HEIGHTS ON ELLIPTIC CURVES AND THE DIOPHANTINE EQUATION $x^4 + y^4 = cz^4$

Grigor Grigorov
Jordan Rizov

Sofia University

January 10, 1998

Abstract. In this paper we give sharp explicit estimates for the difference of the Weil height and the Néron – Tate height on the elliptic curve $v^2 = u^3 - cu$. We then apply this in the proof of the fact that if $c > 2$ is a fourth power free integer and the rank of $v^2 = u^3 - cu$ is 1 then the equation $x^4 + y^4 = cz^4$ has no nonzero solutions in integers.

1. Heights on the Elliptic Curve $v^2 = u^3 - cu$

In this section E is the elliptic curve $v^2 = u^3 - cu$, where $c \geq 1$ is a fourth power free integer. For a subgroup $\Gamma \subset E(\mathbb{Q})$, defined below, we give an absolute, independent of c bound for the difference between the Weil height and the Néron - Tate height.

Let Γ be $I \cap E_0(\mathbb{Q})$, where I and $E_0(\mathbb{Q})$ are defined as follows:

Over $\mathbb{R}$ the elliptic curve E consists of two components and $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as Lie groups (cf. Silverman [2, Ch.V §2]). We denote by I the identity component.

For a prime p dividing c the elliptic curve $E/\mathbb{Q}$ has additive reduction $\widetilde{E}_{(p)}$ with equation $v^2 = u^3$ and with one singular point $(0, 0)$. We define $E_0(\mathbb{Q})$ to be the subgroup of E consisting of all $P \in E(\mathbb{Q})$ such that $\widetilde{P}$ is a nonsingular point of $\widetilde{E}_{(p)}$ for all prime p.

In other words

$$\Gamma = \{P \in E(\mathbb{Q}) \mid u(P) = \frac{s}{t}, s \geq t \geq 0, \gcd(s,t) = 1 \text{ and } \gcd(s,c) = 1\}.$$

As we will see Γ is a subgroup of $E(\mathbb{Q})$ of finite index (Corollary 1.8 below).

In what follows we frequently use the duplication formula:

If $P = (u_0, v_0) \in E$ then

$$u(2P) = \frac{(u_0^2 + c)^2}{4v_0^2} = \frac{(u_0^2 + c)^2}{4u_0(u_0^2 - c)}.$$

The following Lemma is clear from the definitions.

1991 *Mathematics Subject Classification.* 11G30 11D25.

Key words and phrases. elliptic curves, canonical height, diophantine equation.

Lemma 1.1. a) *If $P \in E_0(\mathbb{Q})$ then $2P \in \Gamma$;*
b) *If $P \in \Gamma$ then $u(P) \geq \sqrt{c}$.*

Proof. a) From $P \in E(\mathbb{R})$ follows that $2P \in I$ and consequently $2P \in I \cap E_0(\mathbb{Q}) = \Gamma$;
b) If $P \in \Gamma$ then $P \in I$ and for all these points $u(P) \geq \sqrt{c}$. $\square$

We denote by $H_u(P)$ the u – coordinate height of P. Respectively the logarithmic height is denoted by h_u, and $\hat{h}$ is the Néron – Tate (canonical) height.

Proposition 1.2. *Let $P \in \Gamma$, then*

$$|h_u(2P) - 4h_u(P)| \leq 3\log 2.$$

Proof. Let $P \in \Gamma$ and $u(P) = \frac{s}{t}$, where s and t are relatively prime natural numbers. From Lemma 1.1 b) $s \geq \sqrt{c}t \geq t$, so that $H_u(P) = s$. We have

$$u(2P) = \frac{(s^2 + ct^2)^2}{4st(s^2 - ct^2)}.$$

Let $q \geq 3$ be a prime number, dividing booth the numerator and the denominator of $u(2P)$. Then q divides booth s and c, which is contradiction with the fact that $P \in \Gamma$. Consequently $\delta := \gcd((s^2 + ct^2)^2, 4st(s^2 - ct^2))$ is a power of 2.

Suppose now that $16|\delta$. Then $4|s^2 + ct^2$ and $4|st(s^2 - ct^2)$. If c is even then s is odd and this is impossible. If c is odd then s and t have to be odd, and 4 divides booth $s^2 + ct^2$ and $s^2 - ct^2$ – again a contradiction. Thus we see that $\delta \leq 8$.

For $P \in \Gamma$ the height $H_u(2P)$ is $\frac{(s^2+ct^2)^2}{\delta}$, and the logarithmic height is

$$h_u(2P) = 2\log(s^2 + ct^2) - \log\delta.$$

On the other hand from Lemma 1.1 b) $0 \leq ct^2 \leq s^2$, and consequently

$$2\log s^2 - \log\delta \leq h_u(2P) \leq 2\log(2s^2) - \log\delta \Longrightarrow$$

$$4h_u(P) - \log\delta \leq h_u(2P) \leq 4h_u(P) - \log\frac{\delta}{4} \Longrightarrow$$

$$|h_u(2P) - 4h_u(P)| \leq \log\delta \leq 3\log 2. \quad \square$$

Remark 1.3. In the applications in section 2 there is an additional restriction that $c \equiv 1, 2 \pmod 4$. In this case it is easily seen that $\delta \leq 4$ and therefore a stronger estimate $|h_u(2P) - 4h_u(P)| \leq 2\log 2$ holds. The same remark applies to most of the results below, but this improvements actually are unimportant for the proofs in the next section.

We use Proposition 1.2 for estimating the difference $|\hat{h}(P) - \frac{1}{2}h_u(P)|$ for the points P in Γ. The tool is:

Lemma 1.4. *Let S be a subset of $E(\mathbb{Q})$, such that if $P \in S$ then $2P \in S$. Suppose that there is a constant C, such that for all $P \in S$ there holds $|h_u(2P) - 4h_u(P)| \leq C$. Then*

$$|2\hat{h}(P) - h_u(P)| \leq \frac{C}{3}.$$

Proof. This is essentially Silverman [1, Ch.VIII §9], the proof of Th.9.3(e), where the wrong constant $C/4$ should be $C/3$. $\square$

Lemma 1.4 applied to $S = \Gamma$ and Proposition 1.2 give:

Theorem 1.5. *If $P \in \Gamma$, then* $|2\hat{h}(P) - h_u(P)| \leq \log 2$. $\square$

Remark 1.6. As was pointed out to us by Joseph Silverman one of the inequalities in this theorem can be generalized in the following way: Let A and B be integers and let $E/\mathbb{Q}$ be the elliptic curve with Weierstrass equation $v^2 = u^3 + Au + B$. Let $E_0(\mathbb{Q})$ be the subgroup of E consisting of all $P \in E(\mathbb{Q})$ such that $\widetilde{P}$ is a nonsingular point of $\widetilde{E}_{(p)}$ for all prime p. Then for $P \in E_0(\mathbb{Q})$ we have the estimate

$$-\frac{1}{8}h(j) - 0.973 \leq \hat{h}(P) - \frac{1}{2}h_u(P)$$

where j is the j–invariant of E. The proof is the same as in Example 2.2 in Silverman [3]. For our particular curves this gives

$$-2.252 \leq \hat{h}(P) - \frac{1}{2}h_u(P) \quad \text{if} \quad u(P) = \frac{s}{t}, \ \gcd(s,c) = 1.$$

Our estimates are -0.347 and -0.232, if in addition $c \equiv 1, 2 \pmod 4$ (see Remark 1.3), but they are valid only for $E_0(\mathbb{Q}) \cap I$.

When $P \in \Gamma$ Theorem 1.5 provides a bound for the difference $|\hat{h}(P) - \frac{1}{2}h_u(P)|$, which is independent of c. Of course an estimate valid for all $P \in E(\mathbb{Q})$ will depend on c. We will proof below that Γ is of finite index in $E(\mathbb{Q})$, which amounts to say something about the heights for all $P \in E(\mathbb{Q})$.

Lemma 1.7. *For $P \in E(\mathbb{Q})$ let $s(P)$ be the denominator of $u(P)$. Let $d := \gcd(s(P), c)$ and $d_1 := \gcd(s(2P), c)$. Then d_1 divides $\gcd(d, \frac{c}{d})$. In particular d_1^2 divides c.*

Proof. Let $u(P) = \frac{s}{t}$, where s and t are relatively prime. Also let $s = ds_1$ and $c = dc_1$, where $\gcd(s_1, c_1) = 1$. Then

$$u(2P) = \frac{(ds_1^2 + c_1t^2)^2}{4s_1t(ds_1^2 - c_1t^2)}$$

and d_1 divides $c = dc_1$ and $(ds_1^2 + c_1t^2)^2$, but $\gcd(s_1, c_1) = \gcd(t, d) = 1$ and consequently $d_1 | \gcd(d, c_1)^2$. Let us note now that $\gcd(d, c_1)$ appears in the denominator too, and consequently $d_1 | \gcd(d, c_1)$. $\square$

We apply this Lemma in the proof of the following statement:

Proposition 1.8. *Let P be a point of $E(\mathbb{Q})$. Then*
a) $4P \in \Gamma$;
b) *If c is squarefree then* $2P \in \Gamma$.

Proof. From the structure of $E(\mathbb{R})$, if $P \in E(\mathbb{Q})$ then $2P \in I$ and it is enough to prove that $4P \in E_0(\mathbb{Q})$ and $2P \in E_0(\mathbb{Q})$ if c is squarefree. This follows directly from the previous Lemma. $\square$

Remark 1.9. The existence of Néron models implies that an analogous fact is true for local fields (cf. Silverman [2, Ch.IV, §9 Table 4.1]). This also gives another proof of the Proposition. We just note that $E_0(\mathbb{Q})$ is the intersection of all $E_0(\mathbb{Q}_p)$ and consequently if $n \in \mathbb{Z}$ is such that $nE(\mathbb{Q}_p) \subset E_0(\mathbb{Q}_p)$ for all prime p then $nE(\mathbb{Q}) \subset E_0(\mathbb{Q})$.

Corollary 1.10. *The group* Γ *is of finite index in* $E(\mathbb{Q})$.

Proof. This group contains the group $4E(\mathbb{Q})$, which according to Mordell – Weil theorem is of finite index. □

As a combination of Theorem 1.5 and Proposition 1.8 we get the following result.

Proposition 1.11. *Let* $P \in E(\mathbb{Q})$.
a) *If* 4 *divides* m *then* $\left|\frac{1}{2}h_u(mP) - \hat{h}(mP)\right| \leq \frac{\log 2}{2}$. *If* c *is squarefree the same holds for* m *– even*;
b) $\left|\hat{h}(P) - \frac{h_u(4P)}{32}\right| \leq \frac{\log 2}{32}$ *and if* c *is squarefree then* $\left|\hat{h}(P) - \frac{h_u(2P)}{8}\right| \leq \frac{\log 2}{8}$.

Proof. a) For such m from Proposition 1.7 $mP \in \Gamma$ and we can just apply Theorem 1.5.
b) is a) applied for $m = 4$ and $m = 2$ respectively. □

2. The Diophantine Equation $x^4 + y^4 = cz^4$ – Main Result

The equation $x^4 + y^4 = cz^4$ defines a smooth curve C of genus 3. If

$$E : v^2 = u^3 - cu$$

is the elliptic curve considered in section 1 then there exist two morphisms φ_1,$\varphi_2 : C \longrightarrow E$,

$$\varphi_1(x, y, z) = \left(-\frac{x^2}{z^2}, \frac{xy^2}{z^3}\right),$$

$$\varphi_2(x, y, z) = \left(-\frac{y^2}{z^2}, \frac{yx^2}{z^3}\right).$$

Note that x, y, z are projective and u, v are affine coordinates.

The Jacobian of C is isogenious to the product of three elliptic curves, two of them isogenious to E (Serre [1, Ch.5.3]). Then φ_1 and φ_2 can be obtained by injecting C in $\mathrm{Jac}(C)$ and then taking the projections on these two factors.

Using the properties of the heights over functional fields Dem'janenko (see Dem'janenko [1]) proved, as a special case of a more general result, that if $E(\mathbb{Q})$ has rank ≤ 1 then C has finitely many rational points. We use another approach, and applying the results from section 1 we prove that in this case actually $C(\mathbb{Q})$ is empty.

Theorem 2.1. *Let* $c \in \mathbb{N}$ *be a fourth power free integer which is not a perfect square. If* $c > 2$ *and the elliptic curve* $E : v^2 = u^3 - cu$ *has rank* ≤ 1 *then the equation* $x^4 + y^4 = cz^4$ *has no nonzero solutions in integers. If* $c = 2$ *then the only solution in natural numbers is* $(1, 1, 1)$.

Remark 2.2. If c is a perfect square then equation $x^4 + y^4 = cz^4$ has no nontrivial solutions. This follows from the classical result, due to Fermat, that the equation $x^4 + y^4 = z^2$ has no solutions in natural numbers. The second statement of the theorem is also well known. We include it because it comes as a consequence of the proof of the general result.

Before giving the proof of Theorem 2.1 we need the following Lemma.

Lemma 2.3. *Let $Q \in C(\mathbb{Q})$ and $P_1=\varphi_1(Q)$, $P_2=\varphi_2(Q)$. Then:*
a) $|h_u(2P_1)-h_u(2P_2)| \leq 4\log 2$;
b) $|\hat{h}(P_1)-\hat{h}(P_2)| \leq \frac{3}{4}\log 2$.

Proof. a) Let $Q=[x,y,z]$, $\gcd(x,y,z)=1$. Then using the duplication formula on E, and the fact that $x^4+y^4=cz^4$, we get

$$u(2P_1)=\frac{(2x^4+y^4)^2}{4x^2z^2y^4},$$

$$u(2P_2)=\frac{(x^4+2y^4)^2}{4y^2z^2x^4}.$$

It is easy to see that

$$H_u(2P_1)=\frac{(2x^4+y^4)^2}{\delta_1^2},\ \ \delta_1:=\gcd(2,y),$$

$$H_u(2P_2)=\frac{(x^4+2y^4)^2}{\delta_2^2},\ \ \delta_2:=\gcd(2,x).$$

We may assume that $1 \leq t=\frac{x^4}{y^4}$, and then

$$|h_u(2P_1)-h_u(2P_2)| \leq 2\left|\log\frac{2x^4+y^4}{x^4+2y^4}\right|+2\left|\log\frac{\delta_2}{\delta_1}\right| \leq 2\log\frac{2t+1}{2+t}+2\log 2=$$

$$=2\log\left(2-\frac{3}{t+2}\right)+2\log 2 \leq 4\log 2.$$

b) It is clear that $P_1,P_2 \in E_0(\mathbb{Q})$ and from Lemma 1.1 $2P_1, 2P_2 \in \Gamma$. Then applying Theorem 1.5 and a) we get

$$|\hat{h}(P_1)-\hat{h}(P_2)|=\frac{1}{4}\left|\hat{h}(2P_1)-\hat{h}(2P_2)\right| \leq$$

$$\leq \frac{1}{4}\left(\left|\hat{h}(2P_1)-\frac{1}{2}h_u(2P_1)\right|+\frac{1}{2}\left|h_u(2P_1)-h_u(2P_2)\right|+\left|\hat{h}(2P_2)-\frac{1}{2}h_u(2P_2)\right|\right) \leq$$

$$\leq \frac{1}{4}\left(\frac{\log 2}{2}+2\log 2+\frac{\log 2}{2}\right)=\frac{3}{4}\log 2. \quad \square$$

Proof (of Theorem 2.1). We use the notations from Lemma 2.3 and in addition we may assume that $x,y,z>0$. If c is not a perfect square, then $E_{tors}(\mathbb{Q})=\{\mathcal{O},(0,0)\}$ (cf. Silverman [1, Ch.X Prop.6.1]). Evidently $P_1,P_2 \notin \{\mathcal{O},(0,0)\}$ and so the result follows if $\operatorname{rank} E(\mathbb{Q})=0$. If $\operatorname{rank} E(\mathbb{Q})=1$, let T be a generator for the free part of $E(\mathbb{Q})$. Let $P_1=mT$ and $P_2=nT$ in $E(\mathbb{Q})/E_{tors}(\mathbb{Q})$. From the previous discussion $mn \neq 0$. We have

$$\hat{h}(P_1+P_2)=(m+n)^2\hat{h}(T)<|m^2-n^2|\hat{h}(T) \quad \text{if } mn<0,$$

$$\hat{h}(P_1-P_2)=(m-n)^2\hat{h}(T)<|m^2-n^2|\hat{h}(T) \quad \text{if } mn>0.$$

A direct computation gives that the u – coordinate of $P_1 + \varepsilon P_2$ is

$$\left(\frac{x^2 + \varepsilon xy + y^2}{z(x + \varepsilon y)}\right)^2$$

where $\varepsilon = \pm 1$. We may assume that $x \geq y$, then $x \geq z$ and consequently

$$z(x + \varepsilon y) \leq x(x + \varepsilon y) + y^2 = x^2 + \varepsilon xy + y^2.$$

Then $H_u(P_1 + \varepsilon P_2) = (x^2 + \varepsilon xy + y^2)^2$ and Theorem 1.5 applied to $P_1 \pm P_2$ gives:

$$h_u(P_1 + P_2) \leq 2\hat{h}(P_1 + P_2) + \log 2 < 2|m^2 - n^2|\hat{h}(T) + \log 2 \quad \text{ if } \ mn < 0,$$

$$h_u(P_1 - P_2) \leq 2\hat{h}(P_1 - P_2) + \log 2 < 2|m^2 - n^2|\hat{h}(T) + \log 2 \quad \text{ if } \ mn > 0.$$

But $h_u(P_1 - P_2) < h_u(P_1 + P_2)$ and in both cases we have

$$h_u(P_1 - P_2) < 2|m^2 - n^2|\hat{h}(T) + \log 2 = 2|\hat{h}(mT) - \hat{h}(nT)| + \log 2 =$$

$$= 2|\hat{h}(P_1) - \hat{h}(P_2)| + \log 2 \leq \frac{5}{2}\log 2,$$

where the last inequality follows from Lemma 2.3 b). From

$$h_u(P_1 - P_2) = 2\log(x^2 - xy + y^2)$$

we have

$$\log(x^2 - xy + y^2) < \frac{5}{4}\log 2 \implies x^2 - xy + y^2 < 2^{5/4} < 3.$$

Then $x = y = 1$ and $c = 2$. The elliptic curve $v^2 = u^3 - 2u$ has rank 1 and this gives the second statement of the Theorem. □

3. The Diophantine Equation $x^4 + y^4 = cz^4$ – Existence of Solutions

In this section we consider the following question - for which $c \in \mathbb{N}$ the equation $x^4 + y^4 = cz^4$ has nontrivial solutions in integers. This has been extensively studied by Bremner and Morton [1]. They use methods from algebraic number theory, and some of their results are listed in Table 3.1 Here we consider this question from another viewpoint, applying the results of the previous section. We also use the equation above to get some information about the ranks of the elliptic curves $v^2 = u^3 - cu$.

Another natural question for the equation $x^4 + y^4 = cz^4$ is to find all solutions for given c. This seems to be quite difficult. For example according to Serre [1, 5.3] it is not known whether the equation $x^4 + y^4 = 17z^4$ has other solutions in natural numbers then (1,2,1) and (2,1,1).

We may assume that $c > 2$ is a fourth power free integer, which is not a perfect square (see Remark 2.2). Then there are p-adic points on the curve

$$C : x^4 + y^4 = cz^4$$

for all p if and only if
a) $c \equiv 1$ *or* $2 \pmod{16}$,
b) every odd prime factor of c is $\equiv 1 \pmod 8$,
c) $c \not\equiv 3$ *or* $4 \pmod 5$,
d) $c \not\equiv 7, 8$ *or* $11 \pmod{13}$,
e) $c \not\equiv \pm 6, \pm 7 \pmod{17}$,
f) $c \not\equiv 4, 5, 6, 9, 13, 22, 28 \pmod{29}$
(see Serre [1, 5.3]).

If we want to apply the results from section 2, we need to know the ranks of the elliptic curves $E_c : v^2 = u^3 - cu$. Some information is provided by the next Proposition.

Proposition 3.1. *Assume that the 2 – component of the Tate – Shafarevich group of the elliptic curves E_c is finite. Then the following holds:*
a) *If $c \equiv 1 \pmod{16}$ and every prime divisor of c is $\equiv 1 \pmod 8$ then the rank of E_c is even;*
b) *If $c = 2p$, p – prime, $p \equiv 1 \pmod 8$, then the rank of E_c is 1 or 3.*

Proof. We use the descent via two–isogeny (cf. Silverman [1, Ch. X, Prop 4.9] and Silverman and Tate [1, Ch.III]). Let $E' : v^2 = u^3 + 4cu$ and let $\phi : E \longrightarrow E'$ be a 2–isogeny defined over $\mathbb{Q}$ and $\hat{\phi}$ be its dual. If $c \equiv 1 \pmod{16}$ and every prime divisor of c is $\equiv 1 \pmod 8$ then it is easy to see that

$$\#S^{(\phi)}(E/\mathbb{Q}) = \#S^{(\hat{\phi})}(E'/\mathbb{Q}).$$

If $c = 2p$, where $p \equiv 1 \pmod 8$ is a prime number, then

$$\dim_2 S^{(\phi)}(E/\mathbb{Q}) + \dim_2 S^{(\hat{\phi})}(E'/\mathbb{Q}) = 3$$

The assumption that the 2–component of the Tate–Shafarevich group is finite implies that its order is a perfect square. Then from the formulas given in Silverman [1, Ch.X, §6], the proof of Prop. 6.2(c), follows that rank$E(\mathbb{Q})$ is even in the case a) and odd in b). $\square$

The following Proposition is a reformulation of Theorem 2.1.

Proposition 3.2. *Suppose that $c > 2$ and there exist natural numbers x, y, z, such that $x^4 + y^4 = cz^4$. Then the rank of $v^2 = u^3 - cu$ is ≥ 2. If c is twice a prime number then the rank of $v^2 = u^3 - cu$ is 3.*

If the c is a prime number then the rank of E_c is 0 or 2. In this case an argument similar to the proof of Proposition 3.1 gives the following partial "converse" of Theorem 2.1.

Proposition 3.3. *If c is a prime number and the rank of $v^2 = u^3 - cu$ is 2, then there exist natural numbers x, y, z, such that $x^2 + y^4 = cz^4$.*

We now assume that there are p-adic points on C for all p. For the first 14 possible values of c the following table gives solutions of the equation $x^4 + y^4 = cz^4$, if there are such (see Bremner and Morton [1]), and the rank of the elliptic curve $v^2 = u^3 - cu$.

The next twelve possibilities for c are: $1042, 1186, 1297, 1361, 1522, 1777, 1921, 2066, 2161, 2402, 2417, 2482$ (2482 is the first even c which is not twice a prime

c	Solutions	rank$E(\mathbb{Q})$	c	Solutions	rank$E(\mathbb{Q})$
17	(1,2,1)	2	577	—	2
82	(1,3,1)	3	626	(1,5,1)	3
97	(2,3,1)	2	641	(2,5,1)	2
226	—	3	706	(3,5,1)	3
257	(1,4,1)	2	802	—	1 or 3
337	(3,4,1)	2	881	(4,5,1)	2
562	—	1 or 3	977	—	2

TABLE 3.1

number).
In Bremner and Morton [1] is given the example $c = 2161$ for which the elliptic curve E_c has rank 0. This gives an application of Theorem 2.1 (which is trivial in this case). As it seems from computations done with `mwrank` (see Cremona [1]), the elliptic curves E_{562} and E_{802} have rank 1 which gives another (nontrivial) application of the Theorem.

Remark 3.3. The methods of this article can be applied to be given an effective proof of the fact that if the rank of $v^2 = u^3 + c$ is ≤ 1 then the curve $x^6 + y^6 = cz^6$ has finitely many rational points (This is also proved in Dem'janenko [1]). The proof goes in the same lines, except that we have to use the general bounds for the difference $\left|\hat{h}(P) - \frac{1}{2}h_u(P)\right|$ (see Silverman [3] or Lang [1] and Zimmer [1]). We are not able to obtain a result similar to Theorem 2.1 for the diophantine equation $x^6 + y^6 = cz^6$ because we can not proof an analog of Lemma 2.3.

REFERENCES

Bremner, A. and Morton, P.
[1] *A new characterization of the integer 5906*, Manuscripta Math. **44** (1983), 187–229.

Cremona, J.
[1] *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1997.

Dem'janenko, V.A.
[1] *Rational points of a class of algebraic curves*, AMS Transl. **66** (1968), 246–272.

Lang, S.
[1] *Conjectured diophantine estimates on elliptic curves*, Progress in Math. **35** (1983), Birkhäuser.

Serre, J.–P.
[1] *Lectures on Mordell–Weil Theorem*, Asp. of Math. E 15, Vieweg, Brounshweig, 1989.

Silverman, J.H.
[1] *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New-York, 1986.
[2] *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer-Verlag, New-York, 1994.
[3] *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), 723–743.

Silverman, J.H. and Tate, J.
[1] *Rational Points on Elliptic Curves*, UTM, Springer-Verlag, New-York, 1992.

Zimmer, H.

[1] *On the difference of the Weil height and the Néron–Tate height*, Math. Z **147** (1976), 35–51.

SECTION OF ALGEBRA, FACULTY OF MATHEMATICS AND INFORMATICS, SOFIA UNIVERSITY, 5 JAMES BOURCHIER BLVD. SOFIA 1164 BULGARIA
E-mail address: grg@fmi.uni-sofia.bg

SECTION OF ALGEBRA, FACULTY OF MATHEMATICS AND INFORMATICS, SOFIA UNIVERSITY, 5 JAMES BOURCHIER BLVD. SOFIA 1164 BULGARIA
E-mail address: rizov@fmi.uni-sofia.bg