p-adic Numbers and the Hasse Principle

Otmar Venjakob

ABSTRACT

Hasse's local-global principle is the idea that one can find an integer solution to an equation by using the Chinese remainder theorem to piece together solutions modulo powers of each different prime number. This is handled by examining the equation in the completions of the rational numbers: the real numbers and the p-adic numbers. A more formal version of the Hasse principle states that certain types of equations have a rational solution if and only if they have a solution in the real numbers and in the p-adic numbers for each prime p. The aim of this course is to give firstly an introduction into p-adic numbers and analysis (different constructions of p-adic integers) and secondly to apply them to study Diophantine equations. In particular we will sketch the proof of the local-global principles for quadratic forms, i.e., of the HasseMinkowski theorem, and discuss a counter example for cubic forms.

Finally, we want to point out that - while the above results are classical - p-adic methods still play a crucial role in modern arithmetic geometry, i.e., in areas like p-adic Hodge theory, p-adic representation theory/p-adic local Langlands or Iwasawa theory.

1. Diophantine equations

$f_i(X_1, \dots, X_r) \in \mathbb{Z}[X_1, \dots, X_r]$ polynomials with coefficients in $\mathbb{Z}$.

Consider the system of diophantine equations

$$\begin{array}{lll} f_1(X_1, \dots, X_r) & = 0 & \\ \vdots & \vdots & \text{(S)} \\ f_n(X_1, \dots, X_r) & = 0 & \end{array}$$

Theorem 1.1. *Assume that (S) is linear, i.e. deg* $(f_i) = 1$ *for all* $1 \leq i \leq n$. *Then*

(i) *there exists a solution* $a = (a_1, \dots, a_r) \in \mathbb{Z}^r$ *of (S) in the integers if and only if*
(ii) *there exists a solution* $\bar{a} = (\bar{a}_1, \dots, \bar{a}_r) \in (\mathbb{Z}/m)^r$ *of (S) modulo* m *for any natural number* $m \in \mathbb{N}$.
(iii) *for each prime number* p *and each natural number* $m \in \mathbb{N}$ *there exists a solution* $\bar{a} = (\bar{a}_1, \dots, \bar{a}_r) \in (\mathbb{Z}/p^m)^r$.

Proof.
$(i) \Longleftrightarrow (ii)$ exercise
$(ii) \Longleftrightarrow (iii)$ Chinese remainder theorem:

If $m = p_1^{n_1} \dots p_r^{n_r}$, then there is a canonical isomorphism of rings

$$\begin{array}{rl} \mathbb{Z}/m & \xrightarrow{\cong} \prod_{i=1}^{r} \mathbb{Z}/p_i^{n_i} \\ a \mod m & \longrightarrow (a \mod p_i^{n_i})_i \end{array}$$

□

Fix a prime p and consider the projective system

$$\begin{array}{lll} \ldots & \to \mathbb{Z}/p^3\mathbb{Z} & \twoheadrightarrow \mathbb{Z}/p^2\mathbb{Z} \quad \twoheadrightarrow \mathbb{Z}/p\mathbb{Z} \\ & a \mod p^3 & \mapsto a \mod p^2 \quad \mapsto a \mod p \end{array}$$

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n \,|\, a_{n+1} \equiv a_n \mod p^n \text{ for all } n \in \mathbb{N} \right\}$$

is called ring of p-adic integers with

$$\begin{array}{rl} (a_n) + (b_n) & := (a_n + b_n) \\ (a_n) \cdot (b_n) & := (a_n\, b_n) \end{array}$$

$\mathbb{Z}_p$ is compact (Tychonoff!).

Fact 1.2. *Any $N \in \mathbb{N}$ has a unique p-adic expansion*

$$N = a_0 + a_1 p + \ldots + a_n p^n$$

with $a_i \in \{0, 1, \ldots, p-1\}$ (use successively division by p with rest

$$\begin{array}{rl} N & = a_0 + pN_1 \\ N_1 & = a_1 + pN_2 \\ & \vdots \\ N_{n-1} & = a_{n-1} + pN_n \\ N_n & = a_n \end{array}$$

$$\begin{array}{rl} \mathbb{Z} & \xrightarrow{\iota} \mathbb{Z}_p \\ N & \mapsto (N \bmod p^n)_{n\in\mathbb{N}} \end{array}$$

With increasing n we see more "digits", more a_i, of our expansion.

$$N = a_0 + a_1 p + \ldots + a_n p^n.$$

ι is injective:

$$\begin{array}{rrl} \text{if} & N & \equiv 0 \bmod p^n, \text{i.e. } p^n | N \text{ for } n \text{ arbitrary,} \\ \text{then} & N & = 0 \text{ must hold.} \end{array}$$

Copying decimal numbers

$$0,1\,2\,3\,4\ldots \qquad\qquad \sum_{i=-M}^{\infty} a_i 10^{-i}, \quad a_i \in \{0, \ldots, 9\}$$

can we make sense to expression like

$$(p=3) \qquad 1+3+3^2+3^3+\ldots$$

$$\sum_{i=0}^{+\infty} a_i p^i, \quad a_i \in \{0,1,\ldots,p-1\}$$

$$\frac{p^i-1}{p-1}, \ i \mapsto \infty$$

Definition 1.3.

$$v_p(a) = \begin{cases} n & , \textit{if} \quad a = p^n u \neq 0, \ (p,u)=1 \\ \infty & \quad a = 0 \end{cases}$$

$v_p : \mathbb{Q} \longrightarrow \mathbb{Z}$ *(p-adic valuation)*

$|\cdot|_p \colon \mathbb{Q} \longrightarrow \mathbb{R}^{\geq 0}$ *(p-adic norm)*

$$|\ a\ |_p := \begin{cases} p^{-v_p(a)} & , a \neq 0 \\ 0 & , a = 0 \end{cases}$$

"a is small if and only if $p^n | a$ for n big"

Lemma 1.4. *For all $x, y \in \mathbb{Q}$ we have*

(i) $v_p(xy) = v_p(x) + v_p(y)$ *and* $|xy|_p = |x|_p |y|_p$,

(ii) $v_p(x+y) \geq min(v_p(x), v_p(y))$ *and* $|x+y|_p \leq max(|x|_p, |y|_p)$,

(iii) *if* $v_p(x) \neq v_p(y)$ (*respectively* $|x|_p \neq |y|_p$) *in (ii), then "=" holds.*

Example 1.5. With respect to $|\cdot|_p$ the sequence $a_n = p^n$ converges against 0

$$\left(\text{hence } \frac{p^i-1}{p-1} \longrightarrow \frac{-1}{p-1}\right)$$

Recall

$$\mathbb{R} = (\mathbb{Q}, |\cdot|_\infty)^\wedge$$

is the completion with respect to (w.r.t.) usual absolute value $|\cdot|_\infty$, e.g. constructed via space of Cauchy-sequences.

Definition 1.6.

$$\mathbb{Q}_p := (\mathbb{Q}, |\cdot|_p)^\wedge := \{(x_n)_n | x_n \in \mathbb{Q},\ \textit{Cauchy-sequence w.r.t. } |\cdot|_p\} / \sim$$

$$(x_i)_{i\in\mathbb{N}} \sim (y_i)_{i\in\mathbb{N}} :\Longleftrightarrow |x_i - y_i|_p \to 0 \textit{ for } i \mapsto \infty,\ \textit{ i.e.,}$$

where $x_i - y_i$ is a p-adic zero-sequence

The operations on Cauchy-sequences

$$\begin{array}{rl} (x_n)\cdot(y_n) & := (x_n \cdot y_n) \\ (x_n)+(y_n) & := (x_n + y_n) \quad \textit{induce the structure of a field on } \mathbb{Q}_p! \end{array}$$

$|\cdot|_p$ and v_p extend naturally to $\mathbb{Q}_p$:

$$|(x_n)|_p := \lim_{n\mapsto\infty} |x_n|_p, \quad v_p((x_n)) := \lim_{n\mapsto\infty} v_p(x_n)$$

(the latter becomes stationary, if (x_n) is not a zero-sequence!)

In particular, $\mathbb{Q}_p$ is a normed topological space.

Theorem 1.7. *(p-adic version of Bolzano-Weierstraß)*

$\mathbb{Q}_p$ is complete, i.e. each Cauchy-sequence in $\mathbb{Q}_p$ converges in $\mathbb{Q}_p$. Any bounded sequence has a accumulation point. Any closed and bounded subset of $\mathbb{Q}_p$ is compact.

Warning: $\mathbb{Q}_p$ is not ordered like $(\mathbb{R}, \geq)$!

Theorem 1.8. *(Ostrowski)*

Any valuation on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.

$$\left(\begin{array}{rcl} |\cdot|_1 \sim |\cdot|_2 & :\Leftrightarrow & \textit{they define the same topology on } \mathbb{Q} \\ & \Leftrightarrow & |\cdot|_1 = |\cdot|_2^s \textit{ for some } s \in \mathbb{R}^{>0}) \end{array} \right)$$

Theorem 1.9.

(i) $\mathbb{Z}_p = \{x \in \mathbb{Q}_p |\ |x|_p \leq 1\}$ *and* $\mathbb{Z} \subset \mathbb{Z}_p$ *is dense.*
(ii) $\mathbb{Z}_p$ *is a discrete valuation ring (dvr), i.e.* $\mathbb{Z}_p \setminus \mathbb{Z}_p^\times = p\mathbb{Z}_p$, *where* $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p |\ |x|_p = 1\}$ *denotes the group of units of* $\mathbb{Z}_p$.

Theorem 1.10. *There are a canonical isomomorphisms*

$$\mathbb{Z} \times \mathbb{Z}_p^\times \cong \mathbb{Q}_p^\times,\ \ (n,u) \mapsto p^n u,$$

$$\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p),$$

$$1 + p\mathbb{Z}_p \cong \left\{ \begin{array}{ll} \mathbb{Z}_p, & \textit{if } p \neq 2; \\ \{\pm 1\} \times (1 + 4\mathbb{Z}_2) \cong \{\pm 1\} \times \mathbb{Z}_2, & \textit{otherwise.} \end{array} \right.$$

Corollary 1.11. *There is a canonical isomorphism*

$$\mathbb{Q}_p^\times \cong \begin{cases} \mathbb{Z}\times\mathbb{Z}/(p-1)\times\mathbb{Z}_p, & \text{if } p\neq 2; \\ \mathbb{Z}\times\mathbb{Z}/2\times\mathbb{Z}_2, & \text{otherwise.} \end{cases}$$

Corollary 1.12. *$a = p^n u \in \mathbb{Q}_p^\times$ with $u \in \mathbb{Z}_p^\times$ is a square in $\mathbb{Q}_p^\times$, if and only if the following conditions hold:*

(1) *n is even,*

(2) $\begin{cases} \bar{u} \text{ is a square in } \mathbb{F}_p^\times, & \text{if } p\neq 2; \\ u \equiv 1 \mod 8\mathbb{Z}_2, & p=2. \end{cases}$

2. Conics, quadratic forms and residue symbols

2.1. **Conics.** Consider the conic

$$(C)\ \ ax^2+by^2=c \quad (a,b,c\in\mathbb{Q}^\times)$$

When is $C(\mathbb{Q}) := \{(x,y)\in\mathbb{Q}^2 \mid ax^2+by^2=c\}$ non empty, i.e. when does C have a *rational* point? Without loss of generality we may assume: $c=1$

Define

$$(a,b)_\infty = \begin{cases} 1 & \text{if } a>0 \text{ or } b>0 \\ -1 & \text{if } a<0 \text{ and } b<0 \end{cases}$$

Property:

$(a,b)_\infty = 1 \Longleftrightarrow$ There exists $(x,y)\in\mathbb{R}^2$ such that $ax^2+by^2=1$

Now let p be a prime number.

Aim:

To define similarly

$$(-,-)_p : \mathbb{Q}^\times\times\mathbb{Q}^\times \longrightarrow \{\pm 1\}$$

such that the following holds

$(a,b)_p = 1 \Longleftrightarrow$ There exists $(x,y)\in\mathbb{Q}_p^2$ such that $ax^2+by^2=1$

2.2. **Quadratic reciprocity law.** p odd

$$\begin{array}{rcl} \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 & \cong & \{\pm 1\} \\ a & \mapsto & \left(\frac{a}{p}\right) \end{array}$$

$$\text{i.e.} \quad \left(\frac{a}{p}\right) = 1 \quad \Leftrightarrow \quad \text{There exists } x \in \mathbb{Z} \text{ s.t. } x^2 \equiv a \bmod p$$

$$\text{Otherwise} \quad \left(\frac{a}{p}\right) = -1.$$

Theorem 2.1. *Let $p \neq q$ be odd primes.*

(1) *(Quadratic reciprocity law)*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right),$$

(2) *(first supplementary law)*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \mod 4; \\ -1, & p \equiv 3 \mod 4. \end{cases}$$

(3) *(second supplementary law)*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv 1, 7 \mod 8; \\ -1, & p \equiv 3, 5 \mod 8. \end{cases}$$

Define the **Hilbert symbol**

$$(\ ,\ )_p : \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \longrightarrow \{\pm 1\}$$

as follows:
For $a, b \in \mathbb{Q}_p^\times$ write

$$a = p^i u,\ b = p^j v \ \ (i, j \in \mathbb{Z}, u, v \in \mathbb{Z}_p^\times, (u, p) = (v, p) = 1)$$

and put

$$r = (-1)^{ij} a^j b^{-i} = (-1)^{ij} u^j v^{-i} \in \mathbb{Z}_p^\times$$

p odd:

$$(a, b)_p := \left(\frac{r}{p}\right) := \left(\frac{\overline{r}}{p}\right)$$

where $\overline{r}$ denotes the image of r under the $\bmod_p$ reduction

$$^- : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times.$$

p = 2

$$(a, b)_2 := (-1)^{\frac{r^2-1}{8}} \cdot (-1)^{\frac{u-1}{2} \cdot \frac{v-1}{2}}$$

Proposition 2.2. *For $v \in V$ and $a, b, c \in \mathbb{Q}^\times$ we have*

(1) $(a, b)_v = (b, a)_v$
(2) $(a, bc)_v = (a, b)_v (a, b)_v$,

(3) $(a,-a)_v = 1$ *and* $(a,1-a)_v = 1$ *if* $a \neq 1$,
(4) *if* $p \neq 2$ *and* $a, b \in \mathbb{Z}_p^\times$, *then*
  (a) $(a,b)_v = 1$,
  (b) $(a,pb) = \left(\frac{a}{p}\right)$,
(5) *if* $a, b \in \mathbb{Z}_2$, *then*
  (a) $(a,b)_2 = \begin{cases} 1, & \text{if } a \text{ or } b \equiv 1 \mod 4; \\ -1, & \text{otherwise.} \end{cases}$
  (b) $(a,2b)_2 = \begin{cases} 1, & \text{if } a \text{ or } a+2b \equiv 1 \mod 8; \\ -1, & \text{otherwise.} \end{cases}$

Proposition 2.3. *For* $a, b \in \mathbb{Q}_p^\times$ *the following conditions are equivalent:*
(1) $(a,b)_v = 1$
(2) *there exist* $x, y \in \mathbb{Q}_p^\times$ *such that* $ax^2 + by^2 = 1$.

Set $\mathbb{Q}_\infty := \mathbb{R}$ and $V := \{p|\text{prime}\} \cup \{\infty\}$

Theorem 2.4. *(Hilbert product formula)* $a, b \in \mathbb{Q}^\times$. *Then* $(a,b)_v, v \in V$, *is equal to 1 except for a finite number of* v, *and we have*

$$\prod_{v \in V} (a,b)_v = 1$$

Consider the cone

$$C : ax^2 + by^2 = 1 \ ; \ a, b \in \mathbb{Q}^\times$$

Theorem 2.5. *The following statements are equivalent:*
(i) $C(\mathbb{Q}) \neq \emptyset$,
(ii) $C(\mathbb{Q}_v) \neq \emptyset$ *for all* $v \in V$,
(iii) $(a,b)_v = 1$ *for all* $v \in V$.

3. Generalisation to quadratic forms of higher rank

Let W be finite dimensional vector space over field k.

Definition 3.1. *A function* $Q : W \to k$ *is called quadratic form on* W *if*
(i) $Q(ax) = a^2 Q(x)$ *for* $a \in k, x \in W$ *and*
(ii) $(x,y) \mapsto Q(x+y) - Q(x) - Q(y)$ *define a bilinear form.*

(W, Q) *is called* **quadratic space**.

If $char(k) \neq 2$, setting

$$< x, y >:= \frac{1}{2}\{Q(x+y) - Q(x) - Q(y)\}$$

defines a symmetric bilinear form, the *scalar product* associated with Q, such that

$$Q(x) =< x, x >$$

$$\begin{array}{ccc} \{\text{quadratic forms}\} & \overset{1:1}{\longleftrightarrow} & \{\text{symmetric bilinear forms}\} \\ Q & \mapsto & < \ , \ > \end{array}$$

Matrix of Q:

$W = \overset{n}{\underset{i=1}{\oplus}} ke_i \cong k^n$, $A = (a_{ij})$ with $a_{ij} =< e_i, e_j >$

is symmetric and for $x = \sum x_i e_i$ we have

$$Q(x) = \sum_{i,j} a_{ij} x_i x_j = {}^t x A x$$

- $d(Q)$, the image of det(A) in $k^\times/(k^\times)^2 \cup \{0\}$, is called *discriminant* of Q.
- $rk(Q)$, the rank of A, is called *rank* of Q.
- Q is called *non-degenerate*, if $rk(Q) = n$ holds $\big($whence $d(Q) \in k^\times/(k^\times)^2\big)$.
- Q *represents* $a \in k$, if there exists $0 \neq w \in W$ such that $Q(w) = a$.
- (Q', k^n) and (Q, k^n) are *equivalent*, $Q' \sim Q$, if there exists $S \in GL_n(k)$ such that

$$Q'x = Q(Sx) \text{ for all } x \in k^n$$

or equivalently

$$A' = {}^t SAS.$$

Remark 3.2.

(i) $X_1 X_2 \sim X_1^2 - X_2^2$, *because* $(X_1 + X_2)(X_1 - X_2) = X_1^2 - X_2^2$,

(ii) $aX_1^2 \sim bX_1^2 \Leftrightarrow a = bc^2$ *for some* $c \in k^\times$,

(iii) $Q(X_1, \ldots, X_n) \sim Q(X_{\pi(1)}, \ldots, X_{\pi(n)})$ *for any* $\pi \in S_n$ *(symmetric group on* n *elements),*

(iv) *If* $Q \sim Q'$*, then* Q *represents* $a \in k$ *if and only if* Q' *does.*

Proposition 3.3. $(Q, k^n), a \in k^\times$

(i) *If* Q *represents* a*, then* $Q \sim aX_1^2 + G(x_2, \ldots, x_n)$ *for some quadratic space* (G, k^{n-1}).

(ii) $Q \sim a_1X_1^2 + \ldots + a_nX_n^2 =: < a_1, \ldots, a_n >$ *for some* $a_i \in k$.

(iii) *If* Q *is non-degenerate and represents* 0*, then* $Q(W) = k$*, i.e. it represents each* $a \in k$.

(iv) *Let* Q *be non-degenerate. Then* Q *represents* a *if and only if*

$$Q(X_1, \ldots, X_n) - aX_{n+1}^2$$

represents 0.

(v) *Let* Q *be non-degenerate. If* Q *represents* 0*, than*

$$Q \sim X_1X_2 + G(X_3, \ldots, X_n)$$

for some quadratic space (G, k^{n-2}).
(X_1X_2, k^2) *(and any quadratic space equivalent to it) is called* hyperbolic space.

For quadratic spaces $(Q, k^n), (Q', k^m)$ let $(Q \perp Q', k^{n+m})$ be the quadratic space defined by

$$(Q \perp Q')(X_1, \ldots, X_{n+m}) = Q(X_1, \ldots, X_1) + Q'(X_{n+1}, \ldots, X_{n+m})$$

Theorem 3.4. *(Witt's cancelation theorem)*

For $(Q, k^n), (Q', k^n), (G, k^m)$ *quadratic spaces it holds*

$$Q \perp G \sim Q' \perp G \Rightarrow Q \sim Q'$$

Corollary 3.5. *If* Q *is non-degenerate, then (uniquely up to equivalence)*

$$Q \sim G_1 \perp G_2 \perp \ldots \perp G_m \perp H$$

with G_i *hyperbolic and* H *does not represent* 0.

3.1. **Quadratic forms over the reals.**
Let $(Q, \mathbb{R}^m)$ be of $rk(Q) = n \leq m$

then

$$Q \sim X_1^2 + \ \dots \ + X_r^2 - (Y_1^2 + \ \dots \ + Y_s^2) \qquad =< \underbrace{1, \ \dots \ , 1}_{r \ times}, \ \underbrace{-1, \ \dots \ -1}_{s \ times}, \ 0, \dots, 0 >$$
$$=< a_1, \ \dots \ a_n >$$

with $r + s = n$ and (r, s) is the *signature* of Q.

$$Q \text{ is called } \begin{array}{ll} \textit{definite}, & \text{if } r = 0 \text{ or } s = 0 \\ \textit{indefinite}, & \text{otherwise.} \end{array}$$

$$\varepsilon(Q) := \prod_{i<j} (a_i, a_j)_\infty = (-1)^{\frac{s(s-1)}{2}} = \begin{cases} 1 & \text{if } s \equiv 0, 1 \bmod 4 \\ -1 & \text{if } s \equiv 2, 3 \bmod 4 \end{cases}$$

$$d(Q) = (-1)^s = \begin{cases} 1 & \text{if } s \equiv 0 \bmod 2 \\ -1 & \text{if } s \equiv 1 \bmod 2 \end{cases}$$

3.2. **Quadratic forms over $\mathbb{F}_q$.**
$q = p^t$, $\mathbb{F}_q$ field of q elements

Proposition 3.6. *$(Q, \mathbb{F}_q^m)$ of $rk(Q) = n$*

(i) *Q represents $\mathbb{F}_q^\times$ and $\mathbb{F}_q$, if $n \geq 2$ and $n \geq 3$, respectively.*

(ii) *If Q is non-degenerate, then*

$$Q \sim \begin{cases} < 1, \ \dots \ , 1, 1 > & \textit{if } d(Q) \in (\mathbb{F}_q^\times)^2 \\ < 1, \ \dots \ , 1, a > & \textit{otherwise,} \end{cases}$$

i.e. $rk(Q)$ and $d(Q)$ determine the equivalence class of Q uniquely.

3.3. **Quadratic forms over $\mathbb{Q}_p$.**
For $Q \sim < a_1, \ \dots \ , a_n >$ the Hilbert symbol

$$\varepsilon(Q) := \prod_{i<j} (a_i, a_j)_p$$

is well defined!

Theorem 3.7. *(Q, k^n) non-degenerate, $d = d(Q), \varepsilon = \varepsilon(Q)$*
Then Q represents $0 \Leftrightarrow$

(i) *$n = 2$ and $d = -1$ in $k^\times/(k^\times)^2$*

(ii) *$n = 3$ and $(-1, -d)_p = \varepsilon$*

(iii) *$n = 4$ and either $d \neq 1$ or $d = 1$ and $\varepsilon = (-1, -1)_p$*

(iv) *$n \geq 5$*

Corollary 3.8. *Q represents $a \in k^\times/(k^\times)^2$ if and only if*

(1) *$n = 1$ and $a = d$,*
(2) *$n = 2$ and $(a, d) = \varepsilon$,*
(3) *$n = 3$ and either $a \neq -d$ or $a = -d$ and $(-1, -d) = \varepsilon$,*
(4) *$n \geq 4$.*

Theorem 3.9. *The equivalence class of Q is uniquely determined by its invariants $rk(Q), d(Q), \varepsilon(Q)$.*

3.4. **Quadratic forms over $\mathbb{Q}$.**

$(Q, \mathbb{Q}^n)$ non-degenerate quadratic space

$Q \sim < a_1, \ \ldots \ , a_n >$ has invariants

- $d(Q) = a_1, \cdot \ \ldots \ \cdot a_n \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$
- Consider the quadratic form Q_v over $\mathbb{Q}_v$ induced from Q via $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$

$$\begin{array}{lll} d_v(Q) := & d(Q_v) & \text{image of } d(Q) \text{ in } \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2 \\ \varepsilon_v(\mathbb{Q}) := & \varepsilon(Q_v) = & \prod\limits_{i<j} (a_i, a_j)_v \end{array}$$

  $(\Rightarrow \prod\limits_{v \in V} \varepsilon_v(Q) = 1)$
- (r, s) signature of Q_∞

Theorem 3.10. *(Hasse-Minkowski)*

$$Q \text{ represents } 0 \Leftrightarrow Q_v \text{ represents } 0 \text{ for all } v \in V.$$

Corollary 3.11. *Let a be in $\mathbb{Q}^\times$.*

$$Q \text{ represents } a \Leftrightarrow Q_v \text{ represents } a \text{ for all } v \in V$$

Theorem 3.12. *(Classification) $(Q, \mathbb{Q}^n), (Q', \mathbb{Q}^n)$*

$$\begin{array}{ll} Q \sim Q' & \Leftrightarrow Q_v \sim Q_v' \text{ for all } v \in V \\ & \Leftrightarrow d(Q) = d(Q'), (r, s) = (r', s') \text{ and } \varepsilon_v(Q) = \varepsilon_v(Q') \text{ for all } v \in V. \end{array}$$

Remark 3.13. *$d = d(Q)$, $\epsilon_v = \epsilon_v(Q)$ and (r, s) satisfy the following relations:*

(1) *$\varepsilon_v = 1$ for almost all $v \in V$ and $\prod_{v \in V} \varepsilon_v = 1$,*
(2) *$\varepsilon_v = 1$ if $n = 1$ of if $n = 2$ and if the image d_v of d in $\mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$ equals -1,*
(3) *$r, s \geq 0$ and $r + s = n$,*
(4) *$d_\infty = (-1)^s$,*

(5) $\varepsilon_\infty = (-1)^{\frac{s(s-1)}{2}}$.

Conversely:

Proposition 3.14. *If the above relations are satisfied for d, $(\varepsilon_v)_{v\in V}$, and (r,s) then there exists a quadratic form Q which has the corresponding invariants.*

4. Failure of local-global principal and generalisations

Theorem 4.1. *(Lind, Reichardt) $X^4 - 17 = 2Y^2$ has solutions in $\mathbb{R}, \mathbb{Q}_p$ all p, but not in $\mathbb{Q}$!*

(see [2] § 3.5)

- **cohomological interpretation:**(see [4, chapter X])

Over a field k the first Galois cohomology group (with non-abelian coefficients)

$$\mathrm{H}^1(k, O_n)$$

classifies isomorphism classes of non-degenerate quadratic forms of rank n over k. Theorem 3.12 translates as follows:

The canonical global to local map

$$\mathrm{H}^1(\mathbb{Q}, O_n) \hookrightarrow \prod_{v\in V} \mathrm{H}^1(\mathbb{Q}_v, O_n)$$

is injective! This is not true in general for connected linear algebraic groups G instead of O_n.

- **Brauer group**

$Br(k) = H^2(k, (k^{sep})^\times)$ classifies classes of central simple algebras (finite dimensional k-algebras, isomorphic to $M_n(D)$ for some division algebra D with center k and some n) over k; A is equivalent to A' per definition if $D \cong D'$ over k.

Class field theory leads to the injectivity of the canonical global to local map

$$Br(\mathbb{Q}) \hookrightarrow \prod_{v\in V} Br(\mathbb{Q}_v)$$

- **elliptic curves, Selmer/Tate-Shafarevich group** (see [5, §X.3])

Let E be an ellipic curve over a field k ($\mathrm{char}(k) = 0$) and $E(\bar{k})$ its points over an algebraic closure. Then

$$\mathrm{H}^1(k, E(\bar{k}))$$

classifies equivalence classes of homogeneous spaces for E/k (a homogeneous space is a smooth curve C/k with a transitive algebraic group action of E on C defined over k)

The canonical global to local map

$$\mathrm{H}^1(\mathbb{Q}, E(\bar{\mathbb{Q}})) \to \prod_{v\in V} \mathrm{H}^1(\mathbb{Q}_v, E(\overline{\mathbb{Q}_v}))$$

is in general not injective, its kernel $Ш(\mathbb{Q}, E)$ is called Tate-Shafarevich group. Tate has conjectured that it is 'at least' finite. We have the following fact:

A homogeneous space C/k for E/k is in the trivial equivalence class, i.e., equivalent to E/k, if and only if $C(k)$ is non-empty, i.e., C has a k-rational point.

5. Exercises

I.

1. Calculate $\sum_{i=0}^{\infty}(-5)^i$ and expand -1, $\frac{2}{3}$, $-\frac{2}{3}$ (5-adically).
2. Find the inverse of 4 in $Z/3^4\mathbb{Z}$.
3. For $n = a_0 + a_1 p \cdots a_{r-1}p^{r-1} \geq 0$ in its p-adic expansion show that

$$v_p(n!) = \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right] = \frac{n-s}{p-1},$$

where $[x]$ denotes the Gauss symbol, i.e. largest integer less than or equal to x, and $s := a_0 + a_1 + \cdots a_{r-1}$.

4. $a \in \mathbb{Z}$ with $a \equiv \pm 1 \bmod 5$. Show that there exist a square root of a in $\mathbb{Q}_5$.

5. Show that -1 has a square root in $\mathbb{Q}_p$ if and only if $p \equiv 1 \bmod 4$.

6. Show that if $p \neq 2$, there exist exactly 3 quadratic extensions of $\mathbb{Q}_p$. Determine them for $p = 5$.

7. Show that $\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X-p)$, where $\mathbb{Z}[[X]]$ denotes the ring of formal power series over $\mathbb{Z}$.

8. Show that a p-adic number $a = \sum_{\nu=-m}^{\infty} a_\nu p^\nu$ is in $\mathbb{Q}$ if and only if the sequence a_ν is periodic for ν big enough.

9. Show that an integral p-adic number $a = \sum_{\nu=0}^{\infty} a_\nu p^\nu$ is a unit in $\mathbb{Z}_p$ if and only if $a_0 \neq 0$.

II.

1. Let p be a prime number. Show the following

   (i) $X^2 = -2$ has a solution in $\mathbb{Q}_p \Leftrightarrow p \equiv 1, 3 \bmod 8$.

   (ii) $X^2 + Y^2 = -2$ has a solution in $\mathbb{Q}_p \Leftrightarrow p \neq 2$.

   (iii) $X^2 + Y^2 + Z^2 = -2$ has a solution in $\mathbb{Q}_p$ for any p.

2. Prove proposition 3.3.
3. Prove the following theorem of Gauß: A natural number n is the sum of three quare numbers, if $n \neq 4^a(8b+7)$ for all integers $a, b \geq 0$. To this end assume the (non-trivial) fact that the natural number n is the sum of three square numbers in $\mathbb{Z}$ if and only if it is the sum of three square numbers in $\mathbb{Q}$.

References

[1] K. Kato, N. Kurokawa, T. Saito, *Number Theory I - Fermat's Dream*, Translations of Mathematical Monographs 186, AMS
[2] A. Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer
[3] J.P. Serre, *A course in arithmetic*, Springer
[4] J.P. Serre, *Local fields*, Springer
[5] J.H. Silverman, *The arithmetic of elliptic curves*, Springer