A FIRST VIEW OF DIOPHANTINE EQUATIONS

Diophantine equations are polynomial equations with integer coefficients (and any number of variables) to which solutions are sought in integers. A famous (and recent!) results that should immediately comes to mind is “Fermat’s last [i.e. Wiles’s] Theorem”

\[ x^n + y^n = z^n, \; n > 2, \; x, y, z \in \mathbb{Z} \implies xyz = 0. \]

We will mainly concentrate on quadratic (degree 2) and cubic (degree 3) equations.

First some history: Hilbert’s 10th problem (1900) asks for an algorithm which determines (in a finite number of operations) whether a given Diophantine equation is soluble (in integers). In 1970 — building on at least four decades of work (of Hilary Putnam, Martin Davis, and especially Julia Robinson\(^1\)), some of it in logic and analytic philosophy — Yuri Matiyasevich proved that such an algorithm does not in general exist. (His method involved the famous Fibonacci numbers, and so-called “Diophantine sets”.) There exist, for example, Diophantine equations with no solutions, but such that this fact cannot be proved (“within a given axiomatization of number theory”). This may be viewed as a “concrete” instance of Gödel’s Incompleteness Theorem.

So while Diophantine equations withhold their secrets from any method, it is certainly true that algebraic number theory has been tremendously successful in making them more accessible — a case in point will be our study of Pell’s equation

\[ x^2 - y^2 d = \begin{cases} 
\pm 1 & \text{if } d \equiv 2, 3 \pmod{4} \\
\pm 4 & \text{if } d \equiv 1 \pmod{4} 
\end{cases} \quad (d \text{ squarefree}). \]

\(^1\)see the documentary Julia Robinson and Hilbert’s 10th problem
But we shall begin instead with a pair of fun examples to introduce the topic.

**Lagrange’s four-square theorem.** I claim that for any \( N \in \mathbb{N} \), there exist \( w, x, y, z \in \mathbb{Z} \) such that

\[
N = x^2 + y^2 + z^2 + w^2;
\]

that is, \( N \) is a “4-square”. (Note that any of \( x, y, z, w \) are allowed to be 0.)

**Example 1.** \( 111 = 9^2 + 5^2 + 2^2 + 1^2 \), and \( 2 = 1^2 + 1^2 + 0^2 + 0^2 \).

**Step 1: Reduction to \( N \) prime.** An identity of Euler

\[
(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (aw + bx + cy + dz)^2 + (ax - bw - cz + dy)^2 + (ay + bz - cw - dx)^2 + (az - by + cx - dw)^2
\]

says that any product of 4-squares is again a 4-square. So it is sufficient to prove the 4-square theorem for (odd) primes \( p \).

**Step 2: For each odd prime \( p \), there exists \( 0 < m < p \) such that \( mp \) is a 4-square.** More precisely, we will show that \( mp = x^2 + y^2 + 1 \) for some \( x, y \in \mathbb{Z} \) and \( 0 < m < p \). You see, either \(-1\) is a square (mod \( p \)), and we can take \( x = 0 \); or the set of \((p+1)/2\) numbers (mod \( p \)) \(-1 - y^2\) and \((p+1)/2\) numbers (mod \( p \)) \(x^2\) must have an intersection, by the pigeonhole principle. [Details are left as an exercise.]

**Step 3: If \( mp \) is a 4-square, then there exists \( 0 < m' < m \) such that \( m'p \) is a 4-square.** (Then we will be done, since by repeatedly applying this we eventually get \( m' = 1 \).)

Case I (\( m \) even): If \( 2N = w^2 + x^2 + y^2 + z^2 \), then there are an even number of odd integers and an even number of even integers amongst \( x, y, z, w \). Group them in pairs accordingly, say \( x \equiv w \) for (2) \( y \equiv z \) for (2). Then

\[
N = \left( \frac{w+x}{2} \right)^2 + \left( \frac{w-x}{2} \right)^2 + \left( \frac{y+z}{2} \right)^2 + \left( \frac{y-z}{2} \right)^2
\]

presents \( N \) as a 4-square. In particular, if \( mp \) is a 4-square, then so is \( \frac{m}{2} p \).
Case II \((m \text{ odd})\): Given \(mp = w^2 + x^2 + y^2 + z^2\), with \(0 < m < p\) (see Step 2), choose the unique \(a, b, c, d \equiv w, x, y, z\) with \(-\frac{m}{2} < a, b, c, d < \frac{m}{2}\). Then we have

\[
a^2 + b^2 + c^2 + d^2 \equiv w^2 + x^2 + y^2 + z^2 \pmod{m}
\]

\[
\implies a^2 + b^2 + c^2 + d^2 = mk,
\]

for some \(0 < k < m\). (If \(k \geq m\), this contradicts \(|a, b, c, d| < \frac{m}{2}\); if \(k = 0\), then \(0 = a = b = c = d \implies m \mid x, y, z, w \implies m^2 \mid x^2 + y^2 + z^2 + w^2 = mp \implies m \mid p\) contradicting \(0 < m < p\).)

Now we use Euler’s identity (1) again, in which the left-hand side equals \((a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = km \cdot mp\). The right-hand side is a sum squares of four expressions, each divisible by \(m\): e.g.

\[
aw + bx + cy + dz \equiv a^2 + b^2 + c^2 + d^2 = mk \equiv 0,
\]

\[
ax - bw - cz + dy \equiv ab - ba - cd + dc = 0.
\]

Therefore

\[
kp = X^2 + Y^2 + Z^2 + W^2,
\]

where \(k < m\). This finishes Step 3 hence the proof of Lagrange’s Theorem.

**Fermat’s Last Theorem with \(n = 4\).** I make the slightly stronger claim that

\[(2) \quad X^4 + Y^4 = Z^2\]

has no solution in (all nonzero) integers. Clearly it suffices to show there is no solution in positive integers. In fact, it suffices to prove there is no primitive solution — that is, a solution \((x, y, z)\) with \(x, y, z > 0\) and \(\gcd(x, y, z) = 1\). For if a positive solution \((X, Y, Z)\) exists with \(p \mid X, Y, Z\), then actually \(p^2 \mid Z\) and \((\frac{X}{p}, \frac{Y}{p}, \frac{Z}{p})\) is a new solution; repeating this, one eventually arrives at a primitive one.

So suppose we have a primitive solution \((x, y, z)\). Writing it as \((x^2)^2 + (y^2)^2 = z^2\), this is a Pythagorean triple. In §IV.B we will
prove that the complete list of Pythagorean triples \( a^2 + b^2 = c^2 \) is \( \{(2rs, s^2 - r^2, s^2 + r^2) \mid r, s \in \mathbb{N}\} \). So there must be integers \( r, s \) with \( s > r \) such that

\[
x^2 = 2rs, \quad y^2 = s^2 - r^2, \quad \text{and} \quad z = s^2 + r^2.
\]

From the primitivity assumption it also follows that \((r, s) = 1\), and \((y, z) = 1\) (since any prime dividing \( y \) and \( z \) also would divide \( x \)).

We rewrite (2) as

(3) \[
x^4 = (z - y^2)(z + y^2) \left( = 2r^2 \cdot 2s^2 \right)
\]

Suppose \( r \in \mathbb{N} \) divides both factors on the right-hand side of (3). Then

\[
r \mid z - y^2 + z + y^2 = 2z \quad \text{and} \quad r \mid z + y^2 - (z - y^2) = 2y^2 \quad \implies \quad r \mid 2,
\]

and so \((z - y^2, z + y^2) = 2\) (and not \( 2^k > 1 \)). Using (3) again, we find

(a) \[
z - y^2 = 2a^4 \quad \text{(a odd)} \quad \text{and} \quad z + y^2 = 2b^4;
\]

(b) \[
z - y^2 = 2^3 a^4 \quad \text{and} \quad z + y^2 = 2b^4 \quad \text{(b odd)}.
\]

If (a) holds, then \( 2y^2 = 2^3 b^4 - 2a^4 \implies y^2 = 4b^4 - a^4 \implies y^2 \equiv -a^4 \equiv -1 \pmod{4}\), which is impossible as \(-1\) is not a quadratic residue mod 4.

So (b) holds (with both \( a \) and \( b \) nonzero), and adding/subtracting equations yields

\[
y^2 = b^4 - 4a^4
\]

\[z = b^4 + 4a^4,
\]

which imply

(4) \[
4a^4 = (b^2 - y)(b^2 + y) \quad 0 < b < z.
\]

Suppose some prime \( p \) divides \( b^2 - y \) and \( b^2 + y \). Then \( p \mid 2b^2 \) and \( p \mid 2y \). If \( p \neq 2 \) then \( p \) divides \( y \) and \( 2b^4 - y^2 = z \), hence also \( z - y^2 \) and \( z + y^2 \), which contradicts \((z - y^2, z + y^2) = 2\). So \( p = 2 \), and \((b^2 - y, b^2 + y) = 2\) (It can’t be \( 2^k > 1 \), since \( b \) is odd.)
So we can rewrite (4) as

\[ a^4 = \left( \frac{b^2 - y}{2} \right) \left( \frac{b^2 + y}{2} \right) \]

with the right-hand factors relatively prime (and nonzero). By the fundamental theorem of arithmetic, we conclude from this that \( b^2 - y = 2c^4 \) and \( b^2 + y = 2d^4 \), and so

\[ b^2 = c^4 + d^4, \text{ where } 0 < b < z. \]

In fact, since \( c \) and \( d \) are coprime and nonzero (we may take them to be positive), \((c, d, b)\) is a second primitive solution to (2), like the solution \((x, y, z)\) we started with. But there is an important difference: \( b \) is smaller than \( z \).

This is the end of the proof: we could always have taken \((x, y, z)\) to be a primitive solution with minimal \( z \) \((> 0)\). The method of descent just described (and essentially due to Fermat) then produces a primitive solution with smaller \( z \) \((> 0)\), which is absurd. Consequently, there can’t have been a primitive solution, hence any solution in nonzero integers, in the first place.