# **Math 530**: Problem Set 10

**Due date:** In class on Wednesday, April 29.
**Course Web Page:** `http://dunfield.info/530`

1. Let $q$ be a non-degenerate quadratic form on $\mathbb{Q}_p^n$. For $a \in \mathbb{Q}_p^\times$, show that $q$ represents $a$ if and only if:

   (a) $n = 1$ and $a = d$,

   (b) $n = 2$ and $(a, -d) = \epsilon$,

   (c) $n = 3$ and either $a \neq -d$ or ($a = -d$ and $(-1, -d) = \epsilon$),

   (d) $n \geq 4$.

   Here, equalities between $a$ and $d$ are as elements of $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$.

2. Show that, up to isometry, there is a unique quadratic form on $\mathbb{Q}_p^4$ which does not represent 0, namely the form $x^2 - ay^2 - bz^2 + abt^2$, where $a$ and $b$ are such that $(a, b) = -1$.

3. A quadratic form $q$ on $\mathbb{Q}^k$ is *matrix-integral* if there exists a basis in which the Gramm matrix of the associated bilinear form has integral entries. The form $q$ is *positive definite* if it is equivalent over $\mathbb{R}$ to $x_1^2 + \cdots + x_k^2$.

   Let $q$ be a positive definite matrix-integral quadratic form on $\mathbb{Q}^k$, and fix a basis where the Gramm matrix of $q$ is integral. Assume that for every $x \in \mathbb{Q}^k$ there is a $y \in \mathbb{Z}^k$ such that $q(x - y) < 1$. Fix $n$ in $\mathbb{Z}$. Prove that if $q$ represents $n$ on $\mathbb{Q}^k$ it also does so on $\mathbb{Z}^k$.

4. Combine Problem 3 with the Hasse-Minkowski Theorem to prove the following classical result of Fermat:

   Let $n \in \mathbb{N}$. The following conditions are equivalent:

   (a) The integer $n$ is the sum of two squares of elements of $\mathbb{Z}$.

   (b) The integer $n$ is the sum of two squares of elements of $\mathbb{Q}$.

   (c) For every prime factor $p$ of $n$ such that $p \equiv 3 \pmod 4$, we have $v_p(n)$ is even. (Here $v_p(n)$ is the exponent of $p$ in the factorization of $n$.)