Descent I

1 Pythagorean triples

We want to find all right triangles with all three sides of integral length. In other words, we want to solve the diophantine equation

$$x^2 + y^2 = z^2. \tag{1}$$

Note that any solution generates a positive solution by changing the sign, hence solving the equation in $\mathbb{Z}$ is equivalent to solving it in $\mathbb{Z}_{>0}$, which is the same as finding all right triangles with integral sides. We can further reduce the problem to finding solutions with $(x, y, z) = 1$, that is we exclude similar triangles. Each such solution will generate infinitely many solutions (dx, dy, dz) with gcd $= d$ and vice versa.

It is worth noticing that if a prime p divides two of the number x, y, z then it would have to divide the third one as well. Hence we must have $(x, y) = (y, z) = (x, z) = 1$.
There is one more observation we can make to simply our problem.

Claim $x \not\equiv y \pmod 2$.

Proof. We know that we cannot have $x \equiv y \equiv 0 \pmod 2$ because that force x and y to not be relatively prime. We are going to argue by contradiction for the other case as well. Assume that $x \equiv y \equiv 1 \pmod 2$. Then $x^2 \equiv y^2 \equiv 1 \pmod 4$, and this would mean that $z^2 \equiv 2 \pmod 4$, which is impossible. □

Since x and y are interchangeable in our problem, we can assume without loss of generality that x is odd and y is even. This also implies that z is odd. We can rewrite our equation as

$$y^2 = z^2 - x^2 = (z - x)(z + x)$$

and further as

$$\left(\frac{y}{2}\right)^2 = \frac{z-x}{2} \cdot \frac{z+x}{2}.$$

All the fractions above are really positive integers since y is even and x, z are both odd with $z > x$. Next we want to use the following observation.
Fact If $a, b, c \in \mathbb{Z}$ with $(a, b) = 1$ and $ab = c^2$, then there exist integers a_1, b_1 such that $a = a_1^2$ and $b = b_1^2$. Clearly a_1 and b_1 have to be relatively prime as well.

In order to do that, we need to show that $\gcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$. Assume that p is a prime that divides both of them. Then p divides both their sum and their difference, that is it has to divide both x and z. That would imply that p divides y as well, and this contradicts the fact that $(x, y, z) = 1$.

Hence the gcd of the two fractions is indeed 1 and there must exist positive integers u and v with $(u, v) = 1$ such that

$$\frac{z-x}{2} = v^2 \qquad \text{and} \qquad \frac{z+x}{2} = u^2.$$

This leads to

$$\begin{cases} x = u^2 - v^2 \\ y = 2uv \\ z = u^2 + v^2. \end{cases}$$

Note that since x and z are odd, we must also have $u \not\equiv v \pmod 2$. Also, $x > 0$ implies $u > v$.

In short, we proved that all positive Pythagorean triples are of the form

$$\begin{cases} x = d(u^2 - v^2) \\ y = 2duv \\ z = d(u^2 + v^2) \end{cases}$$

where $u, v \in \mathbb{Z}$, $u > v > 0$ and $u \not\equiv v \pmod 2$.

2 More descent

We want to study the Fermat equation for $n = 4$,

$$x^4 + y^4 = z^4. \tag{2}$$

Fermat himself proved that it has no non-trivial solutions (i.e. no integer solutions with $xyz \neq 0$). His proof uses again the method of descent.

Assume that x, y, z are positive integers satisfying (2). Set $d = (x, y, z)$. Then $x = dx_1$, $y = dy_1$ and $z = dz_1$ where $(x_1, y_1, z_1) = 1$ and x_1, y_1, z_1 are also positive integers satisfying the same equation (2). In particular, $x_1^2, y_1^2, t_1 = z_1^2$ is a relatively prime Pythagorean triple. In particular, x_1, y_1, t_1 are relatively prime positive integers that form a solution to the equation

$$X^4 + Y^4 = T^2. \tag{3}$$

Note that x_1 and y_1 are interchangeable, so we can assume without loss of generality that x_1 is odd and y_1 is even. It follows from our study of Pythagorean triples (Section 1) there exist integers $u > v > 0$ such that $(u, v) = 1$ and $u \not\equiv v \pmod 2$ such that

$$\begin{cases} x_1^2 = u^2 - v^2 \\ y_1^2 = 2uv \\ t_1 = u^2 + v^2. \end{cases}.$$

Since x_1 is odd, we have $x_1^2 \equiv 1 \pmod 4$ and therefore u is odd and v is even.

Note that this implies further that $(u, 2v) = 1$. Since $u(2v) = y_1^2$ and $2v$ is even, we have $u = t_2^2$ and $2v = 4d^2$ for some positive *relatively prime* integers t_2 and d, with t_2 odd.

We can rewrite the formula for x_1 as

$$x_1^2 + v^2 = u^2.$$

Since $(u, v) = 1$ it follows that x_1, v, u is a relatively prime Pythagorean triple with x_1 odd and v even. Applying again the results from Section 1, there exist integers $a > b > 0$ such that $(a, b) = 1$, $a \not\equiv b \pmod 2$ and

$$\begin{cases} x_1 = a^2 - b^2 \\ v = 2ab \\ u = a^2 + b^2. \end{cases}.$$

Since $v = 2ab$ and $2v = 4d^2$ it follows that $ab = d^2$. But $(a, b) = 1$ and therefore $a = x_2^2, b = y_2^2$ for some integers $x_2 > y_2 > 0$ with $(x_2, y_2) = 1$ and $x_2 \not\equiv y_2 \pmod 2$.

To recap, we have

$$\begin{aligned} u &= a^2 + b^2 \\ a &= x_2^2 \\ b &= y_2^2 \\ u &= t_2^2. \end{aligned}$$

Therefore x_2, y_2, t_2 are relatively prime positive integers that satisfy

$$x_2^4 + y_2^4 = t_2^2.$$

But we also have

$$t_2 \leq t_2^4 = u^2 < u^2 + v^2 = t_1.$$

We proved that if we start with a relatively prime positive solution (x_1, y_1, t_1) to (3) we can produce another relatively prime solution (x_2, y_2, t_2) with $0 < t_2 < t_1$. Applying this fact over and over again we obtain infinitely many positive solutions (x_n, y_n, t_n) to (3) with

$$0 < \ldots < t_n < t_{n-1} < \ldots < t_1.$$

This is impossible because there are only finitely many integers between 0 and t_1. (In fact, there are $t_1 - 1$ of them!)

In short, the assumption that we can find a positive solution to (2) led to a contradiction, and that proves that no such solution can exist.