REMARKS ON THE SIZE OF THE TAMAGAWA PRODUCT

HECTOR PASTEN

Abstract. The Tamagawa product of an elliptic curve is a quantity that naturally appears in the Birch and Swinnerton-Dyer conjecture, and it is often conjectured to be small with respect to the conductor. In this note we propose a precise version of such a conjectural bound, we give some evidence for it, and we investigate arithmetic consequences beyond the context of the Birch and Swinnerton-Dyer conjecture.

1. Tamagawa factors

Let E be an elliptic curve over $\mathbb{Q}$. The Tamagawa factor of E at a prime p is denoted by $c_p(E)$. We recall that $c_p(E) = [\mathscr{E}(\mathbb{F}_p) : \mathscr{E}_0(\mathbb{F}_p)]$, where $\mathscr{E}$ is the Neron model of E over $\mathbb{Z}$ and $\mathscr{E}_0$ is the identity component of $\mathscr{E}$. Equivalently, $c_p(E)$ is the number of irreducible components of $\mathscr{E} \otimes \mathbb{F}_p$ over $\mathbb{F}_p$. Thus, $c_p(E) = 1$ if E has good reduction at p.

The Tamagawa product $\tau(E)$ is defined by

$$\tau(E) = \prod_p c_p(E)$$

where the product is over all primes p. Tate [Ta75] proved that $\tau(E)$ is precisely the "fudge factor" appearing in the Birch and Swinnerton-Dyer conjectural formula for the first non-zero Taylor coefficient of $L(E, s)$ at $s = 1$. Due to this, the Tamagawa product plays an important role in various questions involving other quantities appearing in the Birch and Swinnerton-Dyer conjecture, such as the study of the conjectural size of Tate-Shafarevich groups [dW98, Ni00, Hi07], statistics of ranks of elliptic curves [Wa08], or heuristics for uniform boundedness of ranks [PPVW16].

The main point in this note is to clarify the role of $\tau(E)$ in Diophantine problems beyond the context of the Birch and Swinnerton-Dyer conjecture. We will be interested in the size of $\tau(E)$, first with respect to the minimal discriminant of E, and then with respect to the conductor N_E. It turns out that showing that $\tau(E)$ is small with respect to the conductor is a difficult open problem closely related to the abc-conjecture. To me, it seems plausible that the following holds

Conjecture 1.1. *Let $\epsilon > 0$. For all elliptic curves E over $\mathbb{Q}$ we have*

$$\log \tau(E) \leq \left(\frac{7 \log 3}{3} + \epsilon\right) \frac{\log N_E}{\log \log N_E} + O_\epsilon(1).$$

Presumably, the constant $7(\log 3)/3 = 2.563...$ is not optimal, but is its fairly small and it is not too difficult to give some evidence for it. Among the Diophantine applications, we will explain how this conjecture relates to sub-exponential versions of the abc-conjecture.

2. Notation and preliminaries

We will use the following standard arithmetic functions for positive integers n:

- For a prime p the p-adic valuation of n is $v_p(n)$.
- $d(n)$ is the number of divisors of n. It satisfies $d(n) = \prod_{p|n}(1 + v_p(n))$.

Date: April 5, 2020.
Supported by FONDECYT Regular grant number 1190442.

- $\omega(n)$ is the number of different prime factors of n, without counting repetitions.
- $\mathrm{rad}(n)$ is the radical of n, i.e. it is the product of the different prime factors of n, without counting repetitions.

For any given $\epsilon > 0$, one has the following classical estimates:

$$\omega(n) \le (1+\epsilon)\frac{\log n}{\log\log n} + O_\epsilon(1), \quad \log d(n) \le (\log 2 + \epsilon)\frac{\log n}{\log\log n} + O_\epsilon(1).$$

In addition, we will consider de Weger's function (cf. [dW98])

$$W(n) = \prod_{p|n} v_p(n).$$

Erdös conjectured and de Weger proved that for any given $\epsilon > 0$

$$W(n) \le \left(\frac{\log 3}{3} + \epsilon\right)\frac{\log n}{\log\log n} + O_\epsilon(1).$$

For an elliptic curve E over $\mathbb{Q}$ we denote the absolute value of the minimal discriminant of E by Δ_E, and the conductor by N_E. The Ogg's formula and the Neron-Ogg-Shafarevich theorem gives that $N_E|\Delta_E$ and these two integers have the same prime factors.

We already observed that the Tamagawa factor of E at a prime p of good reduction satisfies $c_p(E) = 1$. Tate's algorithm [Ta75] provides further information:

Theorem 2.1. *Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime. The Tamagawa factor $c_p(E)$ satisfies:*

(i) $c_p(E) \le 4$ *if E has additive reduction at p*
(ii) $c_p(E) \le 2$ *if E has non-split multiplicative reduction at p*
(iii) $c_p(E) = v_p(\Delta_E)$ *if E has split multiplicative reduction at p.*

The *abc*-conjecture and Szpiro's conjecture will be relevant in our discussion, so let us recall them here.

Conjecture 2.2 (*abc*-conjecture)**.** *Let $\epsilon > 0$. There is a number κ_ϵ depending only on ϵ, such that for all coprime positive integers a, b, c with $a + b = c$ we have*

$$c \le \kappa_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}.$$

Conjecture 2.3 (Szpiro's conjecture)**.** *Let $\epsilon > 0$. There is a number K_ϵ depending only on ϵ, such that for all elliptic curves E over $\mathbb{Q}$ we have $\Delta_E \le K_\epsilon \cdot N_E^{6+\epsilon}$.*

It is a classical result that, up to the precise values of the exponents, these two conjectures are essentially equivalent [Fr89].

3. Smallness of the Tamagawa factor

From Theorem 2.1 we get $\tau(E) \le 4^{\omega(\Delta_E)} d(\Delta_E)$. Thus, the estimates in Section 2 give the following well-known lemma (cf. [dW98, Hi07, PPVW16])

Lemma 3.1. *For all elliptic curves E over $\mathbb{Q}$ we have*

$$\log \tau(E) = O\left(\frac{\log \Delta_E}{\log\log \Delta_E}\right).$$

In particular, $\log \tau(E) = o(\log \Delta_E)$.

In fact, a more careful analysis gives

Proposition 3.2. *Let $\epsilon > 0$. For all elliptic curves E over $\mathbb{Q}$ we have*

$$\log \tau(E) \le \left(\frac{\log 3}{3} + \epsilon\right) \frac{\log(\Delta_E N_E)}{\log\log \Delta_E} + O_\epsilon(1).$$

Proof. Let us factor $\Delta_E = AM$ where the primes of additive reduction appear in A, and those of multiplicative reduction appear in M. If $p|A$ then $v_p(N_E) \ge 2$, and since $N_E|\Delta_E$ we deduce

$$v_p(\Delta_E N_E) \ge \begin{cases} v_p(\Delta_E) & \text{if } p|M \\ 4 & \text{if } p|A. \end{cases}$$

Thus, $\tau(E) \le W(\Delta_E N_E)$. We conclude by de Weger's bound on $W(n)$, using $N_E|\Delta_E$. $\square$

Lemma 3.1 and Proposition 3.2 show that, in a sense, $\tau(E)$ is small. It is natural to expect bounds of this sort where Δ_E is replaced by the conductor N_E.

Conjecture 3.3 (Folklore)**.** *For all elliptic curves E over $\mathbb{Q}$ we have $\log \tau(E) = o(\log N_E)$.*

Lemma 3.1 gives the following well-known fact (cf. [Hi07, dW98])

Proposition 3.4. *Szpiro's conjecture implies Conjecture 3.3. In fact, Szpiro's conjecture implies the stronger estimate*

$$\log \tau(E) = O\left(\frac{\log N_E}{\log\log N_E}\right).$$

From our Proposition 3.2 we can in fact deduce more:

Proposition 3.5. *Szpiro's conjecture implies Conjecture 1.1.*

Proof. Szpiro's conjecture gives $\log(\Delta_E N_E) \le (7+\epsilon)\log N_E + O_\epsilon(1)$. $\square$

Thus, Conjecture 1.1 seems plausible, as it follows from Szpiro's conjecture. Furthermore, the following result is easy to show, and it provides unconditional evidence for Conjecture 1.1:

Proposition 3.6. *Let $\epsilon > 0$. For all elliptic curves E over $\mathbb{Q}$ without primes of split multiplicative reduction, we have*

$$\log \tau(E) \le (\log 4 + \epsilon)\frac{\log N_E}{\log\log N_E} + O_\epsilon(1).$$

Proof. From the results in Section 2 we get

$$\log \tau(E) \le \omega(N_E)\log 4 \le (\log 4 + \epsilon)\frac{\log N_E}{\log\log N_E} + O_\epsilon(1).$$

$\square$

We observe that there are plenty of elliptic curves as in Proposition 3.6. For instance, all elliptic curves with integral j-invariant satisfy the requirements, because they cannot have multiplicative reduction at any prime.

The hard case in conjectures 3.3 and 1.1 is, of course, when E has primes of split multiplicative reduction. In [Pa17] I proved the following result, which provides further unconditional evidence for Conjecture 3.3 including the cases of split multiplicative reduction:

Theorem 3.7. *Let $\epsilon > 0$. For all semi-stable elliptic curves E over $\mathbb{Q}$, we have*

$$\log \tau(E) \le \left(\frac{11}{2} + \epsilon\right)\log N_E + O_\epsilon(1).$$

In particular, for these elliptic curves we have $\log \tau(E) = O(\log N_E)$.

See [Pa17] for a more general theorem allowing controlled additive reduction. Unlike the previous results discussed so far, the proof of Theorem 3.7 is far from elementary —it is based on the theory of automorphic forms, Arakelov theory on Shimura curves, proved cases of Colmez's conjecture, and zero density estimates for L-functions, among other tools.

Improving from the estimate $\log \tau(E) = O(\log N_E)$ provided by Theorem 3.7, to the bound $\log \tau(E) = O(\log N_E/\log\log N)$ predicted by 1.1 (possibly with other numerical coefficient) might seem reachable —after all, it is just a $\log\log$ factor! However, I suspect that this is a deep problem. As an indication of this, in the next section we will see that such an improvement would lead to some remarkable Diophantine consequences.

4. Diophantine consequences

Along with Theorem 3.7, in [Pa17] I also proved the following unconditional result towards the abc-conjecture

Theorem 4.1 ($d(abc)$-theorem)**.** *Let $\epsilon > 0$. There is a number K_ϵ depending only on ϵ such that for all coprime positive integers a, b, c with $a + b = c$ we have*

$$d(abc) \le K_\epsilon \cdot \mathrm{rad}(abc)^{8/3+\epsilon}.$$

In particular, $\log d(abc) = O(\log \mathrm{rad}(abc))$.

Here, I would like to propose a conjectural refinement of the $d(abc)$-theorem:

Conjecture 4.2. *There are constants K, M such that for all coprime positive integers a, b, c with $a + b = c$ we have*

$$\log d(abc) \le K \cdot \frac{\log \mathrm{rad}(abc)}{\log\log \mathrm{rad}(abc)} + M.$$

It is easy to see that this refined $d(abc)$ estimate follows from the abc-conjecture

Proposition 4.3. *The abc-conjecture implies that Conjecture 4.2 holds and that K can be taken as any real number with $K > \log 8$.*

Proof. Since $abc \le c^3$, we have

$$\log d(abc) \le (\log 2 + \epsilon/3)\frac{\log(abc)}{\log\log(abc)} + O_\epsilon(1) \le (\log 8 + \epsilon)\frac{\log c}{\log\log c} + O_\epsilon(1).$$

The abc-conjecture states $\log c \le (1+\epsilon)\log \mathrm{rad}(abc) + O_\epsilon(1)$, hence the result. □

It turns out that the bound for $\tau(E)$ proposed in Conjecture 1.1 also implies Conjecture 4.2 without invoking the abc-conjecture, but the proof is less direct.

Theorem 4.4. *Conjecture 1.1 implies that Conjecture 4.2 holds and that K can be taken as any real number with $K > 7\log 3$.*

Proof. Let a, b, c be coprime positive integers with $a + b = c$. Consider the Frey elliptic curve

$$E: \quad y^2 = x(x-a)(x+b).$$

We have that E is semi-stable away from $p = 2$. Furthermore, $\Delta_E = 2^r(abc)^2$ and $N_E = 2^s\mathrm{rad}(abc)$, where $|s|, |t| \le 8$ (cf. p.256-257 [Si09]),.

Each $p > 2$ dividing N_E is a prime of multiplicative reduction for E, and $p = 2$ also is, unless $v_2(abc) \le 4$ (cf. [DK95]).

By the Chinese remainder theorem, we can choose an integer $D \le 8N_E$ coprime to $2N_E$ with the following properties regarding E^D (the quadratic twist of E by D):

(1) Each odd $p|N_E$ is a prime of split multiplicative reduction for E^D.

(2) If E has multiplicative reduction at 2, then E^D has split multiplictive reduction at 2. If E has good or multiplicative reduction at $p = 2$ then

$$\tau(E^D) \geq \prod_p v_p(\Delta_E) \geq 2^{-8} \prod_p (1 + v_p(abc)) = 2^{-8} d(abc).$$

If E has additive reduction at $p = 2$ then $v_2(abc) \leq 4$ and we have

$$\tau(E^D) \geq \prod_{p>2} v_p(\Delta_E) \geq \frac{1}{5} \prod_p (1 + v_p(abc)) = \frac{1}{5} d(abc).$$

Note that $N_{E^D} \leq N_E D^2 = O(N_E^3)$. Conjecture 1.1 applied to E^D gives

$$\log \tau(E^D) \leq \left(\frac{7 \log 3}{3} + \epsilon \right) \frac{3 \log N_E}{\log \log N_E} + O_\epsilon(1)$$

which proves the result. □

Finally, we show that Conjecture 1.1 implies an *abc*-inequality which, although is not as strong as the full *abc*-conjecture, it is certainly stronger than anything we can prove at present —e.g. the exponential bounds $\log c = O_\epsilon(\mathrm{rad}(abc)^{\alpha+\epsilon})$ for $\alpha = 15$ [ST89], $\alpha = 2/3$ [SY91], and $\alpha = 1/3$ [SY01].

Corollary 4.5. *Conjecture 1.1 implies the following sub-exponential version of the abc-conjecture: Let $\epsilon > 0$. For all coprime positive integers a, b, c with $a + b = c$ we have*

$$\log c \leq \exp\left((7 \log 3 + \epsilon) \frac{\log \mathrm{rad}(abc)}{\log \log \mathrm{rad}(abc)} \right) + O_\epsilon(1).$$

Proof. In view of Theorem 4.4, the crude bound

$$\log c \leq \left(\max_{p|abc} v_p(abc) \right) \log \mathrm{rad}(c) \leq d(abc) \log \mathrm{rad}(abc)$$

suffices. □

In particular, a bound for the Tamagawa product of elliptic curves as the one proposed in Conjecture 1.1 would allow one to get bounds for the height of solutions of various Diophantine equations, such as S-unit equations and Mordell equations, in a form that is much stronger than what is available today —these applications for *abc*-estimates are standard, see for instance [MP13, vK14, vKM16].

References

[DK95] F. Diamond, K. Kramer, *Modularity of a family of elliptic curves.* Math. Res. Lett. 2 (1995), no. 3, 299-304.

[Fr89] G. Frey, *Links between solutions of A-B=C and elliptic curves.* Number theory (Ulm, 1987), 31-62, Lecture Notes in Math., 1380, Springer, New York, (1989).

[Hi07] M. Hindry, *Why is it difficult to compute the Mordell-Weil group?*, Diophantine geometry, CRM Series, vol. 4, Ed. Norm., Pisa, 2007, pp. 197-219.

[vK14] R. von Känel, *Integral points on moduli schemes of elliptic curves.* Transactions of the London Mathematical Society 1.1 (2014): 85-115.

[vKM16] R. von Känel, B. Matschke. *Solving S-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture.* arXiv preprint arXiv:1605.06079 (2016).

[MP13] R. Murty, H. Pasten, *Modular forms and effective diophantine approximation.* Journal of Number Theory 133 (2013), no. 11, 3739-3754.

[Ni00] A. Nitaj, *Invariants des courbes de Frey-Hellegouarch et grands groupes de Tate-Shafarevich.* Acta arithmetica 93.4 (2000) 303-327.

[PPVW16] J. Park, B. Poonen, J. Voight, M. Wood, *A heuristic for boundedness of ranks of elliptic curves.* (2016) arXiv:1602.01431.

[Pa17] H. Pasten, *Shimura curves and the abc conjecture.* (2017) arXiv:1705.09251

[Si09] J. Silverman, *The arithmetic of elliptic curves. Second edition.* Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp. ISBN: 978-0-387-09493-9

[ST89] C. Stewart, R. Tijdeman, *On the Oesterlé-Masser conjecture.* Monatsh. Math. 102 (1986), 251-257.

[SY91] C. Stewart, K. R. Yu, *On the abc conjecture.* Math. Ann. 291 (1991), no. 2, 225-230.

[SY01] C. Stewart, K. R. Yu, *On the abc conjecture. II.* Duke Math. J. 108 (2001), no. 1, 169-181.

[Ta75] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil.* In Modular functions of one variable IV. Springer, Berlin, Heidelberg, (1975) p. 33-52.

[Wa08] M. Watkins, *Some heuristics about elliptic curves* Experiment. Math. 17 (2008), no. 1, 105-125.

[dW98] B. de Weger, *$A + B = C$ and big III's.* Quart. J. Math. Oxford Ser. (2) 49 (1998), 105-128.

Departamento de Matemáticas
Pontificia Universidad Católica de Chile
Facultad de Matemáticas
4860 Av. Vicuña Mackenna
Macul, RM, Chile
Email address, H. Pasten: hpasten@gmail.com