Sommersemester 2025 Blatt 10

1. Questions

(1) Consider the equation
$$x^2 - dy^2 = -1.$$
   (a) Show that if $d \leq 0$, then this equation does not have any integer solutions.
   (b) Show that if d is divisible by 4, then this equation does not have any integer solutions.
   (c) Show that if d is divisible by a prime p of the form $p = 4k + 3$ for some integer k, then this equation does not have any integer solutions.
   (d) Assume that $d \neq c^2$ for any positive integer c. Show that if $(u, v) \in \mathbb{Z}^2$ is a solution to our equation, then every solution is of the form
$$(u\alpha - dv\beta, v\alpha - u\beta)$$
   where (α, β) runs through all solutions of $x^2 - dy^2 = +1$.

(2) Use Dirichlet's Approximation Theorem to prove Thue's Lemma.

2. Comments

(1) (a) The first part should not require any hints.
   (b) Show that if a is any positive integer, $a^2 = 0$ or $a^2 = 1$ modulo 4. Then, use this to show there are no solutions if d is divisible by 4.
   (c) If d is divisible by p, show that you have $x^2 = -1$ modulo p. When does this have a solution?

(2) (a) Let us recall Dirichlet's Approximation Theorem: Let $\alpha \in \mathbb{R}$ and N be a positive integer greater than 1. Then, there exist integers p, q with $1 \leq q < N$ and $|\alpha q - p| \leq \frac{1}{N}$. If α is irrational, there are infinitely many $p, q \in \mathbb{Z}$ such that $\gcd(p, q) = 1$ and such that $|\alpha q - p| < \frac{1}{p}$.
   (b) Let us recall Thue's Lemma: Let p be an odd prime. Let a, p be positive integers with $\gcd(a, p) = 1$. Then, the congruence
$$ay = x \mod p$$
   has a solution (x_0, y_0) satisfying $0 < |x_0| < \sqrt{p}$ and $0 < |y_0| < \sqrt{p}$.
   (c) Now, first apply the first part of Dirichlet's formula to $\alpha = a/p$ and $N = \lceil \sqrt{p} \rceil$ to get some solution (P, Q).