Elementary Number Theory - Exercise 11a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Show that, in a primitive Pythagorean triple (a, b, c), a, b, c are pairwise coprime, a and b have different parity, and c is odd.

Solution 1. We have $a^2 + b^2 = c^2$ and $\gcd(a, b, c) = 1$. If p is a prime dividing $\gcd(a, b)$, then p must divide c^2, and hence c, which contradicts $\gcd(a, b, c) = 1$. We can argue in the same for $\gcd(a, c)$ and $\gcd(b, c)$. Hence a, b, c must be pairwise coprime.

If a, b are both even, then $a^2 + b^2$ is even, so c would be even, and the triple would not be primitive. If a, b are both odd, then $a^2 \equiv b^2 \equiv 1 \pmod 4$, but c^2 is even, so $c^2 \equiv 0 \pmod 4$, which yields the contradiction $2 \equiv 0 \pmod 4$. This shows that a and b have different parity, and consequently c is odd.

Problem 2. Find all Pythagorean triples (a, b, c) with $c \leq 25$.

Solution 2. We know that the primitive triples with odd a are given by

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

where $m > n$ are coprime natural numbers of different parity. Since $c \leq 25$, we must have $n < m \leq \sqrt{25} = 5$. Checking if $c = m^2 + n^2$ for all $1 < n < m \leq 25$ which are coprime and have different parity, we find the tuples

$$(m, n) \in \{(2, 1), (4, 1), (3, 2), (4, 3)\},$$

which give the 4 Pythagorean triples

$$[3, 4, 5], \qquad [15, 8, 17], \qquad [5, 12, 13], \qquad [7, 24, 25].$$

These are the primitive ones with odd a. By rescaling the first one with $k = 1, 2, 3, 4, 5$, and replacing a with b in all solutions, we obtain 16 Pythagorean triples.

Problem 3. We have seen in the lecture that every primitive Pythagorean triple (a, b, c) with odd a is given by

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

for some coprime $m > n$ of different parity. Show that m, n are uniquely determined by (a, b, c).

Solution 3. Suppose that we have coprime $m > n$ of different parity, and coprime $M > N$ of different parity, such that

$$m^2 - n^2 = M^2 - N^2, \quad 2mn = 2MN, \quad m^2 + n^2 = M^2 + N^2.$$

Adding and subtracting the first and the third identity we obtain

$$m^2 = M^2, \quad n^2 = N^2.$$

Since m, n, M, N are positive integers, this implies $m = M$ and $n = N$.

Problem 4. A Pythagorean triple (a, b, c) is called *almost isosceles* if $|a - b| = 1$.

1. Show that every almost isosceles Pythagorean triple is, up to switching a and b, of the form
$$\left(\frac{x-1}{2}, \frac{x+1}{2}, y\right)$$
where $(x, y) \in \mathbb{N}^2$ solves the *negative Pell equation* $x^2 - 2y^2 = -1$, and $x \geq 3$.

2. Show that every solution $(x, y) \in \mathbb{N}^2$ of $x^2 - 2y^2 = -1$ is of the form (x_n, y_n) where
$$x_n + \sqrt{2}y_n = (1 + \sqrt{2})^{2n+1}.$$

3. Determine the first three almost isosceles Pythagorean triples.

Solution 4. 1. By interchanging a and b we can assume that $a < b$, i.e. $b = a + 1$. If we put $x = 2a + 1$ and $y = c$, then $a = \frac{x-1}{2}$ and $b = a + 1 = \frac{x+1}{2}$, so (a, b, c) is of the form
$$\left(\frac{x-1}{2}, \frac{x+1}{2}, y\right).$$
Since this is a Pythogorean triple, we have
$$\left(\frac{x-1}{2}\right)^2 + \left(\frac{x+1}{2}\right)^2 = y^2$$
Multiplying out yields $x^2 - 2y^2 = -1$. Since $a \geq 1$, we have $x = 2a + 1 \geq 3$.

2. Every solution $(x, y) \in \mathbb{N}^2$ of the negative Pell equation $x^2 - 2y^2 = -1$ yields a solution of positive Pell equation $z^2 - 2w^2 = 1$ via
$$z + \sqrt{2}w = (x + \sqrt{2}w)(\sqrt{2} - 1) = (2w - x) + \sqrt{2}(x - w).$$
Indeed, we have
$$\begin{aligned} z^2 - 2w^2 &= (z + \sqrt{2}w)(z - \sqrt{2}w) = (x + \sqrt{2}w)(\sqrt{2} - 1)(x - \sqrt{2}w)(-\sqrt{2} - 1) \\ &= (x + \sqrt{2}w)(x - \sqrt{2}w)(\sqrt{2} - 1)(-\sqrt{2} - 1) = -(x^2 - 2y^2) = 1. \end{aligned}$$
Here we used that $(\sqrt{2} + 1)(\sqrt{2} - 1) = 1$. In fact, this gives a bijection between the solutions in $\mathbb{N}^2$ of the negative and the positive Pell equation.

The fundamental solution of $z^2 - 2w^2 = 1$ is given by $(z_1, w_1) = (3, 2)$, and we know from Lagrange's Theorem that every solution $(z, w) \in \mathbb{N}^2$ of $z^2 - 2w^2 = 1$ is of the form (z_n, w_n) where
$$z_n + \sqrt{2}w_n = (z_1 + \sqrt{2}w_1)^n = (3 + 2\sqrt{2})^n.$$
On the other hand, we have
$$3 + 2\sqrt{2} = (1 + \sqrt{2})^2,$$
so
$$z_n + \sqrt{2}w_n = (1 + \sqrt{2})^{2n}.$$
Hence, any solution (x, y) of $x^2 - 2w^2 = -1$ is given by (x_n, y_n) satisfying
$$(x_n + \sqrt{2}y_n)(\sqrt{2} - 1) = (1 + \sqrt{2})^{2n}.$$
Multiplying by $1 + \sqrt{2}$ and using $(1 + \sqrt{2})(1 - \sqrt{2}) = 1$ gives
$$x_n + \sqrt{2}y_n = (1 + \sqrt{2})^{2n+1}.$$

3. We use that $(1+\sqrt{2})^2 = (3+2\sqrt{2})$ and compute

$$
\begin{aligned}
x_1 + \sqrt{2}y_1 &= 1+\sqrt{2}, \\
x_2 + \sqrt{2}y_2 &= (1+\sqrt{2})(3+2\sqrt{2}) = 7+5\sqrt{2}, \\
x_3 + \sqrt{2}y_3 &= (7+5\sqrt{2})(3+2\sqrt{2}) = 41+29\sqrt{2}, \\
x_4 + \sqrt{2}y_4 &= (41+29\sqrt{2})(3+2\sqrt{2}) = 239+169\sqrt{2}.
\end{aligned}
$$

The fundamental solution $(x_1, y_1) = (1, 1)$ does not give a Pythagorean triple since $x < 3$, but the other three solutions give the first three almost isosceles Pythagorean triples

$$(3,4,5), \qquad (20,21,29), \qquad (119,120,169).$$

Problem 5. Fermat's Last Theorem states that for $n \geq 3$ the equation $a^n + b^n = c^n$ has no integer solution with a, b, c all different from 0. Show that it suffices to prove Fermat's Last Theorem for prime exponents $n = p \geq 3$.

Solution 5. Suppose we had proved Fermat's Theorem for each prime exponent $p \geq 3$. Now suppose that there would be a counter-example for some $n \geq 3$, that is, an integer solution of $a^n + b^n = c^n$ with $a, b, c \neq 0$. Let p be a prime factor of n. Then we have

$$(a^{n/p})^p + (b^{n/p})^p = (c^{n/p})^p,$$

and $a^{n/p}, b^{n/p}, c^{n/p}$ are non-zero integer solutions of $a^p + b^p = c^p$, which is a contradiction.

Problem 6. Show that, for each $n \in \mathbb{N}$, the numbers

$$(2n+1,\ 2n^2+2n,\ 2n^2+2n+1)$$

form a primitive Pythagorean triple. Compute them for $n = 10^m$ for $m = 1, 2, 3, 4, 5$ and admire the beautiful pattern that you get.

Solution 6. We just need to check that

$$(2n+1)^2 + (2n^2+2n)^2 = (2n^2+2n+1)^2,$$

which is easy to do. For $n = 10^m$ and $m = 1, 2, 3, 4, 5$ we get the triples

$$
\begin{aligned}
&(21, 220, 221) \\
&(201, 20200, 20201) \\
&(2001, 2002000, 2002001) \\
&(20001, 200020000, 200020001) \\
&(200001, 20000200000, 20000200001).
\end{aligned}
$$

Problem 7 (sage)**.** Write a program which lists all Pythagorean triples (a, b, c) with $c \leq N$ for a given N.