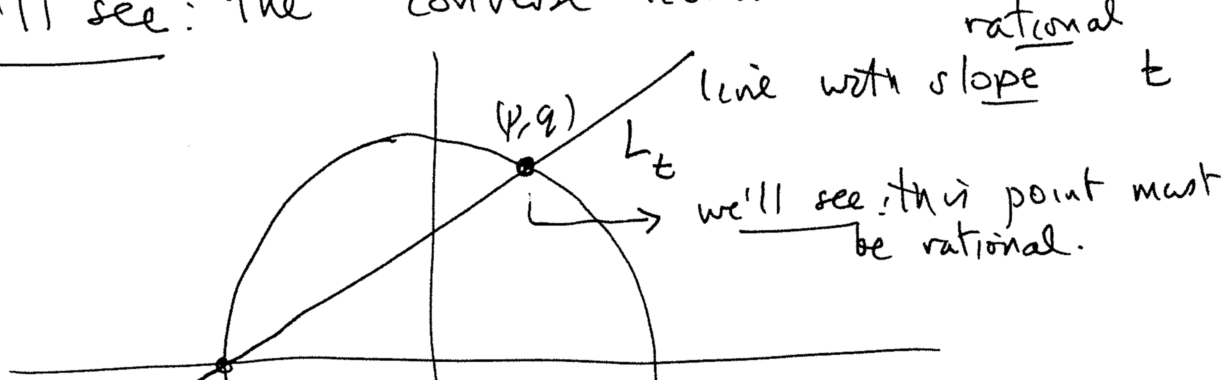
$$1 = p^2 + q^2 = \left(\frac{m}{\ell}\right)^2 + \left(\frac{n}{\ell}\right)^2$$

$\iff \ell^2 = m^2 + n^2 \iff (m, n, \ell)$ is a Pythagorean triple.

So: We must find all rational points on the unit circle.



We'll see: the converse holds



This will give us all rational points.

Observation on ~~polyno~~ quadratics.

~~Supp~~ Given a quadratic $ax^2 + b\cancel{x} + c$ with roots r_1, r_2.

We must have

$$ax^2+bx+c = a(x-r_1)(x-r_2)$$
$$= a(x^2-(r_1+r_2)x + r_1 r_2).$$

$$\Rightarrow \quad b = -a(r_1+r_2) \qquad c = a r_1 r_2.$$
$$r_1+r_2 = -\frac{b}{a}, \quad r_1 r_2 = \frac{c}{a}$$

Consequence (corollary):

Suppose a, b, c are rational.

If r_1 is rational, then so is r_2.

(Since $r_2 = -\frac{b}{a} - r_1$, for example)

The same idea works for cubics, quartics, ...

$$ax^3 + bx^2 + cx + d$$

If r_1, r_2, r_3 are the roots.

Then $r_1 + r_2 + r_3 = -\frac{b}{a}$, $r_1 r_2 r_3 = -\frac{d}{a}$

If a, b, c, d rational, if r_1, r_2 are rational then so is r_3).

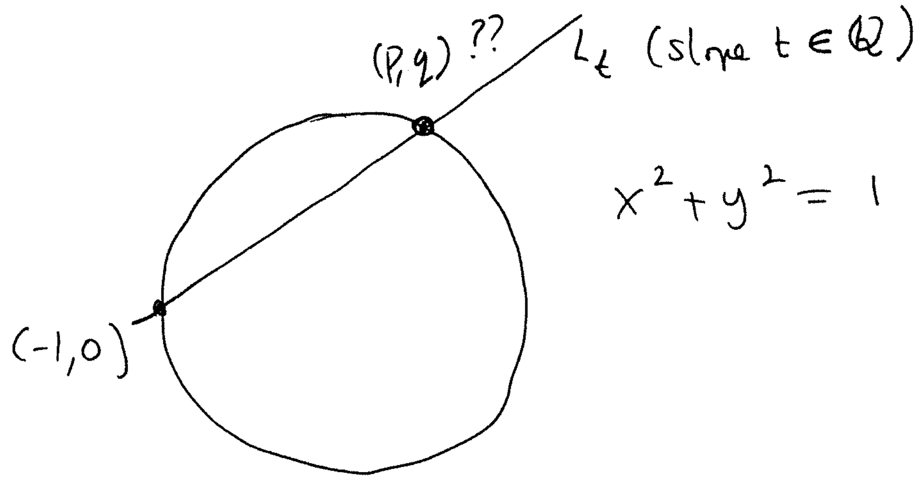
Example $6x^3 - 17x^2 + 11x - 2$.

$2, \frac{1}{2}$ are roots of this.

What is the 3rd root?

Answer $\frac{17}{6} - 2 - \frac{1}{2} = \boxed{\frac{1}{3}}$

or $= \frac{2}{6 \; 2 \cdot \frac{1}{2}} = \frac{1}{3}$.



Equation of L_t: $\quad y = t(x+1)$

<u>Solve</u> $\quad x^2 + [t(x+1)]^2 = 1$

$$x^2(1+t^2) + 2t^2x + (t^2-1) = 0.$$

$x = -1$ is one solution.

$$\therefore x = \frac{t^2-1}{t^2+1} \cdot \frac{1}{-1} = \frac{1-t^2}{1+t^2} = p.$$

Then $y = t(x+1) = t \cdot \left[\dfrac{1-t^2}{1+t^2} + 1\right] = \dfrac{2t}{1+t^2} = q$

<u>Conclusion</u>: The rational points on the unit circle are the points $\left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$ for any $t \in \mathbb{Q}$

Suppose $t = \dfrac{m}{n}$ $\quad m, n$ integers $\quad (m, n \in \mathbb{Z})$

$$\frac{1-t^2}{1+t^2} = \frac{1-\frac{m^2}{n^2}}{1+\frac{m^2}{n^2}} = \frac{n^2-m^2}{n^2+m^2}$$

$$\frac{2t}{1+t^2} = \frac{2\cdot\frac{m}{n}}{1+\frac{m^2}{n^2}} = \frac{2mn}{n^2+m^2}.$$

The rational points are

$$\left(\frac{n^2 - m^2}{n^2 + m^2}, \frac{2mn}{n^2+m^2} \right) \qquad m, n \text{ integers.}$$

$\therefore$ The Pythagorean triples are

$$(n^2 - m^2, \ 2mn, \ n^2 + m^2) \qquad m, n \text{ integers.}$$

$$\begin{array}{ccc} n^2 - m^2 & 2mn & n^2+m^2 \\ \parallel & \parallel & \parallel \\ x & y & z \end{array}$$

<u>Examples</u>

$n = 2, \ m = 1$ $\quad (3, 4, 5)$

$n = 3, \ m = 1$ $\quad (8, 6, 10)$

$n = 3, \ m = 2$ $\quad (5, 12, 13)$ .. etc

Find all integer solutions of

$$2x^2 + 5y^2 = 7z^2$$

(We'll look at this after the break).

(Terminology. "whole number" – not an official mathematical term.

<u>Integers</u> ($\mathbb{Z}$) $\ldots, -2, -1, 0, 1, 2, 3, \ldots$

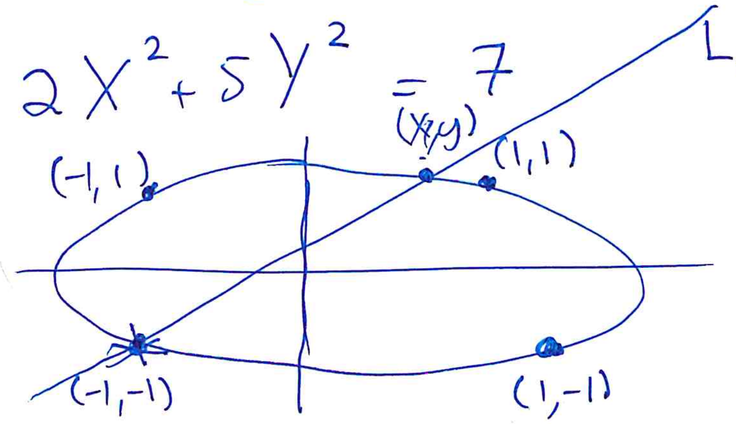
Natural numbers ($\mathbb{N}$) $1, 2, 3, 4, \ldots$ = positive integers

(In French, $\mathbb{N}$ = $0, 1, 2, 3 \ldots$ = nonnegative integers)

$$2x^2 + 5y^2 = 7z^2 \quad \text{(integer solutions)}$$

To solve
We must find all <u>rational</u> points on the curve

$$2X^2 + 5Y^2 = 7$$



Equation of L_t: $\underline{y+1 = t(x+1)}$: $\underline{y = tx + (t-1)}$.

This gives the quadratic equation

$$2x^2 + 5[tx + (t-1)]^2 - 7 = 0$$

$$x^2(\underbrace{5t^2+2}) + \underbrace{10t(t-1)}\, x + \underbrace{5(t-1)^2 - 7} = 0$$

$x = -1$ is a root.

The other root: $x = \dfrac{-10(t-1)}{5t^2+2} + 1 = \dfrac{2 + 10t - 5t^2}{5t^2+2}$.

$$y = tx + (t-1) = \frac{5t^2 + 4t - 2}{5t^2+2}$$

Now $t = \dfrac{m}{n}$, $m, n \in \mathbb{Z}$.

$$x = \frac{2 + 10 \cdot \frac{m}{n} - 5 \cdot \left(\frac{m}{n}\right)^2}{5 \cdot \left(\frac{m}{n}\right)^2 + 2} = \frac{2n^2 + 10mn - 5m^2}{5m^2 + 2n^2}$$

Similarly $\quad y = \dfrac{5m^2 + 4mn - 2n^2}{5m^2 + 2n^2}$.

$\Rightarrow$ $\quad$ m, n any integers

The solutions of $\;2x^2 + 5y^2 = 7z^2$

are $\quad (2n^2 + 10mn - 5m^2,\ 5m^2 + 4mn - 2n^2,\ 5m^2 + 2n^2)$

where $m, n \in \mathbb{Z}$.

$m = 2, n = 1$ gives $\quad (2, 26, 22) = 2(1, 13, 11)$

$$2x^2 + 5y^2 = 7z^2$$
$$\Updownarrow$$
$$2 \cdot \left(\frac{x}{z}\right)^2 + 5 \cdot \left(\frac{y}{z}\right)^2 = 7$$

Consider $\underbrace{1^2, 5^2}_{24}, \underbrace{\ 7^2}_{24}$, 3 squares (of integers).

In arithmetic progression

Find all such triples.

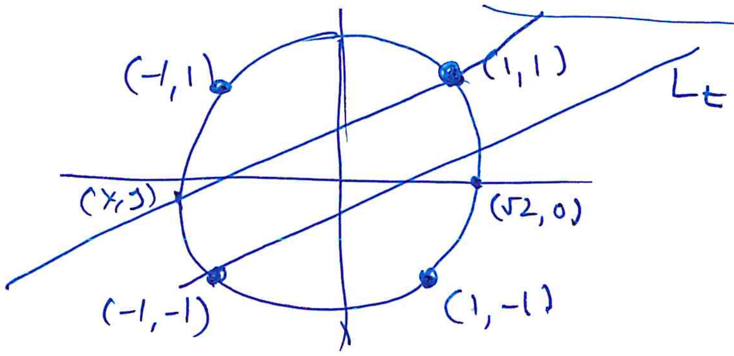
We want a^2, b^2, c^2 such that

$$b^2 - a^2 = c^2 - b^2;$$

i.e. $$\boxed{a^2 + c^2 = 2b^2}$$

In other words, we are looking for all integer solutions of $\underline{x^2 + y^2 = 2z^2}$

$\iff$ rational points on the circle $\boxed{x^2 + y^2 = 2.}$



Start with (1,1): L_t $\quad y - 1 = t(x-1)$

$$\boxed{y = tx + 1 - t}$$

$$x^2 + [tx + (1-t)]^2 = 2$$

$$x^2 \underbrace{(1+t^2)} + \underbrace{2t(1-t)}x + \underbrace{t^2 - 2t - 1}_{c} = 0$$

$x = 1$ is one solution

The other solution is $x = \dfrac{t^2 - 2t - 1}{t^2 + 1}$

This gives $y = tx + 1 - t = \dfrac{t^2 + 2t - 1}{t^2 + 1}$

$t = \frac{m}{n}$ as before.

This gives all integer solutions to $x^2+y^2=2z^2$:

$$(m^2-2mn-n^2,\ m^2+2mn+n^2,\ m^2+n^2)$$

where $m, n \in \mathbb{Z}$

$m=4, n=1$ gives $(7, 23, 17)$. $\quad 7^2, 17^2, 23^2$

Historical note:

Fermat: Do there exist integers a^2, b^2, c^2, d^2 in an arithmetic progression?

The answer is no: To prove this, Fermat used his "method of descent".

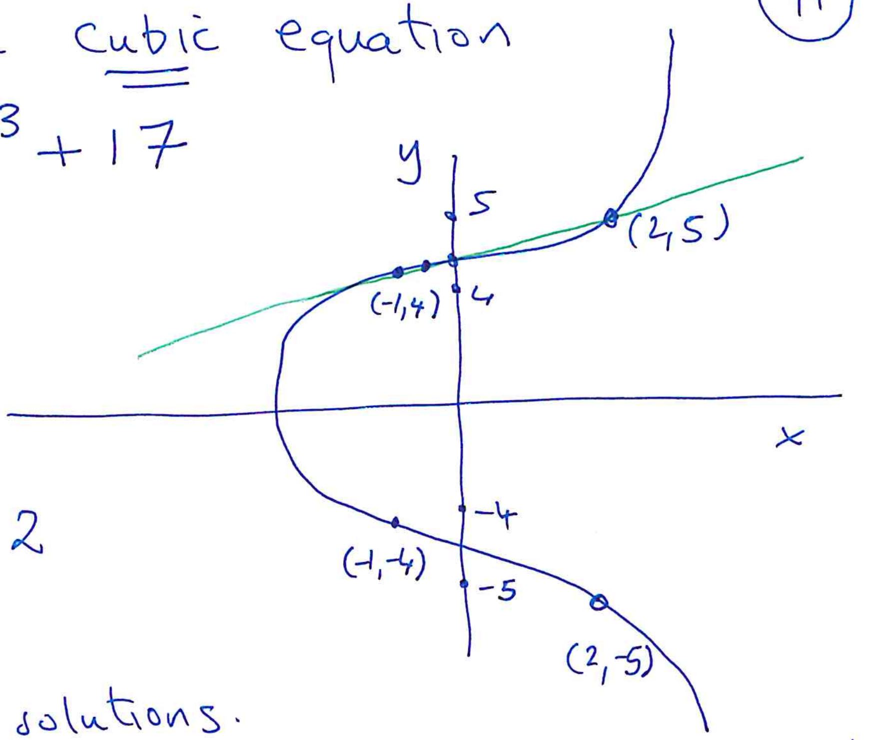
Frank Calegari talk

google youtube calegari fermat

Let's consider the $\underline{\text{cubic}}$ equation

$$y^2 = x^3 + 17$$

"elliptic curve"



$(-1,4)$, $(2,5)$ are 2 rational solutions

Find more rational solutions.

Line joining $(-1,4)$ to $(2,5)$ is $y = \frac{1}{3}(x+13) : L$

Therefore the ~~poin~~ x-coordinates of the points of intersection of L with our curve satisfy

$$\left[\frac{1}{3}(x+13)\right]^2 = x^3 + 17$$

(We know -1, 2 are roots)

$$x^3 - \frac{1}{9}x^2 + \cdots = 0.$$

The third root is $x = \frac{1}{9} + 1 - 2 = -\frac{8}{9}$

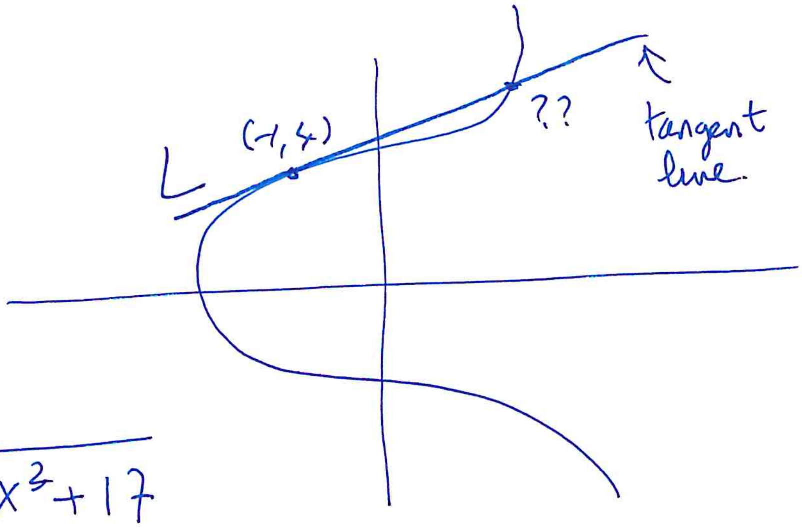
Then $y = \frac{1}{3}(x+13) = \pm\frac{109}{27}$

This gives the new rational point $\left(-\frac{8}{9}, \frac{109}{27}\right)$.

i.e. $\left(\frac{109}{27}\right)^2 = -\left(\frac{8}{9}\right)^3 + 17.$

i.e. $109^2 = -8^3 + 17 \cdot 27^2$

Variation



$$y = \sqrt{x^3+17}$$

Calculus tells us the slope of L is $\frac{3x^2}{2y} = \frac{3}{8}$

So tangent line is $y-4 = \frac{3}{8}(x+1)$

$$y = \frac{1}{8}(3x+35)$$

$$y^2 = x^3+17$$

$$\left[\frac{1}{8}(3x+35)\right]^2 = x^3+17$$

roots are $-1, -1, ?$

$$x^3 - \frac{9}{64}x^2 + \cdots$$

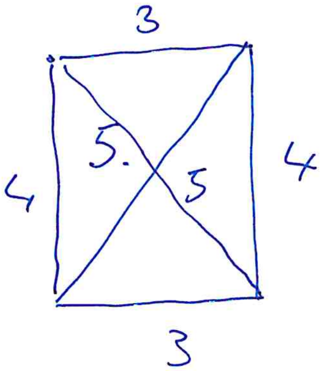
Other root is $x = \frac{9}{64} + 2 = \frac{137}{64}$

Then $y = \frac{1}{8}(3x+35) = \frac{2651}{512}$

another point on $y^2 = x^3+17$

A problem

(3, 4, 5).



(1) Find 6 noncollinear points in the plane such that the distance between any pair is an integer

(2) Show that one can find 1000 not all (noncollinear) points arranged such that all distances are integers.

(3) (**) Can one find infinitely many points in the plane, not all collinear, such that the distance between any pair is an integer?

[Hard!]