Problem Set #11

Due monday December 2nd in Class

Exercise 1: (⋆) 4 points
Find the minimal solutions to $x^2 - 3y^2 = 1$, $x^2 - 6y^2 = 1$.

Solution:
Let $d$ be a positive square free integer. In general, the fundamental solution of a diophantine equation $x^2 - dy^2 = 1$ is the smallest number of
\[ \{a + b\sqrt{d} \mid a^2 - db^2 = 1, a > 0, b > 0\} \]
Hence, the minimal solution to $x^2 - 3y^2 = 1$ is $2 + \sqrt{3}$. The minimal solution to $x^2 - 6y^2 = 1$ is $5 + 2\sqrt{6}$.

Exercise 2: (⋆) 4 points
Parametrize all rational solutions of $x^2 + y^2 = 5$

Solution:
Let $P = (1, 2)$. Note that $P$ is on the circle defined by $x^2 + y^2 = 5$ which we denote by $S^1$. For each rational $t \in \mathbb{Q}$, consider the line $l_t$ passing through $P$ with the slope $t$. Then, $l_t$ meets with $S^1$ at two points, $P$ and another point, and we denote that point by $P_t$. Now, $P_t$ satisfies the system of equations:
\[ x^2 + y^2 = 5 \]
\[ y - 2 = t(x - 1) \]
Solve these equations, then we obtain that
\[ P_t = \left( \frac{t^2 - 4t - 1}{t^2 + 1}, \frac{-2t^2 - 2t + 2}{t^2 + 1} \right) \]
Let $S$ be the set of all rational solutions of $x^2 + y^2 = 5$. Then, from the construction, a map
\[ \Phi : \mathbb{Q} \ni t \mapsto P_t \in S \setminus \{(1, -2)\} \]
is bijective. Thus, all rational solutions are
\[ \left\{ \left( \frac{t^2 - 4t - 1}{t^2 + 1}, \frac{-2t^2 - 2t + 2}{t^2 + 1} \right) \mid t \in \mathbb{Q} \right\} \cup \{(1, -2)\} \]

Exercise 3: (⋆) 4 points
Let \( p \) be a prime \( \equiv 1 \mod 4 \). Prove that \( x^2 - py^2 = -1 \) has a non-trivial integer solution.

**Solution:**

Let \( a + b\sqrt{p} \) be the minimal solution of \( x^2 - py^2 = 1 \). If \( a \) is even, then \( b \) is odd. So, we can conclude that

\[
1 \equiv a^2 - pb^2 \equiv -b^2 \equiv -1 \mod 4
\]

which is a contradiction. Hence, \( a \) must be odd. Then, note that

\[
\frac{a - 1}{2} \cdot \frac{a + 1}{2} = p \left( \frac{b}{2} \right)^2
\]

and \( \frac{a-1}{2}, \frac{a+1}{2}, \frac{b}{2} \) are integers. Thus, the prime factorization theorem tells us that there exist positive integers \( u, v \) such that \( a \pm 1 = 2u^2 \), \( a \mp 1 = 2pv^2 \), and \( b = 2uv \). Then,

\[
u^2 - pv^2 = \frac{1}{2}(2u^2 - 2pv^2) = \frac{1}{2}(a \pm 1 - (a \mp 1)) = \pm 1\]

If \( u^2 - pv^2 = 1 \), then it’s easy to see that \( a \geq u \) and \( b > v \). However, this contradicts that \( a + b\sqrt{p} \) is the minimal solution of \( x^2 - py^2 = 1 \). Hence, \( u^2 - pv^2 = -1 \). **Exercise 4:** (⋆) 4 points

Let \( x_1 = 3, y_1 = 4, z_1 = 5 \) and let \( x_n, y_n, z_n \) for \( n = 2, 3, 4, \ldots \) be defined recursively by

\[
x_{n+1} = 3x_n + 2z_n + 1, \quad y_{n+1} = 3x_n + 2z_n + 2, \quad z_{n+1} = 4x_n + 3z_n + 2.
\]

Show \( x_n, y_n, z_n \) is a Pythagorean triple for each \( n \).

**Solution:**

Clearly this is true for \( n = 1 \), so we now proceed by induction. Assume \( x_n, y_n, z_n \) is a Pythagorean triple. Not by definition \( y_n = x_n + 1 \) for each \( n \). Now consider,

\[
x_{n+1}^2 + y_{n+1}^2 - z_{n+1}^2 = (3x_n + 2z_n + 1)^2 + (3x_n + 2z_n + 2)^2 - (4x_n + 3z_n + 2)^2
\]

\[
= 2x_n^2 + 2x_n - z_n^2 + 1
\]

\[
x_n^2 - z_n^2 + (x_n^2 + 2x_n + 1)
\]

\[
x_n^2 - z_n^2 + (x_n + 1)^2
\]

\[
x_n - z_n^2 + y_n^2
\]

\[
= 0
\]

by the induction hypothesis.

**Exercise 5:** (⋆) 4 points

Show that the Diophantine equation \( x^4 - y^4 = z^2 \) has no solutions in nonzero integers using the method of Fermat’s descent.

**Solution:**

Suppose \( x, y, z \) is a solution, so we may assume \( (x, y) = 1 \). Suppose \( x_0, y_0, z_0 \) is a solution with \( \gcd(x_0, y_0) = 1 \), then we want to find another solution \( x_1, y_1, z_1 \) with \( x_1 < x_0 \) and \( \gcd(x_1, y_1) = 1 \). Since \( x_0^4 = z_0^2 + y_0^4 \), we know \( (z_0, y_0^2, x_0^2) \) is a PPT so there are \( m, n \) with \( m > n \), \( \gcd(m, n) = 1 \), \( m \not\equiv n \mod 2 \) and either

1. \( z_0 = m^2 - n^2, \quad y_0^2 = 2mn, \quad x_0^2 = m^2 + n^2 \)

2. \( z_0 = 2mn, \quad y_0 = m^2 - n^2, \quad x_0^2 = m^2 + n^2 \)
In case 1), \(x_0 = m^2 + n^2\), so \((m, n, x_0)\) is a PPT and since one of \(m, n\) is even, WLOG \(n\) is even. So there are \(r, s\) with \(\gcd(r, s) = 1\), \(r \not\equiv s \mod 2\) and
\[
m = r^2 - s^2, \quad n = 2rs, \quad x_0 = r^2 + s^2.
\]

Now \(y_0^2 = 2mn\) and since \(\gcd(m, n) = 1\) and \(m\) odd, we have \(\gcd(m, 2m) = 1\), and since they product is a square, there are \(z_1\) and \(k\) with \(m = z_1^2, 2n = k^2\), so \(k\) is even. So let \(k = 2l\) then \(2n = (2l)^2\) then \(n = 2l^2 = 2rs\), then \(l = rs\) and \((r, s) = 1\). Then, there are \(x_1\) and \(y_1\) such that \(x_1^2 = r, y_1^2 = s\) (so \((x_1, y_1) = 1\)) and now \(z_1^2 = m = r^2 - s^2 = (x_1^2)^2 - (y_1^2)^2 = x_1^4 - y_1^4\) and \(r < x_0\) and \(x_1 \leq r\) then \(x_1 < x_0\).

\(^1(\ast) = \text{easy}, (\ast\ast)= \text{medium}, (\ast\ast\ast)= \text{challenge}\)