# DIOPHANTINE EQUATIONS
# (MA2316, SIXTH WEEK)

VLADIMIR DOTSENKO

When one talks about Diophantine equations in the context of number theory, this refers to solving polynomial equations with several variables over integers. There are some famous examples of that sort, e.g. the equation $x^2 = 2y^2$ (it has just one integer solution $(0,0)$, this corresponds to the fact that $\sqrt{2}$ is irrational), or the equation $x^2 - Dy^2 = 1$ (Pell's equation that we mentioned before), or the equation $x^2 + y^2 = z^2$ (Pythagorean triples, that is sides of right triangles with integer side lengths), or the equation $x^n + y^n = z^n$ (Fermat's equation). In this lecture, we shall discuss some ways to classify all solutions to some equations like that.

First, let us classify all Pythagorean triples. Note that if $x^2 + y^2 = z^2$, and $x, y$ have a common divisor $d$, then $z$ also is divisible by $d$, and we can cancel out $d^2$. Thus, we should only concern ourselves with "primitive" solutions, that is solutions without common divisors. For such a solution, let us divide both sides by $z^2$, obtaining $s^2 + t^2 = 1$, where $s$ and $t$ are fractions written in lowest terms. To classify rational solutions to quadratic equations in two variables, there is a famous method, which is also known as Euler's substitutions in integral calculus. Namely, we know one rational solution $(1,0)$ to our equation. If we draw a line through that point and another rational solution, it will have rational slope, since it passes through two points with rational coordinates. More interestingly though, every line whose slope is rational, meets our curve (the circle $s^2+t^2 = 1$) at a point with rational coordinates. Indeed, a line with rational slope $k$ passing through $(1,0)$ has the equation $t = k(s-1)$, and substituting it into $s^2 + t^2 = 1$, we get

$$(k(s-1))^2 + s^2 = 1,$$

or

$$(s-1)(k^2(s-1) + s + 1) = 0,$$

which means that besides the root $s = 1$ that we already know, there is also a root

$$s = \frac{k^2-1}{k^2+1},$$

so that the corresponding $t = k(s-1) = \frac{-2k}{k^2+1}$, and we get a *rational parametrisation* of the circle $s^2+t^2 = 1$ as $\left(\frac{k^2-1}{k^2+1}, \frac{-2k}{k^2+1}\right)$. Since $t$ here is arbitrary, we can multiply it by $-1$ to not carry around all the signs, and use the parametrisation $\left(\frac{k^2-1}{k^2+1}, \frac{2k}{k^2+1}\right)$.

Let us now go back to the original equation $x^2 + y^2 = z^2$. Recall that if we assume that a solution is primitive, that is without common factors, we have $s = \frac{x}{z}$ and $t = \frac{y}{z}$ as fractions in lowest terms. If $k = \frac{p}{q}$, we have $(s,t) = \left(\frac{p^2-q^2}{p^2+q^2}, \frac{2pq}{p^2+q^2}\right)$. Almost always these are fractions in lowest terms: e.g., if $p^2 - q^2$ and $p^2 + q^2$ have common divisors, so do $2p^2 = (p^2+q^2) + (p^2-q^2)$ and $2q^2 = (p^2+q^2) - (p^2-q^2)$, so by the assumption on $\frac{p}{q}$ being in lowest terms, the only possible factor involved may be 2. That indeed may happen if $p$ and $q$ are both odd. (If they are of different parities, $p^2+q^2$ is not divisible by 2, and if they are both even, $\frac{p}{q}$ is not in lowest terms). To summarise, we get now two series of solutions that exhaust all solutions to the Pythagorean triple equation: $\left(p^2-q^2, 2pq, p^2+q^2\right)$ where $p, q$ are of different parity, and $\left(\frac{p^2-q^2}{2}, pq, \frac{p^2+q^2}{2}\right)$ where $p, q$

are odd. Let us examine the latter case a bit better. Assume that $p$ and $q$ are both odd. Denote $\frac{p+q}{2} = p'$, $\frac{p-q}{2} = q'$. Then we have $\frac{p^2-q^2}{2} = 2p'q'$, $pq = (p')^2 - (q')^2$, and $\frac{p^2-q^2}{2} = (p')^2 + (q')^2$, that is the other series with $x, y$ swapped. We arrive at the following precise statement:

**Theorem 1.** *Let $(x, y, z)$ be a primitive solution to the Pythagorean triple equation where $y$ is even. Then there exist coprime integers $p, q$ such that $x = p^2 - q^2$, $y = 2pq$, $z = p^2 + q^2$.*

Note that in a primitive Pythagorean triple one of $x, y$ must be even, for if $x, y$ are odd, then both $x^2$ and $y^2$ are congruent to 1 modulo 4, so this would imply that $z^2$ is congruent to 2 modulo 4, which is clearly impossible.

Let us instantly use that result to prove a particular case of Fermat's Last Theorem. We shall deduce it from the following stronger result:

**Theorem 2.** *The equation $x^4 + y^4 = z^2$ has no integer solutions where both $x$ and $y$ are nonzero.*

*Proof.* First of all, it is enough to study primitive solutions. For if $\gcd(x, y) = k$, then clearly $z^2$ is divisible by $k^4$ and $z$ is divisible by $k^2$, so $\left(\frac{x}{k}, \frac{y}{k}, \frac{z}{k^2}\right)$ is a primitive solution. Second, since $x^4 + y^4 = z^2$ now leads to a primitive Pythagorean triple $(x^2, y^2, z)$, we may without loss of generality assume that $y^2$ is even, since in a Pythagorean triple one of the first two entries is even. Therefore we have, for some $u, v$, $(x^2, y^2, z) = (u^2 - v^2, 2uv, u^2 + v^2)$, so in particular $x^2 = u^2 - v^2$, or $x^2 + v^2 = u^2$. Since we assumed that $y^2$ was even, $x^2$ is odd, so $v^2$ is even, and there exist $s, t$ such that $(x, v, u) = (s^2 - t^2, 2st, s^2 + t^2)$. Substituting these above, we get $y^2 = 2uv = 2(s^2 + t^2) \cdot 2st = 4st(s^2 + t^2)$. Since $y$ was assumed even, we can write that as

$$\left(\frac{y}{2}\right) = st(s^2 + t^2).$$

Note that $s, t$ are coprime, and hence $s^2 + t^2$ is coprime with them. A product of coprime integers is a perfect square if and only if each of them is a square, so $s = l^2$, $t = m^2$, $s^2 + t^2 = n^2$ for some $l, m, n$. This implies $l^4 + m^4 = n^2$. Note that $x = s^2 - t^2 = l^4 - m^4$, and $y = \sqrt{4st(s^2 + t^2)} = 2lmn$. In particular, $\max(|l|, |m|) < |y| \leq \max(|x|, |y|)$, so we produced a way to go from a primitive solution to a "smaller" primitive one. Note also that if $y \neq 0$, then $l, m \neq 0$, since $y = 2lmn$. This process of moving to "smaller" solutions cannot continue forever, so we have a contradiction with the existence of a primitive solution with nonzero components. □

Another example that we shall discuss is the equation $x^2 + y^2 + z^2 = kxyz$, where $x, y, z$ are integers. Changing, if necessary, signs of some of $x, y, z$, we may assume that $x, y, z, k \geq 0$. Let us prove the following theorem.

**Theorem 3.** (1) *For $k \neq 1, 3$, the above equation has no solutions besides $x = y = z = 0$.*

(2) *There is a one-to-one correspondence between solutions to the equation $x^2 + y^2 + z^2 = xyz$ and solutions to the* Markov's equation *$x^2 + y^2 + z^2 = 3xyz$.*

(3) *There are infinitely many solutions to the Markov's equation.*

*Proof.* The cases $k = 1$ and $k = 2$ will be discussed in an upcoming tutorial.

Let us show that for $k > 3$ there are no solutions. Suppose that we have a solution, so that $a^2 + b^2 + c^2 = kabc$. If one of coordinates is zero, it is clear that it forces the other coordinates to vanish also, so we may assume that they are all positive.

*Step 1.* Let us show that the numbers $a, b, c$ are pairwise distinct. Indeed, if $a = b$ then our equation becomes $2a^2 + c^2 = ka^2c$, or $c^2 = a^2(kc - 2)$, so that $a^2 \mid c^2$, $a \mid c$, and $c = ad$ for some integer $d$. Substituting it into the original equation, we get $d^2 = kad - 2$, so $d \mid 2$, that is $d = 1$ or $d = 2$, — either way, $d^2 = kad - 2$ becomes $ka = 3$ which contradicts $k > 3$.

*Step 2.* Without loss of generality, we have $a < b < c$. Considering our equation as a quadratic equation $x^2 - kabx + a^2 + b^2 = 0$ for unknown $c$ with $a, b$ fixed, we note that $(a, b, kab - c)$ is also a

solution, since the sum of roots of an equation $x^2+px+q=0$ is equal to $-p$. Moreover, $kab-c$ is positive, since the product of roots of an equation $x^2+px+q=0$ is equal to $q$, so $kab-c=\frac{a^2+b^2}{c}>0$. Note that for $g(x)=x^2-kabx+a^2+b^2$, we have $g(b)=2b^2+a^2-kab^2<3b^2-kab^2=b^2(3-ka)<0$, so $b$ is between $c$ and $3ab-c$. Since $b<c$ by assumption, we have $3ab-c<b<c$. Thus, from a positive solution to our equation, we obtained a positive solution with smaller maximal coordinate. This cannot continue forever, so there can be no solutions.

Let us now explore the case $k=3$. It turns out that the procedure we used above to move to a solution with smaller maximal coordinate can be used to describe a hierarchical structure on solutions in this case. Let us first show that apart two special cases, the coordinates of a solution are pairwise distinct. We proceed as above: if $a=b$ then our equation becomes $2a^2+c^2=3a^2c$, or $c^2=a^2(3c-2)$, so that $a^2 \mid c^2$, $a \mid c$, and $c=ad$ for some integer $d$. Substituting it into the original equation, we get $d^2=3ad-2$, so $d \mid 2$, that is $d=1$ or $d=2$, — either way, $d^2=3ad-2$ becomes $3a=3$, and $a=1$. Then we have $c^2+2=3c$, so $c=1$ or $c=2$. Thus, we get solutions $(1,1,1)$ and $(1,1,2)$, and, of course, the permutations of the latter one, $(1,2,1)$ and $(2,1,1)$.

Apart from the solutions we just described, every solution has pairwise distinct coordinates, and so if $(a,b,c)$ is such a solution, then $(3bc-a,b,c)$, $(a,3ac-b,c)$, and $(a,b,3ab-c)$ are three different solutions that we shall call neighbours of the given one. These solutions have positive coordinates for the same reasons as above. Let us show that for a solution with pairwise distinct coordinates, one of its neighbours has smaller maximal coordinate. This proceeds as the second half of the argument above. Indeed, we may assume $a<b<c$, and for $h(x)=x^2-3abx+a^2+b^2$, we have $h(b)=2b^2+a^2-3ab^2<3b^2-3ab^2=3b^2(1-a)\leq 0$, so $b$ is between $c$ and $3ab-c$. Since $b<c$ by assumption, we have $3ab-c<b<c$. This shows that by a sequence of moves to neighbours, we can arrive at one of the exceptional solutions. Note also that $(1,1,1)$ is a neighbour of $(1,1,2)$, and the neighbour relation is symmetric, since the same move repeated twice brings us back. Therefore all solutions are connected to $(1,1,1)$. Finally, let us show that there are infinitely many solutions. Let us take a solution with pairwise distinct coordinates $a<b<c$, and consider its neighbour $(3bc-a,b,c)$. For $k(x)=x^2-3bcx+c^2+b^2$, we have $h(c)=2c^2+b^2-3bc^2<3c^2-3bc^2=3c^2(1-b)\leq 0$, so $c$ is between $a$ and $3bc-a$. Since $a<c$ by assumption, we have $a<c<3bc-a$. Therefore, one of the neighbours of a solution with pairwise distinct coordinates has a strictly larger maximal coordinate, and we are done. $\square$