COMPOSITIO MATHEMATICA

DANIEL SION KUBERT

# Universal bounds on the torsion of elliptic curves

*Compositio Mathematica*, tome 38, nº 1 (1979), p. 121-128

<http://www.numdam.org/item?id=CM_1979__38_1_121_0>

COMPOSITIO MATHEMATICA, Vol. 38, Fasc. 1, 1979, pag. 121–128.
Sijthoff & Noordhoff International Publishers – Alphen aan den Rijn
Printed in the Netherlands

# UNIVERSAL BOUNDS ON THE TORSION OF ELLIPTIC CURVES

Daniel Sion Kubert*

In [4] the following theorem is announced. Given an elliptic curve $E$ defined over a number field $K$, we say that $E$ is $\ell$-deficient if the field we obtain by adjoining the $\ell$-division points of $E$ has degree over $K$ which is not divisible by $\ell$. Then we have

THEOREM: *Given $K$ finite over $Q$ and $\ell > 3$ prime, there exists $N(\ell, K) \in R^+$ such that if $E$ is an $\ell$-deficient elliptic curve over $K$ and $t \in E_{\text{tor}}(K)$, the group of $K$-torsion points of $E$, then $|t| < N(\ell, K)$.*

Before beginning the proof we present a little historical background. There is the following long-standing boundedness conjecture.

BOUNDEDNESS CONJECTURE: *Let $K$ be a finite extension of $Q$. Then there exists a positive real number $N(K)$ with the following property: if $E$ is an elliptic curve defined over $K$ then the group $E_{\text{tor}}(K)$ of $K$-rational torsion points has order less than $N(K)$.*

The above theorem is a weak version of this conjecture. The techniques used in the proof are derived from ideas of Hellegouarch [3] and Demyanenko [1, 2]. Hellegouarch showed how to associate to points on modular curves points in other algebraic varieties. Demyanenko conceived of the idea of using height arguments to prove the boundedness conjecture. Also using height arguments, Manin [6] succeeded in showing that the $p$-primary part of the torsion is universally bounded.

*Manin's result*

Let $K$ be a finite extension of $Q$. Let $p$ be a prime number, then there exists a positive real number $N(K, p)$ with the following pro-

* A Sloan Fellow, 1977, supported by NSF grants.

perty: if $E$ is an elliptic curve defined over $K$ the $p$-primary part of $E_{\text{tor}}(K)$ of $K$-rational torsion points has order less than $N(K, p)$.

Mazur [7] has proved the following strong version of the boundedness conjecture for $K = Q$.

*Mazur's result*

Let $E$ be an elliptic curve defined over $Q$. Let $t$ belong to $E_{\text{tor}}(Q)$. Then if $t$ has order $N$, the modular curve $X_1(N)$ has genus 0.

Now we begin the proof of the theorem.

The proof of this result is given in [4, theorem II.6.2] for the cases when $K$ is imaginary quadratic or $Q$. We now would like to give the proof of the result for $K$ arbitrary. We follow the proof in [4] and need only supply arguments for the Archimedean absolute values of $K$ which had not been included.

By Manin's result on the universal bound of the $p$-primary part of the torsion group we may suppose that $t$ is a torsion point of prime order $p$. We set $a = 2t$ and choose $b$ belonging to the group generated by $t$ such that $0 \neq b \neq \pm t$, $b \neq \pm a$. Such $b$ may be found if $p \geq 7$.

There will be a nonsingular model of $E$ of the form $y^2 = x^3 + rx^2 + sx + v$ where $r, s, v$ belong to $K$. We set

$$u_{a,b} = (x(a) - x(t))/(x(a) - x(b)) \tag{1}$$

$$v_{a,b} = -(x(b) - x(t))/(x(a) - x(b)).$$

We note that $u_{a,b}$, $v_{a,b}$ do not depend on the model chosen for $E$. We have $u_{a,b} + v_{a,b} = 1$. We know [4, theorem II.4.5] that the fractional ideals $(u_{a,b})$, $(v_{a,b})$ are $\ell$th powers and there is a finite extension $K'$ of $K$, which depends only on $K$ and $\ell$ such that $u_{a,b}$, $v_{a,b}$ are $\ell$th powers in $K'$. If we select $x, y \in K'$ such that $x^\ell = u_{a,b}$, $y^\ell = v_{a,b}$ then $x^\ell + y^\ell = 1$.

What we do is to fix $t$ and $a$ and vary $b$. As seen in [4] if $b \neq \pm b'$ then $(u_{a,b}, v_{a,b}) \neq (u_{a,b'}, v_{a,b'})$ and we can produce $(p-5)/2$ distinct pairs $(u_{a,b}, v_{a,b})$.

We may then produce $(p-5)/2$ distinct $K$-points on the curve $x^\ell + y^\ell = 1$ as above. We will show that the height of these points grows too slowly if $p$ is large. We will let $M(K)$ denote the set of absolute values of $K$, and $M(K')$ denote the set of absolute values of $K'$. We choose as our height function

$$h(x, y) = \sum_{M(K')} \log(\max(|x^\ell y^\ell|, 1)). \tag{2}$$

In our case $x^{\ell}y^{\ell} = u_{a,b}v_{a,b} \in K$ and

$$h(x, y) = [K' : K] \sum_{M(K)} \log(\max(|u_{a,b}v_{a,b}|, 1)) \tag{3}$$

So we need information about $|u_{a,b}v_{a,b}|$. This is provided in [4] ($K$) for the non-Archimedean valuations. To quote [4, proposition II.6.6]:

PROPOSITION: *Let $|\ |$ be a non-Archimedean absolute value of $K$*
(1) *If $|j(E)| \leq 1$ then $|u_{a,b}v_{a,b}| = 1$.*
(2) *Suppose $|j(E)| > 1$. Then either $|u_{a,b}v_{a,b}| = 1$ for all choices of $b$ or $|u_{a,b}v_{a,b}| \neq 1$ for all choices of $b$.*

In the second case we have the inequality

$$\|\log|j(E)|\| \geq \|\log|u_{a,b}v_{a,b}|\| \geq \frac{1}{p}\|\log|j(E)|\|$$

where $\|\ \|$ is the standard Euclidean norm.

We wish to extend this result to the Archimedean case. How is this result obtained? We think of $u$, $v$ as modular functions as we vary the elliptic curve $E$. Thus $u$, $v$ are thought of as belonging to the function field of the scheme $X_1(p)$. If $j$ represents the $j$-function then, in fact, $u$ and $v$ belong to the integral closure of the ring $Z[j]$ and are actually units in the ring. The proof of (*1*) is thus obvious. If $|\ |$ is a non-Archimedian valuation and $|j(E)| \leq 1$ then the ring $Z[j]$ is mapped into the integers of the completion of $K$, under specialization at $E$. Since $u, v$ were units in the integral closure of $Z[j]$, their images under specialization will go to units in the completion of $K$ which implies *i.*

The proof of (*2*) uses the Tate model. We may think of $u_{a,b}$, $v_{a,b}$ as functions of the Tate parameter $q$ [4, §II.2] and the second part of the proposition is merely giving information about the order of the zero of the $q$-expansion of $u_{a,b}v_{a,b}$ as $b$ varies. So the natural thing to do in the Archimedean case is to look at the Archimedean $q$-expansion and read off the relevant information.

Let $|\ |$ be an Archimedean valuation of $K$. We may now think of $K$ as being contained in $\mathbf{R}$ or $\mathbf{C}$. Let $\tau$ belong to the standard fundamental domain $D$ of $\Gamma = \mathrm{SL}(2, Z)/\pm 1$ inside $\mathcal{H}$, the upper half plane, such that $j(\tau) = j(E)$.

We may represent $t$, $a$, $b$ respectively by

$$t = t_1\tau + t_2, \quad a = a_1\tau + a_2, \quad b = b_1\tau + b_2 \tag{4}$$

where $t_1, t_2, a_1, a_2, b_1, b_2 \in (1/p)Z$, and we may normalize so that

$$0 \leq t_1, a_1, b_1 < 1. \tag{5}$$

Then

$$u_{a,b} = (\wp(a, \tau, 1]) - \wp(t, [\tau, 1]))/(\wp(a, [\tau, 1]) - \wp(b, [\tau, 1])) \tag{6}$$

where $\wp$ is the Weierstrass function

$$v_{a,b} = -(\wp(b, [\tau, 1]) - \wp(t, [\tau, 1]))/(\wp(a, [\tau, 1]) - \wp(b, [\tau, 1])).$$

Now $\wp(x, [\tau, 1]) - \wp(y, [\tau, 1]) = (-k(x + y)k(x - y))/(k^2(x)k^2(y))$ where [5, pages 248, 283]:

$$k(z) = k(z, \tau) = \tag{7}$$

$$-q_\tau^{[z_1(z_1-1)]/2} e^{2\pi i z_2(z_1-1)/2}(1 - q_z) \cdot \frac{\prod_1^\infty (1 - q_\tau^n q_z)(1 - q_\tau^n/q_z)}{\prod_1^\infty (1 - q_\tau^n)^2}$$

Here $z = z_1\tau + z_2$ and $q_\tau = e^{2\pi i\tau}$, $q_z = e^{2\pi iz}$.

In order to get the relevant information, we must determine which terms in the $q$-expansion dominate. As $\tau \mapsto i\infty$ clearly the term $q_\tau^{[z_1(z_1-1)]/2}$ will dominate. This was the only information which was relevant in the non-Archimedean case since the other terms are then units. Part (*2*) of the proposition is merely a statement about the order of the zero of $u_{a,b}v_{a,b}$ at $i\infty$ which we translate as follows into our present language.

PROPOSITION 2: *Let $\nu_{i\infty}(u_{a,b}v_{a,b})$ be the order of the zero of $u_{a,b}v_{a,b}$ at $i\infty$. Then if $t_1 = 0$, $\nu_{i\infty}(u_{a,b}v_{a,b}) = 0$ for all choices of $a, b$. If $t_1 \neq 0$, $\nu_{i\infty}(u_{a,b}v_{a,b}) \neq 0$ and $1 = \nu_{i\infty}(j^{-1}) \geq \|\nu_{i\infty}(u_{a,b}v_{a,b})\| \geq 1/p$ where $\| \ \|$ is the Euclidean norm.*

The proof is as follows. We first calculate the order of the zero of $\wp(x, [\tau, 1]) - \wp(y, [\tau, 1])$ at $i\infty$ where $x = x_1\tau + x_2$, $y = y_1\tau + y_2$. If $t \in R$, define $\langle t \rangle$ to be the residue of $t$ mod 1 if the residue is less than or equal to $\frac{1}{2}$, and otherwise the residue of $-t$. Then we claim that the order of the zero of $\wp(x, [\tau, 1]) - \wp(y, [\tau, 1])$ equals $\min(\langle x_1 \rangle, \langle y_1 \rangle)$ if $x \neq \pm y$. This follows immediately from (7). For since $\wp$ is even we may assume that $0 \leq x_1 \leq \frac{1}{2}, 0 \leq y_1 \leq \frac{1}{2}$ and we then just look at the given $q$-expansion.

Now in the setting of Proposition 2 if $t_1 = 0$ then $a_1 = 0$, $b_1 = 0$, which proves with the above remark the first assertion. For the second assertion one calculates from the above that $v_{i\infty}(u_{a,b}v_{a,b}) = \min(\langle a_1\rangle, \langle t_1\rangle) + \min(\langle b_1\rangle, \langle t_1\rangle) - 2\min(\langle a_1\rangle, \langle b_1\rangle)$ and from this one easily verifies all statements, keeping in mind that $\langle a_1\rangle$, $\langle b_1\rangle$, $\langle t_1\rangle$ are now distinct [4, proposition II.6.6].

We now examine the other terms in (7). Since $|e^{2\pi i z_2(z_1-1)/2}| = 1$ this may be ignored. The denominator $\Pi_1^\infty(1-q_\tau^n)^2$ may be ignored since it will cancel in (6).

We note that we may actually normalize $t$ so that $0 \le t_1 \le \frac{1}{2}$, since we may replace $t$ by $-t$ if necessary. Likewise we may assume $0 \le a_1 \le \frac{1}{2}$, $0 \le b_1 \le \frac{1}{2}$. Then $\log|\Pi_1^\infty(1-q_\tau^n q_z)(1-q_\tau^n/q_z)|$ is bounded on the set $(\tau, z)$, $\tau \in D$, $z \in [0, \frac{1}{2}] \times [0, 1]$. For the above function is continuous on this region and as $\tau \mapsto i\infty$ the value of the function approaches 0.

We now analyze the last term, $(1-q_z)$.

PROPOSITION 3: *Let $p$ be a prime number. Then $\exists C > 0$ such that*

$$\|\log|(1-q_z)|\| < C \log p$$

*where $z = z_1\tau + z_2$, $0 \le z_1 \le \frac{1}{2}$, $\tau \in D$, $p(z_1, z_2) \in Z^2$, $(z_1, z_2) \notin Z^2$.*

Clearly the only way that the left side of the equation can be large is if $1-q_z$ is close to zero. If $z_1 \neq 0$, $|q_z| < 1$ and $|1-q_z| > 1-|q_z|$. $|q_z|$ is maximized for $\tau = e^{2\pi i/6}$, $z_1 = 1/p$ in which case $|q_z| = e^{-(\pi\sqrt{3})/p}$ and

$$\begin{aligned} 1 - e^{-(\pi\sqrt{3})/p} &= e^{-(\pi\sqrt{3})/p}(e^{(\pi\sqrt{3})/p} - 1) \\ &\ge \frac{\pi\sqrt{3}}{p} e^{-(\pi\sqrt{3})/p} \\ &\ge \frac{\pi\sqrt{3}}{p} e^{-\pi\sqrt{3}} \end{aligned}$$

If $z_1 = 0$, $|1-q_z|$ is minimized for $z_2 = \pm 1/p$ in which case $|1-q_z| = 2\sin(\pi/p)$ which, say for $p \ge 3$, exceeds $(2\pi/p)\cos(\pi/3)$, that is $\pi/p$.

Let $h_v(b) \equiv \|\log|u(a,b)v(a,b)|\|$ where the subscript v denotes the given absolute value $|\ |$. We may write

$$\log|u(a,b)v(a,b)| = \ell_v^1(b) + \ell_v^2(b) + \ell_v^3(b) \tag{8}$$

where $\ell_v^1(b)$ is the contribution from the zero at $i\infty$ of $u_{a,b}v_{a,b}$; $\ell_v^2(b)$ is

the contribution from terms of the form $(1-q_z)$; and $\ell^2_v(b)$ is the contribution from the product $\Pi_1^\infty (1-q_\tau^n q_z)(1-q_\tau^n/q_\tau)$.

So we have the estimates, if $t_1 \neq 0$

$$\frac{2\pi \operatorname{Im}\tau}{p} \leq \|\ell^1_v(b)\| = 2\pi \operatorname{Im}\tau \|v_{i\infty}(u_{a,b}, v_{a,b})\| \leq 2\pi \operatorname{Im}\tau \tag{9}$$

If $t_1 = 0$, $\ell^1_v(b) = 0$

$$\|\ell^2_v(b)\| \leq C_1 \log p, \|\ell^3_v(b)\| < C_2$$

where $C_1, C_2 > 0$ are universal constants. Now by the product formula we have

$$2h(b) = [K', K] \sum_{M(K)} \|\log|u_{a,b}, v_{a,b}|\|. \tag{10}$$

We define $S \subset M(K)$ as follows. If v is non-Archimedean, $v \in S$ iff $|j(E)| > 1$ and $|u_{a,b}v_{a,b}| \neq 1$ for each $a, b$ as in Proposition 1. If v is Archimedean, $v \in S$ iff $t_1 \neq 0$ where $t = t_1\tau + t_2$ and $2\pi \operatorname{Im}\tau > 2p(C_1 \log p + C_2)$. Set

$$\gamma = \frac{[K':K]}{2}\left(\sum_{S_{\text{non-Arch}}} |j(E)| + \sum_{S_{\text{Arch}}} 4\pi \operatorname{Im}\tau\right).$$

Then $h(b) = h_1(b) + h_2(b)$ where $h_1(b) = ([K':K]/2)\,\Sigma_S \|\log|u_{a,b}v_{a,b}|\|$ and $h_2(b) = ([K':K]/2)\,\Sigma_{M(K)-S}\|\log|u_{a,b}v_{a,b}|\|$. The only nonzero contributions in $h_2$ will come from Archimedean absolute values. For such a value we have

$$\|\log|u_{a,b}v_{a,b}|\| \leq \|\ell^1_v(b)\| + \|\ell^2_v(b)\| + \|\ell^3_v(b)\| \leq Cp \log p \tag{11}$$

where $C > 0$ is some universal constant. For the term $h_2(b)$ we get the following inequality.

$$0 \leq h_2(b) \leq C'p \log p \tag{12}$$

where $C' > 0$ is some universal constant. If v is Archimedean and $v \in S$ we have

$$\begin{aligned} \|\log|u_{a,b}v_{a,b}|\| &\leq \|\ell^1_v(b)\| + \|\ell^2_v(b)\| + \|\ell^3_v(b)\| \leq 4\pi \operatorname{Im}\tau \\ \|\log|u_{a,b}v_{a,b}|\| &\geq \|\ell^1_v(b)\| - \|\ell^2_v(b)\| - \|\ell^3_v(b)\| \geq (\pi \operatorname{Im}\tau)/p \end{aligned} \tag{13}$$

So for $h_1(b)$ we have

$$\gamma/4p \leq h_1(b) \leq \gamma. \tag{14}$$

We now order our $(p-5)/2$ points by increasing height. Since $\ell \geq 5$ the curve $x^\ell + y^\ell = 1$ has genus greater than 1 and we may apply Mumford's criterion [4, §II.6.3.M]. We index the points by $b$. Then there exists an $N$ independent of $p$ such that $h(b(N)) > 1$ and $h(b((p-5)/2)) \geq C^{[((p-5)/2-N)/N]} h(b(N)) > 0$ where $C > 1$ is the constant in Mumford's theorem and depends only on $K$ and $\ell$. Substituting from the above inequalities we have

$$\begin{aligned} h_1(b((p-5)/2)) + C'p \log p &\geq C^{[((p-5)/2-N)/N]} h(b(N)) \\ &\geq C^{[((p-5)/2-N)/N]} \\ &\quad \max(1, h(b((p-5)/2)/4p)) \end{aligned} \tag{15}$$

Dividing by $p^2$ and letting $p$ increase we must have $h_1(b((p-5)/2)) > p^2$ so we may assume $h_1(b((p-5)/2))/4p > 1$ and then we get

$$h_1(b((p-5)/2)) + C'p \log p \geq C^{[((p-5)/2-N)/N]} h_1(b((p-5)/2))/4p. \tag{16}$$

Dividing by $h_1(b((p-5)/2))/4p$ we find $4p + C'p \log p \geq C^{[((p-5)/2-N)/N]}$ which is absurd for $p$ large enough. This concludes the proof of the theorem.

In conclusion we note that if $\ell = 2$ or 3 then the theorem does not apply since the relevant Fermat curves have genus 0 and 1 respectively. However since the curves $x^4 + y^4 = 1$, $x^9 + y^9 = 1$ have genus exceeding one, by the above techniques we have the following.

THEOREM 1: *Given $K$ finite over $Q$ there exists a constant $C(K) > 0$ such that if $E$ is an elliptic curve over $K$ whose 4-division points generate an extension field whose degree over $K$ is not divisible by 2 then the order of $E_{\text{tor}}(K)$* is less than $C(K)$.

THEOREM 2: *Given $K$ finite over $Q$ there exists a constant $C(K) > 0$ such that if $E$ is an elliptic curve over $K$ whose 9-division points generate an extension field whose degree over $K$ is not divisible by 3, then the order of $E_{\text{tor}}(K)$ is less than $C(K)$.*

## REFERENCES

[1] V.A. DENYANENKO: On torsion points of elliptic curves, *Izv. Akad. Nauk. S.S.S.R. Ser. Mat., 34* (1970), No. 4.
[2] V.A. DENYANENKO: On the torsion of elliptic curves, *Izv. Akad. Nauk. S.S.S.R. Ser. Mat., 35* (1971) 280–307.
[3] Y. HELLEGOUARCH: Points d'ordre fini sur les courbes elliptiques, *C.R. Acad. Sci. Paris Sér. A-B, 273* (1971) A540–543.
[4] D.S. KUBERT: Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc., third series, 33* (1976) 193–237.
[5] S. LANG: *Elliptic functions*. Addison-Wesley, Reading, Mass. (1973).
[6] S. MANIN: The $p$-torsion of elliptic curves is uniformly bounded, *Izv. Akad. Nauk. S.S.S.R. Ser Mat., 33* (1969) No. 3.
[7] B. MAZUR: Modular curves and the Eisenstein ideal, I.H.E.S., Paris (1978).
[8] D. MUMFORD: A remark on Mordell's conjecture, *American J. Math., 87* (1965) 1007–1016.

(Oblatum 16-V-1977 & 29-XII-1977)

Department of Mathematics
Cornell University
Ithaca, N.Y. 14853
U.S.A.