Since $\mathscr{X}(\mathbb{C})$ is compact, there is a positive constant D such that

$$\frac{1}{D} < \frac{\| . \|_2(x)}{\| . \|_1(x)} < D$$

for every $x \in \mathscr{X}(\mathbb{C})$. This implies the claim.

b) Clearly, for every $x \in \mathscr{X}(\mathbb{Q})$, one has

$$\begin{aligned} \mathrm{h}_{(\overline{\mathscr{L}_1} \otimes \overline{\mathscr{L}_2})}(x) = \widehat{\deg}\left(\overline{x}^*(\overline{\mathscr{L}_1} \otimes \overline{\mathscr{L}_2})\right) &= \widehat{\deg}\left((\overline{x}^*\overline{\mathscr{L}_1}) \otimes (\overline{x}^*\overline{\mathscr{L}_2})\right) \\ &= \widehat{\deg}\,(\overline{x}^*\overline{\mathscr{L}_1}) + \widehat{\deg}\,(\overline{x}^*\overline{\mathscr{L}_2}) = \mathrm{h}_{\overline{\mathscr{L}_1}}(x) + \mathrm{h}_{\overline{\mathscr{L}_2}}(x) \,. \end{aligned}$$

c) There is some $n \in \mathbb{N}$ such that $\mathscr{L}^{\otimes n}$ is very ample. Part b) shows that it suffices to verify the assertion for $\overline{\mathscr{L}}^{\otimes n}$. Thus, we may assume that $\mathscr{L}$ is very ample.

Let $i\colon X \hookrightarrow \mathbf{P}^n$ be the closed embedding induced by $\mathscr{L}$. Then $\mathscr{L} = i^*\mathscr{O}(1)$. It follows from Tietze's Theorem that there is a hermitian metric on $\mathscr{O}(1)$ such that $\overline{\mathscr{L}} = i^*\overline{\mathscr{O}(1)}$. Then $\mathrm{h}_{\overline{\mathscr{L}}}(x) = \mathrm{h}_{\overline{\mathscr{O}(1)}}(i(x))$. It, therefore, suffices to show fundamental finiteness for the height function $\mathrm{h}_{\overline{\mathscr{O}(1)}}$ on $\mathbf{P}^n(\mathbb{Q})$.

Part a) together with Observation 3.11 shows that $\mathrm{h}_{\overline{\mathscr{O}(1)}}$ differs from $\mathrm{h}_{\mathrm{naive}}$ by a bounded summand. Fact 1.3 yields the assertion. □

3.16. Remark. — It should be noted that there is a strong formal analogy of the concept of a height on an arithmetic variety to the concept of a degree in algebraic geometry over a ground field. The only obvious difference is that the role of the sections of an invertible sheaf is now played by small sections, say, of norm less than one. Nevertheless, it seems that the height of a point is actually some sort of arithmetic intersection number.

This is an idea that has been formalized first by S. Yu. Arakelov [**Ara**] for two-dimensional arithmetic varieties and later by H. Gillet and C. Soulé [**G/S90**] for arithmetic varieties of arbitrary dimension.

We will not give any details on arithmetic intersection theory here as this is not formally necessary for an understanding of the next chapters. To get an impression, the reader is advised to consult the articles [**G/S90, G/S92**] of H. Gillet and C. Soulé, the textbook [**S/A/B/K**], and the references therein. The article [**B/G/S**] is a good starting point, as well. It explains, in particular, how to construct a height not only for points but for algebraic cycles.

The particular case of the arithmetic intersection theory on a curve over a number field had been developed earlier. The articles of S. Yu. Arakelov [**Ara**] and G. Faltings [**Fa84**] present the point of view taken before around 1990, which is a bit different from today's.

4. The adelic Picard group

i. *The local case. Metrics induced by a model.*

4.1. — Let K be an algebraically closed valuation field. The cases we have in mind are $K = \overline{\mathbb{Q}}_p$ for a prime number p and $K = \overline{\mathbb{Q}}_\infty = \mathbb{C}$.

We will denote the valuation of $x \in K$ by $|x|$. In the case $K = \overline{\mathbb{Q}}_p$, we assume that $|\,.\,|$ is normalized by $|p| = \frac{1}{p}$. We also write $\nu(x) := -\log|x|$.

4.2. Definition. — Let X be a K-scheme. Then, by a *metric* on an invertible sheaf $\mathscr{L} \in \operatorname{Pic}(X)$, we mean a system of K-norms on the K-vector spaces $\mathscr{L}(x)$ for $x \in X(K)$.

This means, to every point $x \in X(K)$ there is associated a function $\|\,.\,\|\colon \mathscr{L}(x) \to \mathbb{R}_+$ such that

i) $\forall x \in X(K)\ \forall y \in \mathscr{L}(x)\colon \|y\| = 0 \Leftrightarrow y = 0$,

ii) $\forall x \in X(K)\ \forall y \in \mathscr{L}(x)\ \forall t \in K\colon \|ty\| = |t|\|y\|$.

4.3. Remark. — If $K = \mathbb{C}$, then a metric on $\mathscr{L}$ is the same as a (possibly discontinuous) hermitian metric.

4.4. Definition. — Assume K to be non-Archimedean, and let $\mathscr{O}_K$ be the ring of integers in K. Further, let X be a K-scheme, and let $\mathscr{L} \in \operatorname{Pic}(X)$.

Then, by a *model* of $(X, \mathscr{L})$, we mean a triple $(\mathscr{X}, \widetilde{\mathscr{L}}, n)$ consisting of a natural number n, a flat projective scheme $\pi\colon \mathscr{X} \to \mathscr{O}_K$ such that $\mathscr{X}_K \cong X$, and an invertible sheaf $\widetilde{\mathscr{L}} \in \operatorname{Pic}(\mathscr{X})$ fulfilling $\widetilde{\mathscr{L}}|_X \cong \mathscr{L}^{\otimes n}$.

4.5. Example. — Assume K to be non-Archimedean, let $\mathscr{O}_K$ be the ring of integers in K, and let X be a K-scheme equipped with an invertible sheaf $\mathscr{L}$. Then a model $(\mathscr{X}, \widetilde{\mathscr{L}}, n)$ of $(X, \mathscr{L})$ induces a metric $\|\,.\,\|$ on $\mathscr{L}$ as follows.

$x \in X(K)$ has a unique extension $\overline{x}\colon \operatorname{Spec} \mathscr{O}_K \to \mathscr{X}$. Then $\overline{x}^*\widetilde{\mathscr{L}}$ is a projective $\mathscr{O}_K$-module of rank one. Each $l \in \mathscr{L}(x)$ induces $l^{\otimes n} \in \mathscr{L}^{\otimes n}(x)$ and, therefore, a rational section of $\overline{x}^*\widetilde{\mathscr{L}}$. Put

$$\|l\|(x) := \left[\inf\left\{|a| \mid a \in K,\, l \in a \cdot \overline{x}^*\widetilde{\mathscr{L}}\right\}\right]^{\frac{1}{n}}. \qquad (*)$$

4.6. Definition. — The metric $\|\,.\,\|$ given by $(*)$ is called the metric on $\mathscr{L}$ *induced by the model* $(\mathscr{X}, \widetilde{\mathscr{L}}, n)$.

4.7. Remark. — Note here that $\mathscr{O}_K$ is, in general, a *non-discrete* valuation ring. In particular, $\mathscr{O}_K$ will usually be non-Noetherian.

Nevertheless, projectivity includes being of finite type [**EGA**, Chapitre II, Définition (5.5.2)]. This means, for the description of $\mathscr{X}$, only a finite number of elements from $\mathscr{O}_K$ are needed.

In the particular case $K = \overline{\mathbb{Q}}_p$, the group $\nu(K)$ is isomorphic to $(\mathbb{Q}, +)$. Thus, for any finite set $\{a_1, \ldots, a_s\} \subset \mathscr{O}_{\overline{\mathbb{Q}}_p}$, there exists a *discrete* valuation ring $O \subseteq \mathscr{O}_{\overline{\mathbb{Q}}_p}$ containing $a_1, \ldots, a_s$.

By consequence, $\mathscr{X}$ is the base change of some scheme that is projective over a discrete valuation ring.

4.8. Definition. — Let K be an algebraically closed valuation field. Assume K to be non-Archimedean.

Then a metric $\| . \|$ on $\mathscr{L} \in \mathrm{Pic}(X)$ is called *continuous,* respectively *bounded,* if $\| . \| = f \cdot \| . \|'$ for $\| . \|'$ a metric induced by some model and f a function on $X(K)$ that is continuous or bounded, respectively.

4.9. Remark. — If $K = \mathbb{C}$, then we adopt the concepts of bounded, continuous, and smooth metrics in their the usual meaning from complex geometry. Note that smooth metrics are continuous and that continuous metrics are automatically bounded in the case $K = \mathbb{C}$.

ii. *The global case. Adelically metrized invertible sheaves.*

4.10. Definition. — Let X be a projective variety over $\mathbb{Q}$ and $m \in \mathbb{N}$.

Then, by a *model* of X over $\operatorname{Spec} \mathbb{Z}[\frac{1}{m}]$, we mean a scheme $\mathscr{X}$ that is projective and flat over $\operatorname{Spec} \mathbb{Z}[\frac{1}{m}]$ such that the generic fiber of $\mathscr{X}$ is isomorphic to X.

4.11. Definition. — Let X be a projective variety over $\mathbb{Q}$ and $\mathscr{L} \in \mathrm{Pic}(X)$ be an invertible sheaf.

a) Then an *adelic metric* on $\mathscr{L}$ is a system

$$\| . \| = \{\| . \|_\nu\}_{\nu \in \mathrm{Val}(\mathbb{Q})}$$

of continuous and bounded metrics on $\mathscr{L}_{\overline{\mathbb{Q}}_\nu} \in \mathrm{Pic}(X_{\overline{\mathbb{Q}}_\nu})$ such that

i) for each $\nu \in \mathrm{Val}(\mathbb{Q})$, the metric $\| . \|_\nu$ is $\mathrm{Gal}(\overline{\mathbb{Q}}_\nu/\mathbb{Q}_\nu)$-invariant,

ii) for some $m \in \mathbb{N}$, there exist a model $\mathscr{X}$ of X over $\operatorname{Spec} \mathbb{Z}[\frac{1}{m}]$, an invertible sheaf $\widetilde{\mathscr{L}} \in \mathrm{Pic}(\mathscr{X})$, and a natural number n such that

$$\widetilde{\mathscr{L}}|_X \cong \mathscr{L}^{\otimes n}$$

and, for all prime numbers $p \nmid m$, the metric $\| . \|_{\nu_p}$ is induced by $(\mathscr{X}_p, \widetilde{\mathscr{L}}|_{\mathscr{X}_p}, n)$.

b) An invertible sheaf equipped with an adelic metric is called an *adelically metrized invertible sheaf.*

c) All adelically metrized invertible sheaves on X form an abelian group, which will be called the *adelic Picard group* of X and denoted by $\widetilde{\mathrm{Pic}}(X)$.

4.12. Notation. — Let $\mathscr{X}$ be a model of X over $\operatorname{Spec} \mathbb{Z}$. Then taking the induced metric yields two natural homomorphisms

$$\begin{aligned} i_{\mathscr{X}} &\colon \widehat{\mathrm{Pic}}(\mathscr{X}) \to \widetilde{\mathrm{Pic}}(X)\,, \\ a_{\mathscr{X}} &\colon \ker(\mathrm{Pic}(\mathscr{X}) \to \mathrm{Pic}(X)) \otimes_{\mathbb{Z}} \mathbb{Q} \to \widetilde{\mathrm{Pic}}(X)\,. \end{aligned}$$

Further, one has the forgetful homomorphism

$$v \colon \widetilde{\mathrm{Pic}}(X) \to \mathrm{Pic}(X)\,.$$

4.13. Notation. — The models of X, together with all birational morphisms between them, form an inverse system of schemes. This is a filtered inverse system since, for two models $\mathscr{X}$ and $\mathscr{X}'$, the closure of the diagonal $\Delta \subset X \times_{\operatorname{Spec}\mathbb{Q}} X \subset \mathscr{X} \times_{\operatorname{Spec}\mathbb{Z}} \mathscr{X}'$ projects to both of them.

Thus, the arithmetic Picard groups $\widehat{\operatorname{Pic}}(\mathscr{X})$ for all models $\mathscr{X}$ of X form a filtered direct system. The injections $\widehat{\operatorname{Pic}}(\mathscr{X}) \hookrightarrow \widetilde{\operatorname{Pic}}(X)$ fit together to yield an injection

$$\iota_X \colon \varinjlim \widehat{\operatorname{Pic}}(\mathscr{X}) \hookrightarrow \widetilde{\operatorname{Pic}}(X)\,.$$

Similarly, the usual Picard groups $\operatorname{Pic}(\mathscr{X})$ form a filtered direct system, too. We get a homomorphism

$$\alpha_X \colon \varinjlim \ker(\operatorname{Pic}(\mathscr{X}) \to \operatorname{Pic}(X)) \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \widetilde{\operatorname{Pic}}(X)\,.$$

4.14. Definition (Metric on $v^{-1}(\mathscr{L}) \subseteq \widetilde{\operatorname{Pic}}(X)$). — Let X be a projective variety over $\mathbb{Q}$. On X, let $(\mathscr{L}, \|\,.\|)$ and $(\mathscr{L}, \|\,.\|')$ be two adelically metrized invertible sheaves with the same underlying sheaf.

Then the *distance* between $(\mathscr{L}, \|\,.\|)$ and $(\mathscr{L}, \|\,.\|')$ is given by

$$\delta((\mathscr{L}, \|\,.\|), (\mathscr{L}, \|\,.\|')) := \sum_{\nu \in \operatorname{Val}(\mathbb{Q})} \delta_\nu(\|\,.\|_\nu, \|\,.\|'_\nu)$$

for

$$\delta_\nu(\|\,.\|_\nu, \|\,.\|'_\nu) := \sup_{x \in X(\overline{\mathbb{Q}}_\nu)} \left| \log \frac{\|\,.\|'_\nu(x)}{\|\,.\|_\nu(x)} \right| .$$

4.15. Lemma. — *δ is a metric on the set $v^{-1}(\mathscr{L})$ of all metrizations of $\mathscr{L}$.*

Proof. We have to show that the sum is always finite.

For this, we note first that the metrics $\|\,.\|_\nu$ and $\|\,.\|'_\nu$ are bounded by definition. Therefore, each summand is finite.

We may thus ignore a finite set S of primes and assume that $\|\,.\|$ and $\|\,.\|'$ are given by triples $(\mathscr{X}, \widetilde{\mathscr{L}}, n)$ and $(\mathscr{X}', \widetilde{\mathscr{L}}', n')$, respectively, in the sense of Definition 4.11.a.ii).

The isomorphism $\mathscr{X}_\mathbb{Q} \xrightarrow{\cong} X \xrightarrow{\cong} \mathscr{X}'_\mathbb{Q}$ may be extended to an open neighbourhood of the generic fiber. Therefore, enlarging S if necessary, we have an isomorphism $\mathscr{X}' \xrightarrow{\cong} \mathscr{X}$ of schemes over $\operatorname{Spec}\mathbb{Z}\backslash S$. Further, the triple $(\mathscr{X}, \widetilde{\mathscr{L}}, n)$ may be replaced by $(\mathscr{X}, \widetilde{\mathscr{L}}^{\otimes n'}, nn')$ without any change of the induced metric. Thus, without restriction, $n = n'$.

To summarize, we are reduced to the case that $\|\,.\|$ and $\|\,.\|'$ are given by $(\mathscr{X}, \widetilde{\mathscr{L}}, n)$ and $(\mathscr{X}, \widetilde{\mathscr{L}}', n)$. We have an isomorphism

$$\widetilde{\mathscr{L}}|_{\mathscr{X}_\mathbb{Q}} \xrightarrow{\cong} \mathscr{L}^{\otimes n} \xrightarrow{\cong} \widetilde{\mathscr{L}}'|_{\mathscr{X}_\mathbb{Q}}\,,$$

which may be extended to an open neighbourhood of the generic fiber. Therefore, in the definition of $\delta((\mathscr{L}, \|\,.\|), (\mathscr{L}, \|\,.\|'))$, all the summands vanish, except finitely many.

Positivity, symmetry, and the triangle inequality are clear. □

4.16. Remark. — It is convenient to consider two adelically metrized invertible sheaves with different underlying sheaves as of distance infinity. Then the distance δ is no longer a metric but only a separated écart in the sense of N. Bourbaki [**Bou-T**, §1].

4.17. Lemma. — *Let $f\colon X \to Y$ be a morphism of projective varieties over $\mathbb{Q}$.*
i) *Then the homomorphism $f^*\colon \widetilde{\mathrm{Pic}}(Y) \to \widetilde{\mathrm{Pic}}(X)$ is continuous with respect to the metric topology.*
ii) *Even more,*

$$\delta(f^*\overline{\mathscr{L}}_1, f^*\overline{\mathscr{L}}_2) \leq \delta(\overline{\mathscr{L}}_1, \overline{\mathscr{L}}_2)$$

for arbitrary adelically metrized invertible sheaves $\overline{\mathscr{L}}_1, \overline{\mathscr{L}}_2 \in \widetilde{\mathrm{Pic}}(Y)$.

Proof. ii) is obvious. i) follows immediately from ii). □

iii. *Adelic heights.*

4.18. Example. — Let K be a number field. Then there is an isomorphism

$$l\colon \widetilde{\mathrm{Pic}}(\operatorname{Spec} K) \cong \bigoplus_{w \in \mathrm{Val}(K)} \mathbb{R} \Big/ \operatorname{im} \lambda\,,$$

where λ is the mapping

$$\begin{aligned} \lambda\colon K^* &\longrightarrow \bigoplus_{w \in \mathrm{Val}(K)} \mathbb{R}\,, \\ t &\mapsto (-\log |t|_w)_{w \in \mathrm{Val}(K)}\,. \end{aligned}$$

Proof. We have $\mathrm{Pic}(\operatorname{Spec} K) = 0$. Thus, only the metrizations of the trivial invertible sheaf $\mathscr{O}_{\operatorname{Spec} K}$ have to be considered. We choose a section $0 \neq s \in \Gamma(\operatorname{Spec} K, \mathscr{O}_{\operatorname{Spec} K}) = K$.

For every $\nu \in \mathrm{Val}(\mathbb{Q})$, one has $K \otimes_{\mathbb{Q}} \mathbb{Q}_\nu \cong \prod_w K_w$ [**Cas67**, formula (10.2)], where w runs through the valuations of K, extending ν. Hence,

$$\operatorname{Spec} K \times_{\operatorname{Spec} \mathbb{Q}} \operatorname{Spec} \mathbb{Q}_\nu \cong \coprod_w \operatorname{Spec} K_w,$$

and accordingly for the structure sheaves. Thus, the section s induces the homomorphism

$$\iota\colon \widetilde{\mathrm{Pic}}(\operatorname{Spec} K) \longrightarrow \bigoplus_{w \in \mathrm{Val}(K)} \mathbb{R}\,,$$

given by $(\mathscr{L}, \{\|\,.\|_\nu\}_{w \in \mathrm{Val}(K)}) \mapsto (-\log \|s\|_w)_{w \in \mathrm{Val}(K)}$. Here, condition ii) of Definition 4.11.a) ensures that all the valuations of s, except finitely many, are actually equal to 1. Therefore, the image of ι is indeed contained in the direct sum.

Furthermore, ι is a surjection, as the existence of an appropriate model is required only outside a finite number of primes.

Finally, there is the ambiguity caused by the choice of the section s. Two non-zero sections $s, s' \in \Gamma(\operatorname{Spec} K, \mathscr{O}_{\operatorname{Spec} K})$ differ by a factor $t \in K^*$. Thus, the corresponding images in $\bigoplus_w \mathbb{R}$ differ by the summand $(-\log |t|_w)_{w \in \mathrm{Val}(K)}$. The assertion follows. □

4.19. Definition (Arithmetic degree). — For an adelically metrized invertible sheaf $(\mathscr{L}, \| . \|)$ on $\operatorname{Spec} K$, define its *arithmetic degree* by

$$\widetilde{\deg}\,(\mathscr{L}, \| . \|) := s(l(\mathscr{L}, \| . \|))\,.$$

Here, $s\colon \bigoplus_w \mathbb{R} \big/ \operatorname{im} \lambda \to \mathbb{R}$ is the summation map.

4.20. Remarks. — i) The product formula implies that the summation map s factors via $\bigoplus_w \mathbb{R} \big/ \operatorname{im} \lambda$.

ii) The arithmetic degree is a group homomorphism $\widetilde{\deg} : \widetilde{\operatorname{Pic}}(\operatorname{Spec} K) \to \mathbb{R}$.

iii) For every $\overline{\mathscr{L}} \in \widehat{\operatorname{Pic}}(\operatorname{Spec} \mathbb{Z})$, one has $\widetilde{\deg}\,(i_{\operatorname{Spec} \mathbb{Z}}(\overline{\mathscr{L}})) = \widehat{\deg}\,(\overline{\mathscr{L}})$. Indeed, this is directly seen from the various definitions.

4.21. Remarks. — The adelic Picard groups as defined here tend to be very large groups. They are not designed to be particularly interesting invariants for a purpose such as distinguishing between non-isomorphic varieties.

They just give a general framework for the determination of an individual height function. This framework is in fact more flexible than the concept of a height with respect to a hermitian line bundle, introduced in the definition in Subsection 3.12.

Further, the height function defined by an ample adelically metrized invertible sheaf $\overline{\mathscr{L}}$ differs only by a bounded function from that defined in a naive way by the underlying invertible sheaf $\mathscr{L}$, cf. Definition 2.10.

4.22. Definition. — Let X be a regular, projective variety over $\mathbb{Q}$, and let $\overline{\mathscr{L}} \in \widetilde{\operatorname{Pic}}(X)$ be an adelically metrized invertible sheaf.

Then the *absolute height* with respect to $\overline{\mathscr{L}}$ of an K-valued point $x \in X(K)$ for K a number field is given by

$$\mathrm{h}_{\overline{\mathscr{L}}}(x) := \frac{1}{[K : \mathbb{Q}]}\, \widetilde{\deg}\, \overline{\mathscr{L}}|_x\,.$$

4.23. Example. — Consider the situation that $X = \mathbf{P}^n_{\mathbb{Q}}$ and $\mathscr{L} = \mathscr{O}(1)$, equipped with the adelic metric, induced by the model $(\mathbf{P}^n_{\mathbb{Z}}, \mathscr{O}(1), 1)$.

Then $\mathrm{h}_{\overline{\mathscr{L}}}$ coincides with the naive height $\mathrm{h}_{\mathrm{naive}}$.

Proof. This is immediate from Definitions 4.22 and 4.6, combined with Definitions 2.4 and 2.9. □

4.24. Lemma. — *Let $f\colon X \to Y$ be a morphism of projective varieties over $\mathbb{Q}$, and let $\overline{\mathscr{L}}$ be an adelically metrized invertible sheaf on Y.*

Then, for every number field K and every $x \in \mathscr{X}(K)$,

$$\mathrm{h}_{f^*\overline{\mathscr{L}}}(x) = \mathrm{h}_{\overline{\mathscr{L}}}(f(x))\,.$$

Proof. According to Definition 4.22, we have

$$\mathrm{h}_{f^*\overline{\mathscr{L}}}(x) = \frac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\left(\overline{x}^*(f^*\overline{\mathscr{L}})\right) = \frac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\left((f\circ\overline{x})^*\overline{\mathscr{L}}\right) = \mathrm{h}_{\overline{\mathscr{L}}}(f(x))\,. \quad \square$$

4.25. Proposition. — *Let X be a projective variety over $\mathbb{Q}$.*

a) *Let $\|\,.\|_1$ and $\|\,.\|_2$ be adelic metrics on one and the same invertible sheaf $\mathscr{L}$. Then there is a constant C such that*

$$|\mathrm{h}_{(\mathscr{L},\|\,.\|_1)}(x) - \mathrm{h}_{(\mathscr{L},\|\,.\|_2)}(x)| < C$$

for every number field K and every $x \in X(K)$.

b) *Let $\overline{\mathscr{L}_1}$ and $\overline{\mathscr{L}_2}$ be two adelically metrized invertible sheaves. Then*

$$\mathrm{h}_{(\overline{\mathscr{L}_1}\otimes\overline{\mathscr{L}_2})} = \mathrm{h}_{\overline{\mathscr{L}_1}} + \mathrm{h}_{\overline{\mathscr{L}_2}}\ .$$

c) *Let $\overline{\mathscr{L}}$ be an adelically metrized invertible sheaf such that the underlying invertible sheaf is ample. Then, for every $B, D \in \mathbb{R}$, there are only finitely many points $x \in X(K)$ such that $[K:\mathbb{Q}] < D$ and*

$$\mathrm{h}_{\overline{\mathscr{L}}}(x) < B\,.$$

Proof. a) Over some $\operatorname{Spec}\mathbb{Z}[\frac{1}{m}]$, the adelic metrics $\|\,.\|_1$ and $\|\,.\|_2$ are induced by models $(\mathscr{X}_1, \widetilde{\mathscr{L}}_1, n_1)$ and $(\mathscr{X}_2, \widetilde{\mathscr{L}}_2, n_2)$, respectively. We may assume without restriction that $n_1 = n_2 =: n$, as a model $(\mathscr{X}, \widetilde{\mathscr{L}}, n)$ may always be replaced by $(\mathscr{X}, \widetilde{\mathscr{L}}^{\otimes n'}, nn')$ without change.

Further, there is a birational equivalence $\iota\colon \mathscr{X}_1 \dashrightarrow \mathscr{X}_2$ that extends the identity map on X. It defines an isomorphism $\mathscr{U}_1 \dashrightarrow \mathscr{U}_2$ between suitable open subschemes completely containing the generic fibers. As $\mathscr{X}_1$ and $\mathscr{X}_2$ are proper, the complementary closed subsets are contained in finitely many special fibers. Hence, ι induces an isomorphism over some $\operatorname{Spec}\mathbb{Z}[\frac{1}{mm'}]$ for $m \neq 0$.

As an analogous argument applies to the invertible sheaves $\widetilde{\mathscr{L}}_1$ and $\widetilde{\mathscr{L}}_2$, we see that $\|\,.\|_1$ and $\|\,.\|_2$ coincide up to finitely many primes $\nu_1, \ldots, \nu_k$. Further, an adelic metric consists of bounded metrics. Hence, there is a constant D such that

$$\frac{1}{D}\|\,.\|_{1,\nu_i} \leq \|\,.\|_{2,\nu_i} \leq D\|\,.\|_{1,\nu_i}$$

for $i = 1, \ldots, k$.

For $x \in X(K)$, we now have

$$\begin{aligned} \mathrm{h}_{(\mathscr{L},\|\,.\,\|_1)}(x) - \mathrm{h}_{(\mathscr{L},\|\,.\,\|_2)}(x) &= \tfrac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\left(x^*\mathscr{L}, x^*\|\,.\,\|_1\right) - \tfrac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\left(x^*\mathscr{L}, x^*\|\,.\,\|_2\right) \\ &= \tfrac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\left(\mathscr{O}_{\operatorname{Spec} K}, x^*(\|\,.\,\|_1 \otimes \|\,.\,\|_2^{-1})\right). \end{aligned}$$

Working with the non-zero section $1 \in \Gamma(\operatorname{Spec} K, \mathscr{O}_{\operatorname{Spec} K})$, we see that the latter expression is equal to

$$\tfrac{1}{[K:\mathbb{Q}]} \sum_{w \in \operatorname{Val}(K)} - \log \|1\|_w = \tfrac{1}{[K:\mathbb{Q}]} \sum_{i=1}^{k} \sum_{w|\nu_i} - \log \|1\|_w$$

for $\|\,.\,\|_w$ the extension of $(\|\,.\,\|_1 \otimes \|\,.\,\|_2^{-1})_\nu$ from $\mathbb{Q}_\nu$ to K_w. This includes a raise to the $[K_w : \mathbb{Q}_\nu]$-th power [**Cas67**, Sec. 11]. Hence,

$$|\,\mathrm{h}_{(\mathscr{L},\|\,.\,\|_1)}(x) - \mathrm{h}_{(\mathscr{L},\|\,.\,\|_2)}(x)| \leq \tfrac{1}{[K:\mathbb{Q}]} \sum_{i=1}^{k} \sum_{w|\nu_i} [K_w : \mathbb{Q}_\nu] \log D = k \log D\,,$$

when we observe the fact that $\sum\limits_{w|\nu_i} [K_w : \mathbb{Q}_\nu] = [K : \mathbb{Q}]$. This is the assertion.

b) Clearly, for every $x \in \mathscr{X}(K)$, one has

$$\begin{aligned} \mathrm{h}_{(\overline{\mathscr{L}_1} \otimes \overline{\mathscr{L}_2})}(x) &= \tfrac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\left(\overline{x}^*(\overline{\mathscr{L}_1} \otimes \overline{\mathscr{L}_2})\right) = \tfrac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\left((\overline{x}^*\overline{\mathscr{L}_1}) \otimes (\overline{x}^*\overline{\mathscr{L}_2})\right) \\ &= \tfrac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\,(\overline{x}^*\overline{\mathscr{L}_1}) + \tfrac{1}{[K:\mathbb{Q}]}\,\widetilde{\deg}\,(\overline{x}^*\overline{\mathscr{L}_2}) = \mathrm{h}_{\overline{\mathscr{L}_1}}(x) + \mathrm{h}_{\overline{\mathscr{L}_2}}(x)\,. \end{aligned}$$

c) There is some $k \in \mathbb{N}$ such that $\mathscr{L}^{\otimes k}$ is very ample. Part b) shows that it suffices to verify the assertion for $\overline{\mathscr{L}}^{\otimes k}$. Thus, we may assume that $\mathscr{L}$ is very ample.

Let $i\colon X \hookrightarrow \mathbf{P}^N_{\mathbb{Q}}$ be the closed embedding induced by $\mathscr{L}$. Then $\mathscr{L} = i^*\mathscr{O}(1)$. Tietze's Theorem shows that there exists a hermitian metric $\|\,.\,\|$ on $\mathscr{O}(1)_{\mathbf{P}^N_{\mathbb{C}}}$ such that $\|\,.\,\|_{\mathscr{L},\infty} = i^*\|\,.\,\|$.

Further, there is the model $(\mathscr{X}, \widetilde{\mathscr{L}}, n)$ over some $\operatorname{Spec} \mathbb{Z}[\frac{1}{m}]$, which induces the adelic metric $\|\,.\,\|_{\mathscr{L}}$ outside the primes dividing m. The morphism $i\colon X \hookrightarrow \mathbf{P}^N_{\mathbb{Q}}$ extends to a rational map $i'\colon \mathscr{X} \dashrightarrow \mathbf{P}^N_{\mathbb{Z}[\frac{1}{m}]}$, the locus of indeterminacy of which is a closed subset of $\mathscr{X}$ not meeting the generic fiber. As $\mathscr{X}$ is proper, this shows that i' is actually a morphism over $\operatorname{Spec} \mathbb{Z}[\frac{1}{mm'}]$, for a certain $m' \neq 0$.

Now, by [**EGA**, Chapitre III, Proposition (4.4.1)] together with [**EGA**, Chapitre III, Corollaire (4.4.9)], there is an open subset $\mathscr{U} \subseteq \mathscr{X}$ containing the generic fiber such that $i'|_{\mathscr{U}}$ is an embedding. Again as $\mathscr{X}$ is proper, we see that i' is an embedding over $\operatorname{Spec} \mathbb{Z}[\frac{1}{mm''}]$ for some $m'' \neq 0$.

Define on $\mathscr{O}(1)$ an adelic metric in such a way that, at the finite primes ν dividing mm'', it extends the metric defined by $\|\,.\,\|_{\mathscr{L},\nu}$ on $i(X) \subseteq \mathbf{P}^N$ and, at the remaining finite primes, it is induced by the model $(\mathbf{P}^N_{\mathbb{Z}[\frac{1}{mm''}]}, \mathscr{O}(1), 1)$. Further, at the infinite prime, we let it agree with the hermitian metric $\|\;\|$ from above.

Then $i^*\overline{\mathscr{O}(1)} = \overline{\mathscr{L}}$. Consequently, $\mathrm{h}_{\overline{\mathscr{L}}}(x) = \mathrm{h}_{\overline{\mathscr{O}(1)}}(i(x))$. It is, therefore, sufficient to show the assertion for the height function $\mathrm{h}_{\overline{\mathscr{O}(1)}}$ on $\mathbf{P}^N$.

But part a) together with Example 4.23 shows that $\mathrm{h}_{\overline{\mathscr{O}(1)}}$ differs from $\mathrm{h}_{\mathrm{naive}}$ by a bounded summand. Thus, Proposition 2.6 implies the assertion. □

4.26. Remarks. — a) The concept of an adelically metrized invertible sheaf as described here is essentially that introduced by V. V. Batyrev and Yu. I. Manin in [**B/M**]. It was used, for example, by E. Peyre in [**Pe02**].

A small difference is that Batyrev and Manin fix norms on the spaces $\mathscr{L}(x)$ only for $x \in X(\mathbb{Q}_\nu)$, not for $x \in X(\overline{\mathbb{Q}}_\nu)$. Correspondingly, their concept of adelic metric leads to a height for points rational over the base field and not to an absolute height.

b) There is a somewhat different concept of an adelic Picard group, which is due to S. Zhang [**Zh95b**]. His definition leads to by far smaller groups. In fact, the adelically metrized invertible sheaves that are globally induced by a model are topologically dense in $\widetilde{\mathrm{Pic}}_{\mathrm{Zh}}(X)$.

This has the following consequence, which is highly interesting for many applications. There is a continuous $\mathbb{Z}$-multilinear map

$$\underbrace{\widetilde{\mathrm{Pic}}_{\mathrm{Zh}}(X) \times \ldots \times \widetilde{\mathrm{Pic}}_{\mathrm{Zh}}(X)}_{\dim X+1 \text{ times}} \longrightarrow \mathbb{R}\,,$$

which is called the adelic intersection product. It is uniquely determined by the condition that it agrees with the arithmetic intersection product of H. Gillet and C. Soulé [**G/S90**, Theorem 4.2.3] when restricted to adelically metrized invertible sheaves induced by models. More details are given in [**Zh95b**].

CHAPTER II

Conjectures on the asymptotics of points of bounded height

I have no satisfaction in formulas unless I feel their numerical magnitude.

WILLIAM THOMSON 1ST BARON KELVIN,
(Life (1943) by Sylvanus Thompson, p. 827)

1. A heuristic

1.1. — Let X be a projective variety over $\mathbb{Q}$. Then one of the most natural questions to ask is

($*$) Does X have finitely many or infinitely many $\mathbb{Q}$-rational points?

1.2. — If the answer is that $\#X(\mathbb{Q}) < \infty$, then one might ask for the precise number. Otherwise, if $X(\mathbb{Q})$ is infinite, then one may ask for the asymptotics of the rational points with respect to a certain height function H on $X(\mathbb{Q})$.

($\dagger$) What is the asymptotics of the function $N_{X,\mathrm{H}}$ given by

$$N_{X,\mathrm{H}}(B) := \#\{x \in X(\mathbb{Q}) \mid \mathrm{H}(x) < B\}$$

for $B \to \infty$?

1.3. — If X is a hypersurface of degree d in $\mathbf{P}^n$, then there is a statistical heuristic for the asymptotics of $N_{X,\mathrm{H}_{\mathrm{naive}}}$.

1.4. Statistical heuristic. — *Let X be a hypersurface of degree d in $\mathbf{P}^n_{\mathbb{Q}}$. Then*

$$N_{X,\mathrm{H}_{\mathrm{naive}}}(B) \sim C \cdot B^{n+1-d}$$

for some positive constant C.

Proof. On $\mathbf{P}^n$, the total number of $\mathbb{Q}$-rational points of height $< B$ is $\sim B^{n+1}$. Indeed, these points may be given in the form

$$(x_0 : \ \ldots \ : x_n)$$

for $x_i \in \mathbb{Z}$ such that $x_i \in [-B, B]$. There are $\sim B^{n+1}$ such $(n+1)$-tuples and the probability that $\gcd(x_0, \ \ldots \ , x_n) = 1$ is positive.

Further, X is given by a homogeneous form F of degree d. Its range of values on $[-B,B]^{n+1}$ is, a priori, $[-DB^d, DB^d]$ for a certain positive constant D.

We assume that the values of F are equally distributed in that range. The value zero is then hit $\sim B^{n+1-d}$ times. □

1.5. Remark. — This heuristic is definitely an interesting guideline about which behaviour to expect. It is, however, too naive in order to work well in all cases.

1.6. Example (Too few points—p-adic unsolvability). — Consider the cubic fourfold X in $\mathbf{P}^5_{\mathbb{Q}}$ given by the equation

$$x^3 + 7y^3 + 49z^3 + 2u^3 + 14v^3 + 98w^3 = 0\,.$$

Then $X(\mathbb{Q}_7) = \emptyset$, which implies $X(\mathbb{Q}) = \emptyset$.

Note that the statistical heuristic would predict cubic growth for the number of $\mathbb{Q}$-rational points x on X such that $\mathrm{H}_{\mathrm{naive}}(x) < B$.

1.7. Example (Too few points—the Brauer–Manin obstruction). — Consider the cubic surface X in $\mathbf{P}^3_{\mathbb{Q}}$ given by the equation

$$w(x+w)(12x+w) = \prod_{i=1}^{3} \big(x + \theta^{(i)}y + (\theta^{(i)})^2 z\big).$$

Here,

$$\theta := -38 + \sum_{i \in (\mathbb{F}_{19}^*)^3} \zeta_{19}^i \in \mathbb{Q}(\zeta_{19})$$

and $\theta^{(i)}$ are the three conjugates of θ in $\overline{\mathbb{Q}}$.

As will be shown in Example IV.5.24, $X(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ but $X(\mathbb{Q}) = \emptyset$. On X, there is an obstruction to the Hasse principle, which is an instance of the general Brauer–Manin obstruction, cf. Section IV.2.

In this case, the statistical heuristic would predict linear growth for the number of $\mathbb{Q}$-rational points x on X such that $\mathrm{H}_{\mathrm{naive}}(x) < B$.

1.8. Examples (Too many points—accumulating subvarieties). — i) Consider the smooth threefold $X \subset \mathbf{P}^4_{\mathbb{Q}}$ given by

$$x^4 + y^4 = z^4 + v^4 + w^4\,.$$

Then the statistical heuristic predicts linear growth. I.e., there should be $\sim CB$ rational points of height $< B$.

However, X contains the line given by $x = z$, $y = v$, and $w = 0$, on which there is quadratic growth, already.

ii) Other examples of interest are provided by the diagonal cubic threefolds $V_{a,1} \in \mathbf{P}^4_{\mathbb{Q}}$ of the form

$$V_{a,1}\colon ax^3 = y^3 + z^3 + v^3 + w^3\,.$$

Here, quadratic growth is predicted by the statistical heuristic.

However, $V_{a,1}$ clearly contains the lines given by $v = -w$ and

$$(x : y : z) = (x_0 : y_0 : z_0)$$

for $(x_0 : y_0 : z_0)$ a $\mathbb{Q}$-rational point on the curve

$$E_a \colon ax^3 = y^3 + z^3 .$$

This is a twisted Fermat cubic. One has the rational point $(0 : 1 : (-1)) \in E_a(\mathbb{Q})$. Therefore, E_a is an elliptic curve over $\mathbb{Q}$. The lines described form a cone over an elliptic curve. There are $\sim B^2$ $\mathbb{Q}$-rational points of height $< B$ alone on this cone.

Examples of twisted Fermat cubics of rank up to three were known to Ernst S. Selmer as early as 1951 [**Sel**]. For example, $E_6(\mathbb{Q})$ is of rank one, generated by $(21 : 17 : 37)$.

1.9. Remark. — These examples grew out of our study of diagonal cubic and quartic threefolds, which is described in Chapter VI.

1.10. Geometric interpretation. — The exponent $n+1-d$ appearing in the statistical heuristic may be positive, zero, or negative. According to this distinction, there are three cases.

This distinction creating three cases coincides perfectly well with the Kodaira classification of projective varieties into Fano varieties, varieties of intermediate type, and varieties of general type. Indeed, the anticanonical divisor $(-K)$ on a degree d hypersurface in $\mathbf{P}^n$ is exactly $\mathscr{O}(n + 1 - d)$.

1.11. Remark. — The Kodaira classification is a purely geometric one. It does not make use of any arithmetic information on the projective variety considered. Only the complex algebraic variety produced by base change to $\mathbb{C}$ is exploited.

It is a very remarkable observation that whether a projective variety X is Fano, of intermediate type, or of general type seemingly has a lot of influence on the set of $\mathbb{Q}$-rational points on X.

1.12. — More concretely, expectations are as follows.

First case. X is a variety of general type.

By definition, this means that the canonical invertible sheaf $\mathscr{K}$ is ample.

In the case of a hypersurface, this corresponds to the case that $n + 1 - d < 0$. Here, the statistical heuristic is rather illogical. It states that for a large height bound, we expect fewer points than for a small one. In the limit for $B \to \infty$, we have $B^{n+1-d} \to 0$.

One would therefore expect only very few $\mathbb{Q}$-rational points on X. This is exactly the content of the conjecture of Lang.

Second case. X is a variety of intermediate type.

In the case of a hypersurface, this corresponds to the case that $n + 1 - d = 0$. Here, the statistical heuristic states that there should be a constant number of points, independently of the height bound B.

One would therefore expect that there are a few $\mathbb{Q}$-rational points on X. A more precise statement is given by the conjecture of Batyrev and Manin.

Third case. X is a Fano variety.

By definition, this means that the anticanonical invertible sheaf $\mathscr{K}^\vee$ is ample.

In the case of a hypersurface, this corresponds to the case that $n + 1 - d > 0$. Here, one would expect that there are a lot of $\mathbb{Q}$-rational points on X. A by-far-more-precise formulation is given by the conjecture of Manin.

2. The conjecture of Lang

2.1. — The conjecture of Lang deals with the case of a variety of general type. There are actually several versions of it [**Lan86**].

2.2. Conjecture (Lang). — *Let X be a smooth, projective variety of general type over a number field K. Then*

i) (Weak Lang conjecture) *The set of rational points $X(K)$ is not Zariski dense in X.*

ii) (Strong Lang conjecture) *There is a Zariski closed subset $Z \subset X$ such that, for any finite field extension $L \supseteq K$, one has that $X(L) \backslash Z(L)$ is finite.*

2.3. Conjecture (Geometric Lang conjecture). — *Let X be a smooth, projective variety of general type over a field K of characteristic* 0*. Then there is a proper Zariski closed subset $Z(X) \subset X$, called the Langian exceptional set, which is the union of all positive dimensional subvarieties that are not of general type.*

2.4. Remark. — These conjectures are strongly interrelated. If the geometric Lang conjecture is true, then the weak Lang conjecture implies the strong Lang conjecture.

2.5. — Lang's conjectures are known to be true when X is a subvariety of an abelian variety. This was proven by G. Faltings in [**Fa91**].

Faltings' 1991 result includes the case that X is a curve of general type. I.e., a curve of genus $g \geq 2$. This particular case of Lang's conjecture has been popular for decades as the Mordell conjecture. The Mordell conjecture was proven by G. Faltings in 1983 [**Fa83**].

2.6. Examples. — If X is a curve, then there is no Langian exceptional set Z. Weak and strong Lang conjectures are therefore equivalent.

This is no longer the case for surfaces of general type.

i) For example, the quintic surface given by

$$x^5 + y^5 + z^5 + w^5 = 0$$

in $\mathbf{P}^3_{\mathbb{Q}}$ contains the line "$x = -y, z = -w$", on which there are infinitely many $\mathbb{Q}$-rational points.

ii) Another example of a surface of general type containing a projective line is provided by the Godeaux surface [**Bv**, Example X.3.4].

iii) Let $V^3_{a,b}$ be the cubic threefold in $\mathbf{P}^4_{\mathbb{Q}}$ given by

$$ax^3 = by^3 + z^3 + v^3 + w^3 \, .$$

Then the moduli space $L_{a,b}$ of the lines on $V_{a,b}$ is a surface of general type [**Cl/G**, Lemma 10.13].

If the cubic curve

$$E_{a,b} \colon ax^3 + by^3 + z^3 = 0$$

contains a rational point, then, on $V_{a,b}$, there are the lines given by $v = -w$ and $(x : y : z) = (x_0 : y_0 : z_0)$ for $(x_0 : y_0 : z_0) \in E_{a,b}(\mathbb{Q})$. We call these lines the *obvious lines* on $V_{a,b}$.

In other words, if $E_{a,b}(\mathbb{Q}) \neq \emptyset$, then the surface $L_{a,b}$, which is of general type, contains a copy of the elliptic curve $E_{a,b}$. There are infinitely many $\mathbb{Q}$-rational points on $E_{a,b}$, for example for $a = 6$ and $b = 1$.

2.7. An experiment. — We searched systematically for $\mathbb{Q}$-rational lines on the cubic threefolds $V_{a,b}$ for $a, b = 1, \ldots, 100$, $a \geq b$. Our method is described in detail in Chapter VI, Section 4. It guarantees that every line that contains a point of height $< 5\,000$ is certainly found.

The results may be interpreted as providing numerical evidence for Lang's conjecture. Indeed, a $\mathbb{Q}$-rational point on $L_{a,b}$ corresponds to a $\mathbb{Q}$-rational line on $V_{a,b}$. Points on the elliptic curves lying on $L_{a,b}$ correspond to the obvious lines.

In agreement with Lang's conjecture, only very few non-obvious lines were found. On all the varieties $V_{a,b}$ for $a, b = 1, \ldots, 100$, $a \geq b$, together, there are only 42 non-obvious lines containing a point of height $< 5\,000$. Each such line actually contains a point of height ≤ 15. We describe these lines explicitly in Chapter VI, Section 4, Table 1.

2.8. Remark. — It is expected that Lang's conjecture is true not only over number fields but over every field that is finitely generated over $\mathbb{Q}$. This version of Lang's conjecture has a number of surprising consequences. The reader may get an impression of these in the article [**A/V**] of D. Abramovich and J. F. Voloch.

3. The conjecture of Batyrev and Manin

i. *Generalities.*

3.1. Conjecture (V. V. Batyrev and Yu. I. Manin). — *Let X be a smooth, projective variety over a number field k, and let $\mathscr{L}$ be an ample invertible sheaf on X. We denote by K and L divisors on X that represent the canonical invertible sheaf and $\mathscr{L}$, respectively.*

Suppose $r \in \mathbb{R}$ is such that

$$[K + rL] \in \mathrm{NS}(X) \otimes_{\mathbb{Z}} \mathbb{R}$$

is the class of an effective $\mathbb{R}$-divisor.

Then, for every $\varepsilon > 0$, there exists a Zariski open subset $X^\circ \subseteq X$ such that

$$N_{X^\circ, \mathrm{H}_{\mathscr{L}}}(B) = \#\{x \in X^\circ(k) \mid \mathrm{H}_{\mathscr{L}}(x) < B\} \ll B^{r+\varepsilon}$$

for $B \to \infty$.

3.2. — Here, $\mathrm{H}_{\mathscr{L}}$ is the exponential of the height $\mathrm{h}_{\mathscr{L}}$ defined by $\mathscr{L}$ as introduced in Definition I.2.10. It is determined only up to a factor that is bounded above and below by positive constants.

The conjecture is consistent with these changes of the height function since $B^{r+\varepsilon}$ and $(CB)^{r+\varepsilon}$ differ by a constant factor.

3.3. Remark. — This conjecture was first formulated by V. V. Batyrev and Yu. I. Manin in [**B/M**]. An excellent presentation may be found in the survey article [**Pe02**] by E. Peyre.

3.4. Fact (Varieties of general type). — *The conjecture of Batyrev and Manin implies the weak Lang conjecture.*

Proof. Indeed, if X is a variety of general type, then the canonical invertible sheaf $\mathscr{K}$ itself is ample and we may work with $\mathscr{L} := \mathscr{K}$.

Then $K + (-1)L = 0$ is an effective $\mathbb{R}$-divisor. Hence, for every $\varepsilon > 0$, the conjecture of Batyrev and Manin yields that

$$\#\{x \in X^\circ(k) \mid \mathrm{H}_{\mathscr{L}}(x) < B\} \ll B^{-1+\varepsilon}$$

for a suitable Zariski open subset $X^\circ \subset X$. In the limit for $B \to \infty$, this shows that $X^\circ(k)$ is empty.

The set $X(k)$ is therefore not Zariski dense in X. □

3.5. — Let X be a smooth Fano variety. Then the anticanonical invertible sheaf $\mathscr{K}^\vee$ is ample, and we may consider an anticanonical height, which is defined by $\mathscr{L} := \mathscr{K}^\vee$.

3.6. Fact (Fano varieties). — *For X a smooth Fano variety, the conjecture of Batyrev and Manin yields that*

$$N_{X^\circ,\mathrm{H}_{\mathscr{K}^\vee}}(B) = \#\{x \in X^\circ(k) \mid \mathrm{H}_{\mathscr{K}^\vee}(x) < B\} \ll B^{1+\varepsilon}$$

for a suitable Zariski open subset $X^\circ \subset X$.

Proof. In this situation, $K + (-K) = 0$ is an effective $\mathbb{R}$-divisor. □

3.7. Remarks. — i) In the case of a Fano hypersurface, this assertion fits perfectly well with the statistical heuristic.

ii) However, for Fano varieties, the conjecture of Manin describes the growth of $N_{X^\circ,\mathrm{H}_{\mathscr{K}^\vee}}$ much more precisely. The most interesting case of the conjecture of Batyrev and Manin is, therefore, that of a variety of intermediate type.

ii. *Varieties of intermediate type.*

3.8. — Let X be a smooth, projective, minimal surface of Kodaira dimension 0. Fix an ample invertible sheaf $\mathscr{L} \in \mathrm{Pic}(X)$.

Then the conjecture of Batyrev and Manin states that, for every $\varepsilon > 0$, there exists a Zariski open subset $X^\circ \subset X$ such that

$$N_{X^\circ,\mathrm{H}_{\mathscr{L}}}(B) = \#\{x \in X^\circ(k) \mid \mathrm{H}_{\mathscr{L}}(x) < B\} \ll B^{\varepsilon}\,.$$

Indeed, $12K$ is linearly equivalent to zero in any of the four cases of the Kodaira classification. Hence,

$$[K] \in \mathrm{NS}(X) \otimes_{\mathbb{Z}} \mathbb{R}$$

is the class of an effective $\mathbb{R}$-divisor on X.

3.9. Example. — If X is an abelian variety, then the conjecture of Batyrev and Manin is true.

Indeed, if the rank of $X(k)$ is equal to r, then

$$N_{X^\circ,\mathrm{H}_{\mathscr{L}}}(B) \sim C \cdot \log^{r/2} B\,.$$

3.10. Remark ($K3$ surfaces—known results). — On the other hand, for $K3$ surfaces, the conjecture of Batyrev and Manin is open. Weak versions of the conjecture have been established only in some particular cases.

i) For special types of $K3$ surfaces, most notably for Kummer surfaces associated to a product of two elliptic curves, a particular result has been obtained by D. McKinnon [**McK00**]. If d is the minimal degree of a rational curve on X, then $N_{X^\circ,\mathrm{H}_{\mathscr{L}}}(B) \ll B^{2/d}$ for X° the complement of the union of all rational curves on X of degree d.

ii) An estimate of the same type was established by H. Billard [**Bill**, Théorème 4.1] for $K3$ surfaces given as a smooth hypersurface of multidegree $(2,2,2)$ in $\mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1$.

3.11. Remark. — Actually, for $K3$ surfaces, the Batyrev–Manin conjecture is implied by a very general conjecture due to P. Vojta [**McK11**].

3.12. Observation. — There are examples of $K3$ surfaces over a number field k that contain infinitely many rational curves defined over k [**Bill**, Sec. 3]. Let X be such a $K3$ surface, and let $C_1, C_2, \ldots$ be rational curves on X. Denote their degrees by $d_1, d_2, \ldots$. Assume that the curves are listed in such a way that the degrees are in ascending order.

Then, on

$$X_l^\circ := X \backslash C_1 \backslash \ldots \backslash C_{l-1} \,,$$

there are still $\geq c_l \, B^{2/d_l}$ k-rational points to be expected. Indeed, X_l° contains a non-empty, open subset of C_l.

In other words, there is no way to choose a uniform Zariski open subset $X^\circ \subset X$ such that

$$N_{X^\circ, \mathrm{H}_{\mathscr{L}}}(B) = \#\{x \in X^\circ(k) \mid \mathrm{H}_{\mathscr{L}}(x) < B\} \ll B^\varepsilon$$

for every $\varepsilon > 0$. In order to fulfill the conjecture of Batyrev and Manin, one therefore has to choose X° in dependence of ε.

3.13. Example. — Consider the diagonal quartic surface X given in $\mathbf{P}^3_{\mathbb{Q}}$ by the equation

$$x^4 + 2y^4 = z^4 + 4w^4 \,.$$

On this $K3$ surface, there are the $\mathbb{Q}$-rational points $(1 : 0 : \pm 1 : 0)$ and

$$(\pm 1\,484\,801 : \pm 1\,203\,120 : \pm 1\,169\,407 : \pm 1\,157\,520) \,.$$

These are the only $\mathbb{Q}$-rational points on X known and the only $\mathbb{Q}$-rational points of (naive) height less than 10^8 [**EJ2, EJ3**].

A systematic search for $\mathbb{Q}$-rational points on the $K3$ surface X is described in Chapter V.

3.14. Remark. — Generally speaking, not much is known about the arithmetic of $K3$ surfaces. Nevertheless, in 1981, F. Bogomolov formulated a very optimistic conjecture.

3.15. Conjecture (F. Bogomolov, cf. [**Bo/T**]). — *Let X be a $K3$ surface over a number field k. Then every k-rational point on X lies on rational curve $C \subset X$ (defined over the algebraic closure $\overline{k}$).*

3.16. Remark. — In general, for varieties of intermediate type, it is known that the validity of the Batyrev-Manin conjecture extends from a variety to all its unramified coverings [**Mo-ta**, Proposition 5].

iii. *A somewhat different example.*

3.17. Example. — Let X be the blowup of $\mathbf{P}^2$ in nine points $P_1, \ldots, P_9$ in general position.

Denote by $E := E_1 + \ldots + E_9$ the sum of the corresponding nine exceptional lines. According to the Nakai–Moizhezon criterion, a divisor $aL - bE$ is ample if and only if $a > 3b > 0$. Further, we have $K = -3L + E$.

Let a and b be such that $aL - bE$ is ample. Then the conjecture of Batyrev and Manin therefore asserts that, for every $\varepsilon > 0$, there exists a Zariski open subset $X^\circ \subset X$ such that

$$N_{X^\circ, \mathrm{H}_{\mathscr{O}(aL-bE)}}(B) \ll B^{3/a+\varepsilon}.$$

On the other hand, assuming $aL - bE$ to be very ample for simplicity, the embedding $\iota\colon (X \twoheadrightarrow)\mathbf{P}^2 \hookrightarrow \mathbf{P}^N$ is given by homogeneous forms of degree a. Hence, $\mathrm{H}_{\mathscr{O}(aL-bE)}\big(\iota(x)\big) \leq c \cdot \mathrm{H}^a_{\mathrm{naive}}(x)$ for some constant c, which shows the lower bound

$$N_{X^\circ, \mathrm{H}_{\mathscr{O}(aL-bE)}}(B) = \Omega(B^{3/a})$$

for any Zariski open subset $X^\circ \subset X$.

3.18. — On X, there are infinitely many exceptional curves D such that $D^2 = -1$ and $DK = -1$. For every $d \in \mathbb{N}$, there are finitely many of the type $dL - a_1E_1 - \ldots - a_9E_9$.

Relative to $aL - bE$, their degrees are

$$\begin{aligned}(dL - a_1E_1 - \ldots - a_9E_9)(aL - bE) &= da - b(a_1 + \ldots + a_9)\\ &= da - b(3d-1)\\ &= d(a-3b) + b\,.\end{aligned}$$

Since $a - 3b > 0$, this expression tends to infinity for $d \to \infty$. Only finitely many of the exceptional curves are of degree $< \frac{2}{3}a$, which is equivalent to $\gg B^{3/a}$ rational points of height $< B$.

However, the closer to three we choose a/b, the more of the exceptional curves are accumulating subvarieties.

3.19. Remark. — What is interesting in this example is that X is a non-minimal surface, the minimal model of which is Fano. In particular, there are many rational points on X.

The only difference to the Fano case might seem to be that there is no distinguished height, which could be used in order to count them. The anticanonical sheaf is not ample.

However, there are, at least potentially, infinitely many accumulating subvarieties in analogy to the observations made for some $K3$ surfaces.

3.20. Problem. — Is it possible to describe the growth of $N_{X^\circ, \mathrm{H}_{\mathscr{O}(aL-bE)}}$ more accurately? At least for a particular choice of a and b? Is there a variant of Manin's conjecture for $\mathbf{P}^2$ blown up in nine points?

4. The conjecture of Manin

i. *Some general facts on the cohomology of Fano varieties.*

4.1. Fact. — *Let X be a smooth, projective variety over a field k of characteristic* 0. *Assume that X is Fano. Then*

$$H^i(X, \mathscr{O}_X) = 0$$

for every $i \geq 1$.

Proof. Denote the canonical invertible sheaf on X by $\mathscr{K}$. Then the vanishing theorem of Kodaira [**G/H**, Chapter 1, Section 2] ensures that

$$H^i(X, \mathscr{K} \otimes_{\mathscr{O}_X} \mathscr{L}) = 0$$

for every ample invertible sheaf $\mathscr{L} \in \mathrm{Pic}(X)$. Put $\mathscr{L} := \mathscr{K}^\vee$. □

4.2. Lemma. — *Let $k \subseteq \mathbb{C}$ be an algebraically closed field of characteristic* 0, *and let X be a smooth, projective variety over k. Assume that X is Fano.*

Then, for every prime number l,

i) $H^1_{\text{ét}}(X, \mathbb{Z}_l) = 0$.

ii) *The first Chern class induces an isomorphism*

$$\mathrm{Pic}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_l \stackrel{\cong}{\longrightarrow} H^2_{\text{ét}}(X, \mathbb{Z}_l(1)) \,.$$

Proof. Let first $i \in \mathbb{N}$ be arbitrary. By [**SGA4**, Exp. XVI, Corollaire 1.6], we have, for every $k \in \mathbb{N}$, $H^i_{\text{ét}}(X, \mu_{l^k}) \cong H^i_{\text{ét}}(X_\mathbb{C}, \mu_{l^k})$. Further, the comparison theorem [**SGA4**, Exp. XI, Théorème 4.4] shows that $H^i_{\text{ét}}(X_\mathbb{C}, \mu_{l^k}) \cong H^i(X(\mathbb{C}), \mathbb{Z}/l^k\mathbb{Z})$. On the other hand, by the universal coefficient theorem for cohomology [**Sp**, Chap. 5, Sec. 5, Theorem 10],

$$\begin{aligned} H^i(X(\mathbb{C}), \mathbb{Z}/l^k\mathbb{Z}) &\cong H^i(X(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/l^k\mathbb{Z} \oplus \mathrm{Tor}_1(H^{i+1}(X(\mathbb{C}), \mathbb{Z}), \mathbb{Z}/l^k\mathbb{Z}) \\ &\cong H^i(X(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/l^k\mathbb{Z} \oplus H^{i+1}(X(\mathbb{C}), \mathbb{Z})_{l^k} \,. \end{aligned}$$

Here, the transition maps $H^{i+1}(X(\mathbb{C}), \mathbb{Z})_{l^{k+1}} \to H^{i+1}(X(\mathbb{C}), \mathbb{Z})_{l^k}$ are given by multiplication by l. A finite composition of them is the zero map. This implies

$$\begin{aligned} H^i_{\text{ét}}(X, \mathbb{Z}_l(1)) &\cong \varprojlim H^i(X(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/l^k\mathbb{Z} \\ &= H^i(X(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_l \,. \end{aligned} \qquad (\ddagger)$$

i) Since $H^1(X(\mathbb{C}), \mathscr{O}_{X(\mathbb{C})}) = 0$, the long exact cohomology sequence associated to the exponential sequence yields that $H^1(X(\mathbb{C}), \mathbb{Z}) = 0$. Formula (‡) implies the claim.

ii) Here, we use both, $H^1(X(\mathbb{C}), \mathscr{O}_{X(\mathbb{C})}) = 0$ and $H^2(X(\mathbb{C}), \mathscr{O}_{X(\mathbb{C})}) = 0$. The long exact cohomology sequence associated to the exponential sequence then shows that

$$c_1\colon \operatorname{Pic}(X) \longrightarrow H^2(X(\mathbb{C}), \mathbb{Z})$$

is an isomorphism. Tensoring yields isomorphisms

$$\operatorname{Pic}(X) \otimes_{\mathbb{Z}} \mathbb{Z}/l^k\mathbb{Z} \longrightarrow H^2(X(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/l^k\mathbb{Z}\,,$$

and going over to the inverse limit implies the assertion. □

4.3. Remarks. — i) The first Chern class in étale cohomology is defined using the Kummer sequence. Recall that there is the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{2\pi i} & \mathscr{O}_X & \xrightarrow{\exp} & \mathscr{O}_X^* & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \exp(\frac{2\pi i}{n}\cdot)} & & \downarrow{\scriptstyle \exp(\frac{1}{n}\cdot)} & & \downarrow{=} & & \\ 0 & \longrightarrow & \mu_n & \longrightarrow & \mathscr{O}_X^* & \xrightarrow{(\cdot)^n} & \mathscr{O}_X^* & \longrightarrow & 0 \end{array}$$

showing that this agrees with the definition based on the exponential sequence.

ii) The tensor product does not, in general, commute with inverse limits. However, for a finitely generated $\mathbb{Z}$-module A,

$$\varprojlim A \otimes_{\mathbb{Z}} \mathbb{Z}/l^k\mathbb{Z} \cong A \otimes_{\mathbb{Z}} \mathbb{Z}_l$$

is the l-adic completion of A [**Mat**, Theorem 8.7].

ii. *Fixing a particular anticanonical height.*

4.4. Remark. — The anticanonical height $\mathrm{H}_{\mathscr{K}^\vee}$ on X is determined only up to a certain factor that is bounded above and below by positive constants. To be able to make any statement on the value of the constant τ, we have to fix a particular height function.

4.5. — For this, according to Definition I.4.22, it is necessary to choose an adelic metric $\|\,.\| = \{\|\,.\|_\nu\}_{\nu \in \mathrm{Val}(\mathbb{Q})}$ on $\mathscr{K}^\vee$.

For the remainder of this section, we fix such an adelic metric once and for all.

4.6. Definition. — Put

$$\mathrm{H}_{\mathscr{K}^\vee}(x) := \exp \mathrm{h}_{(\mathscr{K}^\vee, \|\,.\|)}(x)$$

for $\mathrm{h}_{(\mathscr{K}^\vee, \|\,.\|)}$ the absolute height with respect to the adelically metrized invertible sheaf $(\mathscr{K}^\vee, \|\,.\|) \in \widetilde{\operatorname{Pic}}(X)$ in the sense of the definition in Subsection I.4.22.

We will call this height function the anticanonical height *defined by* the adelic metric given in 4.5.

4.7. — Most height functions occurring in practice are a lot simpler than the general theory. For this reason, it is probably wise to recall an elementary particular case.

Choose

i) a projective embedding $\iota\colon X \to \mathbf{P}^N_{\mathbb{Q}}$ such that $\mathscr{K}^\vee \cong \iota^*\mathscr{O}(d)$ for some $d \in \mathbb{N}$, and

ii) a continuous hermitian metric $\|\,.\|_\infty$ on $\mathscr{K}^\vee_{\mathbb{C}}$.

Then the topological closure of $\iota(X)$ in $\mathbf{P}^N_{\mathbb{Z}}$ is an arithmetic variety $\mathscr{X}$, that is a model of X over $\operatorname{Spec}\mathbb{Z}$.

Put

$$\mathrm{H}_{\mathscr{K}^\vee}(x) := \exp \mathrm{h}_{(\mathscr{O}(d)|_{\mathscr{X}},\|\,.\|_\infty)}(x)$$

for $\mathrm{h}_{(\mathscr{O}(d)|_{\mathscr{X}},\|\,.\|_\infty)}$ the height function with respect to the hermitian line bundle $(\mathscr{O}(d)|_{\mathscr{X}}, \|\,.\|_\infty) \in \widehat{\operatorname{Pic}}^{C^0}(X)$ in the sense of the Definition in Subsection I.3.12.

4.8. — This height function corresponds to the adelic metric on $\mathscr{K}^\vee$, which is given by the following construction. (Cf. Example I.4.5.)

i) $\|\,.\|_\infty$ is part of the data given.

ii) For a prime number p, the metric $\|\,.\|_p$ is given as follows.

Let $x \in \overline{\mathbb{Q}}_p$. There is a unique extension $\overline{x}\colon \operatorname{Spec}\mathscr{O}_{\overline{\mathbb{Q}}_p} \to \mathscr{X}$ of x. Then $\overline{x}^*\mathscr{O}(d)$ is a projective $\mathscr{O}_K$-module of rank one. Each $l \in \mathscr{O}(d)(x)$ induces a rational section of $\overline{x}^*\mathscr{O}(d)$. Put

$$\|l\|(x) := \inf\{|\,a| \mid a \in K,\ l \in a \cdot \overline{x}^*\mathscr{O}(d)\}\,.$$

4.9. Remarks. — i) To define the metric $\|\,.\|_p$ for a particular prime p, a model $\mathscr{L}$ of X over $\operatorname{Spec}\mathbb{Z}[\frac{1}{m}]$ for $p\nmid m$ is sufficient.

ii) For every adelic metric $\|\,.\| = \{\|\,.\|_\nu\}_{\nu\in\mathrm{Val}(\mathbb{Q})}$ on $\mathscr{K}^\vee$, there exist a model $\mathscr{X}$ of X over $\operatorname{Spec}\mathbb{Z}[\frac{1}{m}]$ for a certain $m \in \mathbb{N}$ and an extension of $\mathscr{K}^\vee$ to $\mathscr{X}$ such that $\|\,.\|_{\nu_p}$ is induced by that model for every $p\nmid m$.

iii. *The conjecture.*

4.10. — The conjecture of Manin deals with the anticanonical height $\mathrm{H}_{\mathscr{K}^\vee}$ on a Fano variety.

4.11. Conjecture (Manin). — *Let X be a smooth, projective variety over $\mathbb{Q}$. Assume that X is Fano.*

Then there exist a positive integer r, a real number τ, and a Zariski open subset $X^\circ \subseteq X$ such that

$$N_{X^\circ,\mathrm{H}_{\mathscr{K}^\vee}}(B) = \#\{x \in X^\circ(\mathbb{Q}) \mid \mathrm{H}_{\mathscr{K}^\vee}(x) < B\} \sim \tau B \log^r B\,,$$

for $B \to \infty$.

4.12. Remarks. — i) The factor $\log^r B$ is new in comparison with the statistical heuristic given in 1.4. It has been known for a long time that such a factor is, in general, necessary. In fact, J. Franke, Yu. I. Manin, and Y. Tschinkel [**F/M/T**] showed in 1989 that Manin's conjecture becomes compatible with direct products of Fano varieties only when a suitable $\log^r B$-factor is added.

ii) At least in the case that X is a surface, it is expected that $r = \operatorname{rk}\operatorname{Pic}(X) - 1$. There are, however, counterexamples to this formula in dimension three [**Ba/T96**].

iii) On the other hand, in Chapter VI, we will present numerical evidence for Manin's conjecture for diagonal cubic and quartic threefolds. For those, $\operatorname{rk}\operatorname{Pic}(X) = 1$, and our experiments indicate that $r = 0$.

4.13. Remarks. — i) In this book, we shall not prove Manin's conjecture in any non-trivial case. Nevertheless, Section 8 will contain some information on the methods of proof, working in particular situations, as they are available today.

ii) In addition to the references given there, we recommend that the reader study the survey lecture of E. Bombieri [**Bom**], which originates from the *Journées Arithmétiques* at Edinburgh in 2007. It is concerned with various aspects of rational and algebraic points on algebraic varieties, including evidence for Manin's conjecture, proven cases, and related questions.

5. Peyre's constant I—the factor α

5.1. — In [**Pe95a**], E. Peyre refined Manin's conjecture by providing an explicit description for the value of the coefficient τ. Peyre's constant is a product of several factors, which we will subsequently explain.

5.2. Definition (Cf. [**Pe95a**, Définition 2.4]). — Let X be a projective algebraic variety over $\mathbb{Q}$. Choose an isomorphism

$$\iota\colon \operatorname{Pic}(X)/\operatorname{Pic}(X)_{\text{tors}} \xrightarrow{\cong} \mathbb{Z}^t.$$

Identify $\operatorname{Pic}(X)\otimes_{\mathbb{Z}}\mathbb{R}$ with $\mathbb{R}^t$ according to ι.

Further, let $\Lambda_{\text{eff}}(X) \subset \operatorname{Pic}(X)\otimes_{\mathbb{Z}}\mathbb{R} = \mathbb{R}^t$ be the cone generated by the effective divisors. Consider the dual cone $\Lambda^\vee_{\text{eff}}(X) \subset (\mathbb{R}^t)^\vee$. Then

$$\alpha(X) := t \cdot \operatorname{vol}\{\, x \in \Lambda^\vee_{\text{eff}} \mid \langle x, -K\rangle \leq 1 \,\}.$$

Here, $\langle\,.\,,.\rangle$ denotes the tautological pairing $\langle\,.\,,.\rangle\colon (\mathbb{R}^t)^\vee \times \mathbb{R}^t \to \mathbb{R}$, and vol is the ordinary Lebesgue measure on $(\mathbb{R}^t)^\vee$.

5.3. Remark. — In [**Pe/T**, Definition 2.5], $\alpha(X)$ is defined by an integral. An elementary calculation shows that the two definitions are equivalent.

5.4. Example. — Suppose $\operatorname{Pic}(X) = \mathbb{Z}$. Denote by $[L] \in \operatorname{Pic}(X)$ the ample generator. Let $\delta \in \mathbb{N}$ be such that $[-K] = \delta[L]$. Then $\alpha(X) = 1/\delta$.

In particular, one has $\alpha(X) = 1$ for every smooth cubic surface such that $\operatorname{rk}\operatorname{Pic}(X) = 1$. Indeed, $(-K)^2 = 3$ is square-free. Therefore, $[-K] \in \operatorname{Pic}(X)$ is not divisible.

CHAPTER V

The Diophantine equation $x^4 + 2y^4 = z^4 + 4w^4$*

Hash, x. There is no definition for this word—nobody knows what hash is.

AMBROSE BIERCE: The Devil's Dictionary (1906)

Numerical experiments and the Manin conjecture

Part C of this book is devoted to experiments related to the conjecture of Manin, and in the refined form due to E. Peyre. It mainly consists of two chapters, each of which presents the investigations on one or two particular samples of varieties. In addition, there is the present chapter, which is introductory.

The experiments we are going to report about were carried out by Andreas-Stephan Elsenhans together with the author. Our selection of subjects was, of course, arbitrary to a certain extent. We do not claim it was mandatory in any sense to consider exactly the samples we considered. Nor do we want to give the reader the impression that nobody else ever made experiments related to the Manin conjecture.

To the contrary, important experiments have been accomplished, for instance, by D. R. Heath-Brown [**H-B92a**]. He studied cubic surfaces where weak approximation fails. Heath-Brown's investigations brought to light the fact that the failure of weak approximation is no reason to expect a slower growth of the number of $\mathbb{Q}$-rational points. The main term from the circle method, carried over in the most naive manner that one can think of, seemed to fit perfectly well in the examples, presented in [**H-B92a**]. Cf. Remark II.7.5.iv) in the first part of the book.

Later on, E. Peyre and Y. Tschinkel [**Pe/T**] dealt with the situation in which there is a non-trivial Brauer group, but the Brauer–Manin obstruction does not exclude any adelic point. Their experiments demonstrated that on such Fano varieties (cubic surfaces, actually, in their experiments), there are more $\mathbb{Q}$-rational points than naively expected, in their case well by a factor of three. This showed that any serious definition of what today is called Peyre's constant must take the factor β into account.

In general, experimenting on Manin's conjecture includes calculating Peyre's constant and searching for $\mathbb{Q}$-rational points. To calculate Peyre's constant, one may

*This chapter collects material from the articles:
The Diophantine equation $x^4 + 2y^4 = z^4 + 4w^4$, *Math. Comp.* **75** (2006), 935–940; and
The Diophantine equation $x^4 + 2y^4 = z^4 + 4w^4$—a number of improvements, *Preprint*, both with A.-S. Elsenhans and the author.

essentially proceed according to the definition. The most interesting point is certainly the computation of the special value of the L-function at 1. But even for this, the main ideas go back at least to the 1960s, cf. Remark VII.6.6 below.

On the other hand, algorithmic resolution of Diophantine equations is a very interesting and active field. To get an overview of the state of the art in the year 1998, we refer to the book of N. P. Smart [**Sm**]. Further, M. J. Bright's experiments with diagonal quartic surfaces [**Bri02**] are of significant interest, albeit in this case the relevant arithmetic conjectures are wide open.

The present chapter is devoted to the Diophantine equation $x^4 + 2y^4 = z^4 + 4w^4$. As this defines a $K3$ surface, the conjecture of Batyrev-Manin would apply and, in fact, all the major questions concerning the arithmetic of this surface are open. However, the extreme sparsity of the solutions prevents us even from making an educated guess concerning their asymptotics.

In fact, the goal of Chapter V is entirely different. The truth is, we use that particular equation mainly in order to present in detail our algorithm for the resolution of Diophantine equations. This algorithm works in general for *decoupled* equations. In this situation, it runs significantly faster than the methods applicable in general. It is related to the algorithm of Daniel Bernstein [**Be**].

The two main chapters of this part describe our experiments related to the Manin conjecture for some particular samples of varieties, diagonal cubic and quartic threefolds, and diagonal cubic surfaces. As all these are given by decoupled equations, we may apply our algorithm to efficiently search for $\mathbb{Q}$-rational points.

Generally speaking, Part C is most likely easier to follow than the others, in particular for all those readers who are well acquainted with computers and the concept of an algorithm. Let us emphasize, for example, that Chapter V does not require any of the advanced prerequisites listed on the very first pages of this book. Further, each of the chapters starts with an introduction that tries to make it accessible even for a reader who did not study Parts A and B very well.

1. Introduction

1.1. — Chapter II was devoted to very general conjectures on rational points on algebraic varieties. Let us briefly recall a few facts.

i) An algebraic curve C of genus $g > 1$ over $\mathbb{Q}$ admits at most a finite number of $\mathbb{Q}$-rational points. On the other hand, for genus one curves, $\#C(\mathbb{Q})$ may be zero, finite non-zero, or infinite. For genus zero curves, one automatically has $\#C(\mathbb{Q}) = \infty$ as soon as $C(\mathbb{Q}) \neq \emptyset$.

ii) In higher dimensions, there is a conjecture, due to S. Lang, stating that if X is a variety of general type over a number field, then all but finitely many of its rational points are contained in the union of closed subvarieties that are not of general type (cf. Conjecture II.2.2). On the other hand, abelian varieties (as well as, e.g., elliptic and bielliptic surfaces) behave like genus one curves. I.e., $\#X(\mathbb{Q})$ may be zero, finite non-zero, or infinite. Finally, rational and ruled varieties comport in the same way as curves of genus zero in this respect.

This list does not yet exhaust the classification of algebraic surfaces, to say nothing of dimension three or higher. In particular, the following problem is still open.

1.2. Problem. — *Does there exist a $K3$ surface X over $\mathbb{Q}$ that has a finite non-zero number of $\mathbb{Q}$-rational points? I.e., such that $0 < \#X(\mathbb{Q}) < \infty$?*

1.3. Remark. — This question was posed by Sir Peter Swinnerton-Dyer as Problem/Question 6.a) in the problem session to the workshop [**Poo/T**]. We are not able to give an answer to it.

1.4. — One possible candidate for a $K3$ surface with the property $0 < \#X(\mathbb{Q}) < \infty$ is given by the following.

Problem. *Find a third point on the projective surface $X \subset \mathbf{P}^3$ defined by*

$$x^4 + 2y^4 = z^4 + 4w^4.$$

1.5. Remarks. — i) The Problem in Subsection 1.4 is also due to Sir Peter Swinnerton-Dyer [**Poo/T**, Problem/Question 6.c)]. It was raised, in particular, during his talk [**SD04**, very end of the article] at the Göttingen Mathematisches Institut on June 2, 2004.

ii) $x^4 + 2y^4 = z^4 + 4w^4$ is a homogeneous quartic equation. It, therefore, defines a $K3$ surface X in $\mathbf{P}^3$. As trivial solutions of the equation, we consider those corresponding to the $\mathbb{Q}$-rational points $(1\!:\!0\!:\!1\!:\!0)$ and $(1\!:\!0\!:\!(-1)\!:\!0)$.

iii) Our main result is the following theorem, which contains an answer to Problem 1.4.

1.6. Theorem. — *The diagonal quartic surface X in $\mathbf{P}^3$ given by*

$$x^4 + 2y^4 = z^4 + 4w^4 \qquad (*)$$

admits precisely ten $\mathbb{Q}$-rational points having integral coordinates within the hypercube $|x|, |y|, |z|, |w| < 10^8$.

These are $(\pm 1\!:\!0\!:\!\pm 1\!:\!0)$ *and* $(\pm 1\,484\,801\!:\!\pm 1\,203\,120\!:\!\pm 1\,169\,407\!:\!\pm 1\,157\,520)$.

1.7. Remark. — This result clearly does not exclude the possibility that $\#X(\mathbb{Q})$ is actually finite. It might indicate, however, that a proof for this property is deeper than one originally hoped for.

2. Congruences

2.1. — It seems natural to first try to understand the congruences

$$x^4 + 2y^4 \equiv z^4 + 4w^4 \pmod{p} \qquad (\dagger)$$

modulo some prime number p. For $p = 2$ and 5, one finds that all primitive solutions in $\mathbb{Z}$ satisfy

a) x and z are odd,

b) y and w are even,

c) y is divisible by 5.

For other primes, it follows from the Weil conjectures, proven by P. Deligne [**Del**], that the number of solutions of the congruence (†) is

$$\#CX(\mathbb{F}_p) = 1 + (p-1)(p^2 + p + 1 + E) = p^3 + E(p-1)\,.$$

Here, E is an error-term, which may be estimated by $|E| \leq 21p$.

Indeed, consider the projective variety X over $\mathbb{Q}$ defined by $(*)$. It has good reduction at every prime $p \neq 2$. Therefore, [**Del**, Théorème (8.1)] may be applied to the reduction X_p. This yields $\#X_p(\mathbb{F}_p) = p^2+p+1+E$ and $|E| \leq 21p$. We note that $\dim H^2(\mathscr{X}, \mathbb{R}) = 22$ for every complex surface $\mathscr{X}$ of type $K3$ [**Bv**, p. 98].

2.2. — Another question of interest is to count the numbers of solutions to the congruences $x^4 + 2y^4 \equiv c \pmod p$ and $z^4 + 4w^4 \equiv c \pmod p$ for a certain $c \in \mathbb{Z}$.

This means that we count the $\mathbb{F}_p$-rational points on the affine plane curves C^l_c and C^r_c defined over $\mathbb{F}_p$ by $x^4 + 2y^4 = \overline{c}$ and $z^4 + 4w^4 = \overline{c}$, respectively. If $p \nmid c$ and $p \neq 2$, then these are smooth curves of genus three.

By the work of André Weil [**We48**, Corollaire 3 du Théorème 13], the numbers of $\mathbb{F}_p$-rational points on their projectivizations are given by

$$\#\overline{C}^l_c(\mathbb{F}_p) = p + 1 + E_l \qquad \text{and} \qquad \#\overline{C}^r_c(\mathbb{F}_p) = p + 1 + E_r,$$

where the error-terms can be bounded by $|E_l|, |E_r| \leq 6\sqrt{p}$. There may be up to four $\mathbb{F}_p$-rational points on the infinite line. For our purposes, it suffices to notice that both congruences admit a number of solutions that is close to p.

The case $p|c$, $p \neq 2$, is slightly different since it corresponds to the case of a reducible curve. The congruence $x^4 + ky^4 \equiv 0 \pmod p$ admits only the trivial solution if $(-k)$ is not a biquadratic residue modulo p. Otherwise, it has exactly $1 + (p-1)\gcd(p-1, 4)$ solutions.

Finally, if $p = 2$, then $\#C^l_0(\mathbb{F}_2) = \#C^l_1(\mathbb{F}_2) = \#C^r_0(\mathbb{F}_2) = \#C^r_1(\mathbb{F}_2) = 2$.

2.3. Remark. — The number of solutions of the congruence (†) is

$$\#CX(\mathbb{F}_p) = \sum_{c \in \mathbb{F}_p} \#C^l_c(\mathbb{F}_p) \cdot \#C^r_c(\mathbb{F}_p).$$

Hence, the formulas just mentioned yield an elementary estimate for that count. They show once more that the dominating term is p^3. The estimate for the error is, however, less sharp than the one obtained via the more sophisticated methods in 2.1.

3. Naive methods

3.1. — The most naive method to search for solutions of $(*)$ is probably the following. Start with the set

$$\{(x, y, z, w) \in \mathbb{Z} \mid 0 \leq x, y, z, w \leq N\}$$

and test the equation for every quadruple.

Obviously this method requires about N^4 steps. It can be accelerated using the congruence conditions for primitive solutions noticed above.

3.2. — A somewhat better method is to start with the set

$$\{x^4 + 2y^4 - 4w^4 \mid x, y, w \in \mathbb{Z}, 0 \leq x, y, w \leq N\}$$

and to search for fourth powers. This set has about N^3 elements, and the algorithm takes about N^3 steps. Again, it can be sped up by the above congruence conditions for primitive solutions. We used this approach for a trial run with $N = 10^4$.

An interesting aspect of this algorithm is the optimization by further congruences. Suppose x and y are fixed. Then about one half or three-quarter of the values for w are no solutions to the congruence modulo a new prime. Following this way, one can find more congruences for w and the size of the set may be reduced by a constant factor.

4. An algorithm to efficiently search for solutions

i. *The basic idea.*

4.1. — We need to compute the intersection of two sets

$$\{x^4 + 2y^4 \mid x, y \in \mathbb{Z}, 0 \leq x, y \leq N\} \cap \{z^4 + 4w^4 \mid z, w \in \mathbb{Z}, 0 \leq z, w \leq N\}.$$

Both have about N^2 elements.

It is a standard problem in computer science to find the intersection of two sets that both fit into memory. Using the congruence conditions modulo 2 and 5, one can reduce the size of the first set by a factor of 20 and the size of the second set by a factor of 4.

ii. *Some details.*

4.2. — The two sets described above are too big, at least for our computers and interesting values of N. Therefore, we introduced a prime number p_p, which we call the *page prime.*

Define the sets

$$L_c := \{x^4 + 2y^4 \mid x, y \in \mathbb{Z}, 0 \leq x, y \leq N, x^4 + 2y^4 \equiv c \pmod{p_p}\}$$

and

$$R_c := \{z^4 + 4w^4 \mid z, w \in \mathbb{Z}, 0 \leq z, w \leq N, z^4 + 4w^4 \equiv c \pmod{p_p}\}.$$

This means the intersection problem is divided into p_p pieces and the sets L_c and R_c fit into the computer's memory if p_p is big enough. We worked with $N = 2.5 \cdot 10^6$ and chose $p_p = 30\,011$.

For every value of c, our program computes L_c and stores this set in a hash table. Then it determines the elements of R_c and looks them up in the table. Assuming uniform hashing, the expected running-time of this algorithm is $O(N^2)$.

4.3. Remark — An important further aspect of this approach is that the problem may be attacked in parallel on several machines. The calculations for one particular value of c are independent of the analogous calculations for another one. Thus, it is possible, say, to let c run from 0 to $(p_p - 1)/2$ on one machine and, at the same time, from $(p_p + 1)/2$ to $(p_p - 1)$ on another.

iii. *Some more details.*

4.4. (*The page prime*). — For each value of c, it is necessary to find the solutions of the congruences $x^4 + 2y^4 \equiv c \pmod{p_p}$ and $z^4 + 4w^4 \equiv c \pmod{p_p}$ in an efficient manner. We do this in a rather naive way by letting y (w) run from 0 to $p_p - 1$. For each value of y (w), we compute x^4 (z^4). Then we extract the fourth root modulo p_p.

Note that the page prime fulfills $p_p \equiv 3 \pmod 4$. Hence, the fourth roots of unity modulo p are just ± 1 and, therefore, a fourth root modulo p_p, if it exists, is unique up to sign. This makes the algorithm easier to implement.

4.5. — Actually, we do not execute any modular powering operation or even computation of fourth roots in the lion's share of the running-time. For more efficiency, all fourth powers and all fourth roots modulo p_p are computed and stored in an array during an initialization step. Thus, the main speed limitation to find all solutions to a congruence modulo p_p is, in fact, the time it takes to look up values stored in the machine's main memory.

4.6. (*Hashing*). — We do not compute L_c and R_c directly, because this would require the use of multiprecision integers within the inner loop. Instead, we choose two other primes, the hash prime p_h and the control prime p_c, which fit into the 32-bit registers of our computers. All computations are done modulo p_h and p_c.

More precisely, for each pair (x, y) considered, the expression

$$\big((x^4 + 2y^4) \bmod p_h\big)$$

defines its position in the hash table. In other words, we hash pairs (x, y) whereas $(x, y) \mapsto \big((x^4+2y^4) \bmod p_h\big)$ plays the role of the hash function. For each pair (x, y), we write two entries into the hash table, namely the value of $\big((x^4 + 2y^4) \bmod p_c\big)$ and the value of y.

In the main computation, we worked with the numbers $p_h = 25\,000\,009$ for the hash prime and $p_c = 400\,000\,009$ for the control prime.

4.7. — Note that, when working with a particular value of c, there are around p_p pairs $((x \bmod p_p), (y \bmod p_p))$ that fulfill the required congruence

$$x^4 + 2y^4 \equiv c \pmod{p_p}.$$

Therefore, approximately

$$p_p \cdot \left(\tfrac{N/2}{p_p} \cdot \tfrac{N/10}{p_p}\right) = \tfrac{N^2}{20p_p}$$

values will be written into the table. For our choices, $\frac{N^2}{20p_p} \approx 10\,412\,849$, which means that the hash table will get approximately 41.7% filled.

As for many other rules, there is an exception to this one. If $c = 0$, then approximately $1 + (p_p - 1)\gcd(p_p - 1, 4)$ pairs $((x \bmod p_p), (y \bmod p_p))$ may satisfy the congruence

$$x^4 + 2y^4 \equiv 0 \pmod{p_p}.$$

As $p_p \equiv 3 \pmod 4$ this is not more than $2p_p - 1$, and the hash table will be filled not more than about 83.3%.

4.8. — To resolve collisions within the hash table, we use an open addressing method. We are not particularly afraid of clustering and choose linear probing. We feel free to use open addressing as, thanks to the Weil conjectures, we have a priori estimates available for the load factor.

4.9. — The program makes frequent use of fourth powers modulo p_h and p_c. Again, we compute these data in the initialization part of our program and store them in arrays, once and for all.

5. General formulation of the method

5.1. — The method described in the previous section is actually a systematic method to search for solutions of a Diophantine equation. It works efficiently when the equation is of the form

$$f(x_1, \ldots, x_n) = g(y_1, \ldots, y_m).$$

We find all solutions that are contained within the $(n + m)$-dimensional cube

$$\{(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{Z}^{n+m} \mid |x_i|, |y_i| \leq B\}.$$

The expected running-time of the algorithm is $O(B^{\max\{n,m\}})$.

5.2. — The basic idea may be formulated as follows.

Algorithm H.

i) Evaluate f on all points of the n-dimensional cube

$$\{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid |x_i| \leq B\}.$$

Store the values within a set L.

ii) Evaluate g on all points of the cube

$$\{(y_1, \ldots, y_m) \in \mathbb{Z}^m \mid |y_i| \leq B\}$$

of dimension m. For each value start a search in order to find out whether it occurs in L. When a coincidence is detected, reconstruct the corresponding values of $x_1, \ldots, x_n$ and output the solution.

5.3. Remarks. — a) In fact, we are interested in the very particular Diophantine equation

$$x^4 + 2y^4 = z^4 + 4w^4,$$

which was suggested by Sir Peter Swinnerton-Dyer.

b) i) In the form stated above, the main disadvantage of Algorithm H is that it requires an enormous amount of memory. Actually, the set L is too big to be stored in the main memory even of our biggest computers, already when the value of B is only moderately large.

For that reason, we introduced the idea of *paging.* We choose a *page prime* p_p and work with the sets $L_r := \{s \in L \mid s \equiv r \pmod{p_p}\}$ for $r = 0, \ldots, p_p - 1$, separately. At the cost of some more time spent on initializations, this yields a reduction of the memory space required by a factor of $\frac{1}{p_p}$.

ii) The sets L_r were implemented in the form of a hash table with open addressing.

iii) It is possible to achieve a further reduction of the running-time and the memory required by making use of some obvious congruence conditions modulo 2 and 5.

5.4. — The goal of the remainder of this chapter is to describe an improved implementation of Algorithm H, which we used in order to find all solutions of $x^4 + 2y^4 = z^4 + 4w^4$, contained within the hypercube $\{(x, y, z, w) \in \mathbb{Z}^4 \mid |x|, |y|, |z|, |w| \leq 10^8\}$.

6. Improvements I—more congruences

6.1. — The most obvious way to further reduce the size of the sets L_r and to increase the speed of Algorithm H is to find further congruence conditions for solutions and evaluate f and g only on points satisfying these conditions. As the equation we are interested in is homogeneous, it is sufficient to restrict consideration to primitive solutions.