Higher Diophantine equations

Higher Diophantine equations

Question

Find all triples of integers (a, b, c) *such that*

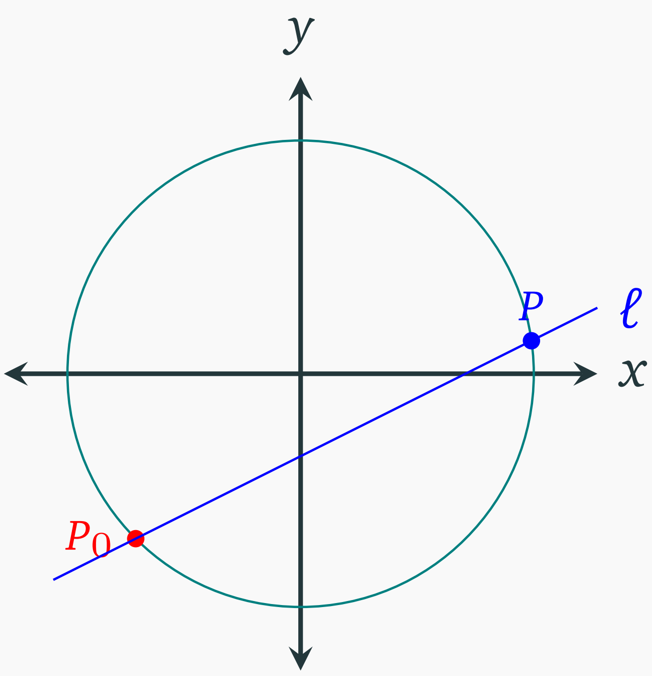
$$a^2 + b^2 = N \cdot c^2.$$

Or, equivalently, find all rational points on the circle

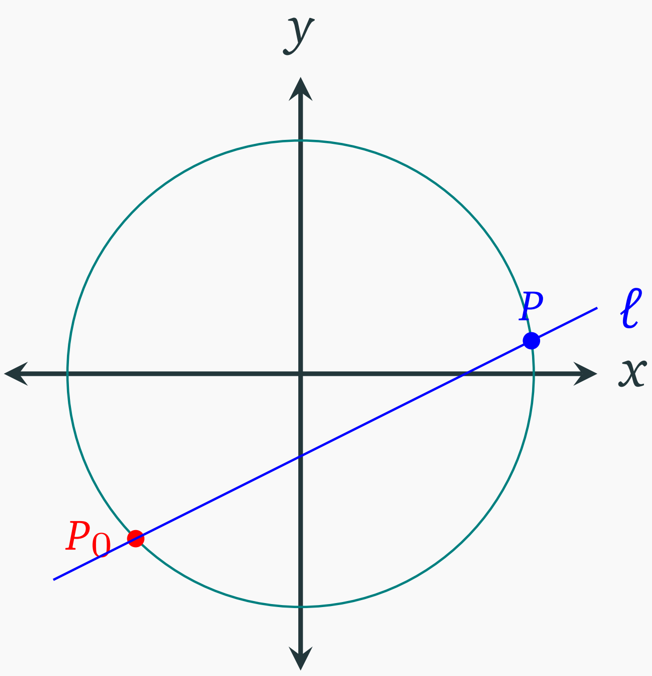
$$X^2 + Y^2 = N.$$

N.B. $(\overset{m}{a^2 + b^2})(\overset{n}{c^2 + d^2}) = \overset{m \cdot n}{(ac - bd)^2 + (ad + bc)^2}$. Hence, it is sufficient to consider only N = primes.

When $N = 2$. We can find some specific rational points on the circle $X^2 + Y^2 = 2$. For instance, $P_0 = (-1, -1)$.
Draw a line ℓ through P_0. Then it intersects with the circle by a point $P = (x, y)$.

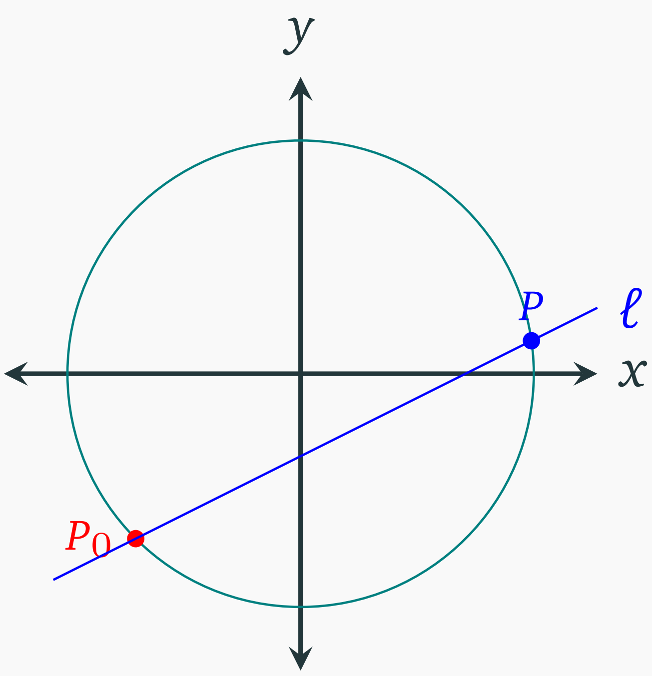


When $N = 2$. We can find some specific rational points on the circle $X^2 + Y^2 = 2$. For instance, $P_0 = (-1, -1)$.
Draw a line ℓ through P_0. Then it intersects with the circle by a point $P = (x, y)$.



Each line ℓ is determined by its slope $t \in \mathbb{Q} \cup \{\infty\}$, where the vertical line has ∞ slope.

When $N = 2$. We can find some specific rational points on the circle $X^2 + Y^2 = 2$. For instance, $P_0 = (-1, -1)$.
Draw a line ℓ through P_0. Then it intersects with the circle by a point $P = (x, y)$.



Each line ℓ is determined by its slope $t \in \mathbb{Q} \cup \{\infty\}$, where the vertical line has ∞ slope. And each line ℓ intersects the circle with another point P except when ℓ is tangent to the circle at P_0.

We thus conclude similarly:

1. The rational points on the circle $X^2 + Y^2 = 2$ are parameterized in $\mathbb{Q} \cup \{\infty\}$ (where P_0 corresponds to -1) via

$$t \in \mathbb{Q} \cup \{\infty\} \longmapsto \left(\tfrac{1+2t-t^2}{1+t^2}, \tfrac{t^2+2t-1}{1+t^2}\right).$$

When plug in $t = \infty$ to $\frac{1+2t-t^2}{1+t^2}$, think it as $\lim\limits_{t\to\infty} \frac{1+2t-t^2}{1+t^2}$. Similar applies to $\frac{t^2+2t-1}{1+t^2}$. Another way to understand uses the notion of *projective line*.

Higher Diophantine equations

We thus conclude similarly:

1. The rational points on the circle $X^2 + Y^2 = 2$ are parameterized in $\mathbb{Q} \cup \{\infty\}$ (where P_0 corresponds to -1) via

$$\underbrace{t}_{=\frac{m}{n}} \in \mathbb{Q} \cup \{\infty\} \longmapsto \Big(\underbrace{\tfrac{1+2t-t^2}{1+t^2}}_{\frac{a}{c}}, \underbrace{\tfrac{t^2+2t-1}{1+t^2}}_{\frac{b}{c}} \Big).$$

2. We thus have

$$\begin{aligned} &\left\{(a, b, c) \in \mathbb{Z}^3 \,\middle|\, a^2 + b^2 = 2c^2\right\} \\ &\quad = \mathbb{Z} \cdot \left\{(n^2 + 2mn - m^2, m^2 + 2mn - n^2, m^2 + n^2) \,\middle|\, (m, n) \in \mathbb{Z}^2\right\} \end{aligned}$$

When $N = 3$, it seems impossible to find any rational point. In fact, we will show that

Theorem 3.9.1

There is no nontrivial triples of integers (a, b, c) *such that*

$$a^2 + b^2 = 3 \cdot c^2.$$

Proof. Indeed, if such a triple (a, b, c) exists, then we may assume $\gcd(a, b, c) = 1$ (since the equation is homogeneous). We have

$$a^2 + b^2 + c^2 = 4 \cdot c^2.$$

Namely, $4 \mid a^2 + b^2 + c^2$.

On the other hand, a square can either be divided by 4 (if the base is even), or equals a multiple of 4 plus 1 (if the base is odd). Hence, the sum $a^2 + b^2 + c^2$ is a multiple of 4 if and only if all of a, b, c are even, contradicting with $\gcd(a, b, c) = 1$. $\square$

To prove the equation $a^2 + b^2 = 3 \cdot c^2$ has no nontrivial solution, we reduce the problem to prove $a^2 + b^2 - 3 \cdot c^2$ is never a multiple of 4 except the trivial cases. Namely, we try to solve the equation in remainders after dividing by 4. Doing so, we reduce an infinite problem to finite problem.