Compositio Mathematica **136:** 1–23, 2003.

Average Root Numbers for a Nonconstant Family of Elliptic Curves

OTTAVIO G. RIZZO*
Dipartimento di matematica, Università di Milano, Via Saldini 50, 20133 Milan, Italy.
e-mail: ottavio.rizzo@mat.unimi.it

(Received: 26 May 2000; accepted in final form: 16 November 2001)

Abstract. We give some examples of families of elliptic curves with nonconstant j-invariant where the parity of the (analytic) rank is not equidistributed among the fibres.

Mathematics Subject Classifications (2000). Primary: 11G05; secondary: 11G07, 14Gxx.

Key words. elliptic curves, root numbers.

Assuming the Birch and Swinnerton-Dyer conjecture, the root number of an elliptic curve $E/\mathbf{Q}$ is -1 to the rank of $E(\mathbf{Q})$, the group of rational points of E. Given a 'generic' algebraic family E_t of elliptic curves, one would expect to find the same numbers of curves with even and odd rank (see, for example, the graph in [16]). If E_t is a family of twists of a given curve (i.e., the j-invariant is constant), then there are known counterexamples: assuming Selmer's Conjecture, Cassels and Schinzel prove in [2] that $(7+7t^4)y^2 = x^3 - x$ has odd rank for any $t \in \mathbf{Q}$. Given E/Q and a polynomial $f(t) \in \mathbf{Q}[t]$, we can build the family $E^{f(t)}$ of twists of E by $f(t)$; then Rohrlich [11] proves that, if E acquires everywhere good reduction over some Abelian extension of $\mathbf{Q}$, then $W(E^{f(t)}) = W(E)\mathrm{sgn}(f(t))$. Given any $E/\mathbf{Q}$, the author ([8, 9]) has shown that the set $\{\mathrm{Av}_{\mathbf{Q}} W(E^{f(t)})\}$ is dense in the interval $[-1, 1]$, where $f(t)$ varies over all polynomials in $\mathbf{Q}[t]$ and $\mathrm{Av}_{\mathbf{Q}} W$ denotes the average value of the root numbers for $t \in \mathbf{Q}$.

It has been suggested by Silverman – see the final remarks in [14] – that this kind of phenomenon could occur only for constant families: we present here some counterexamples with $t \in \mathbf{Z}$.

THEOREM 1. *Let* E_t: $y^2 = x^3 + tx^2 - (t+3)x + 1$. *Then* $j(t) = 256(t^2 + 3t + 9)$, *while* $W(E_t) = -1$ *for every* $t \in \mathbf{Z}$.

THEOREM 2. *Let*

$$E_t\colon y^2 = x^3 + \frac{t}{4}x^2 - \frac{36t^2}{t-1728}x - \frac{t^3}{t-1728}. \tag{1}$$

*This work was supported by a EU TMR fellowship 'Arithmetic Algebraic Geometry', contract ERB FMR XCT 960006.

Then $j(t) = t$ *while the average value over* $\mathbf{Z}$ *of* $W(E_t)$ *is* $0.0037182\ldots$

The example of Theorem 1 is due to L. Washington: he proved that, for every t such that $t^2 + 37 + 9$ is square free and assuming the finiteness of the Tate–Shafarevich group, the rank is odd [15]: this has been verified unconditionally for $t < 1000$ [4]. Theorem 1 is a (not too difficult to prove) consequence of the Halberstadt–Rohrlich tables (as presented in Section 1): for completeness, we give a proof in Section 2. In order to prove Theorem 2, instead, we need to deal with some density result, somewhat in the spirit of [9].

Some remark on notations: we will often be sloppy and confuse an elliptic curve E with its Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$; let c_4, c_6 and Δ be the usual invariants. A prime will always be a finite prime, while p will denote a prime number, unless specified otherwise. We will also shorten $(v_p(c_4), v_p(c_6), v_p(\Delta))$ as $v_p(c_4, c_6, \Delta)$. For any $x \in \mathbf{Q}_p$, we will write $x'_p = x'$ for $x/p^{v_p(x)}$; for $n = 4, 6$ we will also write $c_{n,e}$ for c_n/p^{ω}, where $\omega = n\lfloor v_p(c_n)/n \rfloor + e$. At last, recall that if E is a Weierstrass equation for an elliptic curve with coefficients $a_i \in \mathbf{Q}_p$, then any equivalent equation E with coefficients a_i is obtained by a change of coordinates of the form

$$x = u^2\mathsf{x} + r, \quad y = u^3\mathsf{y} + u^2s\mathsf{x} + t, \tag{2}$$

where $(u, r, s, t) \in \mathbf{Q}_p$ and $u \neq 0$.

1. Root Numbers

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N. By the Modularity Theorem (cf. [5]), the L-function attached to E is the Mellin transform of a normalized Hecke eigenform for $\Gamma_0(N)$ and thus admits an analytic continuation to an entire function satisfying the functional equation

$$\Lambda_E(2 - s) = W(E)\Lambda_E(s), \quad \text{where } \Lambda_E(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s).$$

The number $W(E) = \pm 1$ is called the *root number* of E. It is a consequence of the Birch and Swinnerton-Dyer Conjecture that $W(E) = -1$ if and only if the group of rational points of E has odd rank. On the other hand, $W(E)$ can be expressed as a product $\prod W_p(E)$ taken over all places of $\mathbf{Q}$, each *local* root number W_p being defined in terms of representations of the Weil–Deligne group of $\mathbf{Q}_p$. ([3] and [12]). We recall here some results.

FACT 3. Let p be any prime of $\mathbf{Q}$. Then

(1) If E is any elliptic curve over $\mathbf{R}$, then $W_\infty(E) = -1$.
(2) If $E/\mathbf{Q}_p$ has good reduction, then $W_p(E) = 1$.
(3) If $E/\mathbf{Q}_p$ has multiplicative reduction, $W_p(E) = -1$ if and only if the reduction is split.

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

(4) If $E/\mathbf{Q}_p$ has additive, potentially multiplicative reduction and $p > 2$, then $W_p(E) = (-1/p)$; if $p = 2$, then $W_p(E) \equiv -c_6/2^{v_2(c_6)} \bmod 4$.
(5) If $E/\mathbf{Q}_p$ has additive, potentially good reduction with $p > 3$, let $e = 12/\gcd(v_p(\Delta), 12)$. Then $W_p(E) = (-x/p)$, where $x = 1$ if $e = 2$ or 6, $x = 3$ if $e = 3$ and $x = 2$ if $e = 4$.
(6) If $E/\mathbf{Q}_p$ has additive, potentially good reduction with $p = 3$ (resp. $p = 2$) and E is given in minimal form, then $W_p(E)$ depends only on the p-adic expansion of c_4, c_6 and Δ; if E is given in minimal Weierstrass form, $W_p(E)$ can be read from Table II (resp. Table I) of [6].

Notice that the first four points are classical (but see [11] for proofs) except the 2-adic case of point 4 which, in this form, is due to Connell [2]; the fifth is due to Rohrlich [11] and the last to Halberstadt [6] (by the Modularity Theorem, his result is now unconditional).

It follows that, if $p > 3$, it is straightforward to compute $W_p(E)$. Even for the cases $p \leqslant 3$, the only difficulty is when E has additive, potentially good reduction at p, in which case we need first to compute a minimal equation, which is not a trivial task if we are working on a parametric family. Thus, we would rather remove the minimality restriction on Halberstadt's tables: our results are presented in Tables I, II and III where, for completeness, we have added also the cases missing from [6], namely good and (potentially) multiplicative reduction.

1.1. HOW TO READ THE TABLES

Let (a, b, c) be the smallest triplet of nonnegative integers such that $a \equiv v_p(c_4) \bmod 4$, $b \equiv v_p(c_6) \bmod 6$, $c \equiv v_p(\Delta) \bmod 12$. Then Table I (resp. II, resp. III) lists $W_p = W_p(E)$ for $p > 3$ (resp. $p = 3$, resp. $p = 2$), the different cases classified by the value of (a, b, c). If this value is not enough to make a distinction, a special condition depending only on the p-adic expansion of c_4, c_6, Δ is given.

Table I. The local root number W_p, for $p > 3$

(a, b, c)	Kod	$v(N)$	W_p
$(\geqslant 0, 0, 0)$	I_0	0	$+1$
$(0, \geqslant 0, 0)$	I_0	0	$+1$
$(0, 0, \geqslant 1)$	I_c	1	$-(-c'_6/p)$
$(\geqslant 1, 1, 2)$	II	2	$(-1/p)$
$(1, \geqslant 2, 3)$	III	2	$(-2/p)$
$(\geqslant 2, 2, 4)$	IV	2	$(-3/p)$
$(2, \geqslant 3, 6)$	I_0^*	2	$(-1/p)$
$(\geqslant 2, 3, 6)$	I_0^*	2	$(-1/p)$
$(2, 3, \geqslant 7)$	I_{c-6}^*	2	$(-1/p)$
$(\geqslant 3, 4, 8)$	IV*	2	$(-3/p)$
$(3, \geqslant 5, 9)$	III*	2	$(-2/p)$
$(\geqslant 4, 5, 10)$	II*	2	$(-1/p)$

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

Table II. The local root number W_3

(a, b, c)	Special condition	Kod	$v(N)$	W_3
(0, 0, 0)		I_0	0	+1
$(1, \geqslant 3, 0)$		I_0	0	+1
$(0, 0, \geqslant 1)$		I_c	1	$c_6' \equiv 1$ (3)
*(1, 2, 0)		II^*	4	+1
*($\geqslant$2, 2, 1)		II^*	5	$c_6' \equiv 1$ (3)
$(\geqslant 2, 3, 3)$	$c_6'^2 + 2 \not\equiv 3c_{4,2}$ (9)	II	3	$c_6' \equiv 4, 7, 8$ (9)
$(\geqslant 2, 3, 3)$	$c_6'^2 + 2 \equiv 3c_{4,2}$ (9)	III	2	+1
(2, 4, 3)		II	3	$c_4' \not\equiv c_6'$ (3)
$(2, \geqslant 5, 3)$		III	2	+1
(2, 3, 4)		II	4	+1
(2, 3, 5)		IV	3	$\Delta' \equiv c_6'$ (3)
$(\geqslant 3, 4, 5)$		II	5	$c_6' \equiv 2$ (3)
$(2, 3, \geqslant 6)$		I^*_{c-6}	2	−1
(3, 5, 6)		IV	4	$c_4' \equiv 2$ (3)
$(3, \geqslant 6, 6)$		I_0^*	2	−1
$(\geqslant 4, 5, 7)$		IV	5	$c_6' \equiv 2$ (3)
$(\geqslant 4, 6, 9)$	$c_6'^2 + 2 \equiv 3c_{4,4}$ (9)	III^*	2	+1
(4, 6, 9)	$c_6'^2 + 2 \not\equiv 3c_4$ (9)	IV^*	3	$c_6' \equiv 4, 8$ (9)
$(\geqslant 5, 6, 9)$	$c_6' \equiv \pm 4$ (9)	IV^*	3	$c_6' \equiv 1, 2$ (9)
(4, 7, 9)		IV^*	3	$c_6' \equiv 2$ (3)
$(4, \geqslant 8, 9)$		III^*	2	+1
(4, 6, 10)		IV^*	4	$c_6' \equiv \pm 2$ (9)
(4, 6, 11)		II^*	3	$c_6' \equiv 1$ (3)
$(\geqslant 5, 7, 11)$		IV^*	5	$c_6' \equiv 1$ (3)

A star near the triplet (a, b, c) means that the given equation cannot possibly be minimal: in this case, one needs to apply a change of coordinates of the form (2) with $u = 1/p$(and r, s, t suitably chosen) to put E in minimal Weierstrass form. If there is not such a symbol, then E may already be in minimal form: anyhow, if a change of coordinates is needed, it will have $u = 1$ – i.e., c_4, c_6 and Δ will not vary.

In the next columns we read the Kodaira symbol and the exponent of p in the conductor. In the last column, if W_p is not constant in the mentioned case, a necessary and sufficient condition for W_p to be equal to +1 is given (except in Table I, where the value of W_p is given).

We remark that in the third line of Table 1 of [6], the special condition $c_4' \equiv 1 \bmod 4$ was clearly forgot.

1.2. ADMISSIBLE TRIPLETS

Fix p. We now explain how the minimality condition can be dropped. We may well assume that the Weiestrass equation for $E/\mathbf{Q}_p$ is integral: if it is not, it will suffice to apply a change of coordinates of the form (2) with $(u, r, s, t) = (p^{-\omega}, 0, 0, 0)$ and ω large enough. Notice that, if E is the new equation, then $(c_4(\mathsf{E}), c_6(\mathsf{E}), \Delta(\mathsf{E})) = (p^{4\omega}c_4, p^{6\omega}c_6, p^{12\omega}\Delta)$.

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

Table III. The local root number W_2

(a, b, c)	Special condition	Kod	$v(N)$	W_2
(0, 0, 0)	$c_6 \equiv 3\ (4)$	I_0	0	$+1$
$^*(0, 0, >0)$	$c'_6 \equiv 1\ (4)$	I^*_{c+4}	4	-1
$^*(3, 3, 0)$		III*	5	$c'_4 \equiv 1\ (4)$, $c'_6 \equiv \pm 1\ (8)$ or $c'_4 \equiv 3\ (4)$, $c'_6 \equiv 1, 3\ (8)$
$(\geqslant 4, 3, 0)$	$c'_6 \equiv 1\ (4)$	I_0	0	$+1$
$^*(\geqslant 4, 3, 0)$	$c'_6 \equiv 3\ (4)$	II*	4	-1
$^*(2, \geqslant 4, 0)$	$c'_4 \equiv 3\ (4)$	I^*_2	6	$b = 4$
$^*(2, 4, 0)$	$c'_4 \equiv 1\ (4)$	I^*_3	5	$c'_4 + 4c'_6 \equiv 9, 13\ (16)$
$^*(2, \geqslant 5, 0)$	$c'_4 \equiv 1\ (4)$	I^*_3	5	$c'_4 + 4c_{6,4} \equiv 5, 9\ (16)$
$(0, 0, \geqslant 1)$	$c'_6 \equiv 3\ (4)$	I_c	1	$c'_6 \equiv 3\ (8)$
$^*(2, 3, 1)$		I_2	7	$c'_4 + 4c'_6 \equiv 3\ (16)$ or $c'_4 \equiv 11\ (16)$
$^*(2, 3, 2)$		I^*_4	6	$\Delta' \equiv c'_6\ (4)$
$^*(3, 4, 2)$		III*	7	$c'_4 \equiv 1$, $c'_6 \equiv 5, 7\ (8)$ or $c'_4 \equiv 3$, $c'_6 \equiv 3, 5\ (8)$ or $c'_4 \equiv 5$, $c'_6 \equiv 1, 3\ (8)$ or $c'_4 \equiv 7$, $c'_6 \equiv 1, 7\ (8)$
$^*(\geqslant 4, 4, 2)$		II*	6	$c'_6 \equiv 1\ (4)$
$^*(2, 3, 3)$		I^*_5	6	$\Delta' \equiv 3\ (4)$
$^*(3, 5, 3)$		III*	8	$2c'_6 + c'_4 \equiv 1, 3\ (8)$
$^*(3, \geqslant 6, 3)$		III*	8	$c'_4 \equiv 5, 7\ (8)$
$^*(2, 3, \geqslant 4)$		I^*_{c+2}	6	$c'_6 \equiv 3\ (4)$
(4, 5, 4)	$c'_4 \equiv c'_6\ (4)$	II	4	$c'_4 \equiv 1\ (4)$
(4, 5, 4)	$c'_4 \equiv 1 \equiv -c'_6\ (4)$	III	3	$c'_4 c'_6 \equiv 3\ (8)$
(4, 5, 4)	$c'_6 \equiv 1 \equiv -c'_4\ (4)$	IV	2	-1
$(\geqslant 5, 5, 4)$	$c'_6 \equiv 3\ (4)$	II	4	$a = 5$
(5, 5, 4)	$c'_6 \equiv 1\ (4)$	III	3	$c'_6 \equiv 5\ (8)$
$(\geqslant 6, 5, 4)$	$c'_6 \equiv 1\ (4)$	IV	2	-1
(5, 6, 6)		II	6	$c'_4 \equiv 3\ (4)$
$(\geqslant 6, 6, 6)$		II	6	$c'_6 \equiv 1\ (4)$
$(4, \geqslant 7, 6)$	$c'_4 \equiv 1\ (4)$	II	6	$b = 7$
$(4, \geqslant 7, 6)$	$c'_4 \equiv 3\ (4)$	III	5	$c'_4 - 4c_{6,7} \equiv 7, 11\ (16)$
(4, 6, 7)		II	7	$c'_6 \equiv 5, 5c'_4\ (8)$
(4, 6, 8)	$2c'_6 + c'_4 \equiv 3, 15\ (16)$	I^*_0	4	$2c'_6 + c'_4 \equiv 3\ (16)$
(4, 6, 8)	$2c'_6 + c'_4 \equiv 7\ (16)$	I^*_1	3	$2c'_6 + c'_4 \equiv 23\ (32)$
(4, 6, 8)	$2c'_6 + c'_4 \equiv 11\ (16)$	IV*	2	-1
(5, 7, 8)		III	7	$2c'_4 + c'_6 \equiv 7\ (8)$ or $c'_6 \equiv 3\ (8)$
$(\geqslant 6, 7, 8)$	$c'_6 \equiv 3\ (4)$	I^*_0	4	$a = 6$
(6, 7, 8)	$c'_6 \equiv 1\ (4)$	I^*_1	3	$2c'_4 + c'_6 \equiv 3\ (8)$
$(\geqslant 7, 7, 8)$	$c'_6 \equiv 1\ (4)$	IV*	2	-1
(4, 6, 9)		I^*_0	5	$2c'_6 + c'_4 \equiv 11\ (32)$ or $c'_6 \equiv 7\ (8)$
(5, 8, 9)		III	8	$2c'_6 + c'_4 \equiv \pm 1\ (8)$
$(5, \geqslant 9, 9)$		III	8	$c'_4 \equiv 1, 3\ (8)$
(4, 6, 10)	$c'_6 \equiv 1\ (4)$	I^*_2	4	$+1$
(4, 6, 10)	$c'_6 \equiv 3\ (4)$	III*	3	$c'_4 - 2c'_6 \equiv 3, 19\ (64)$
(6, 8, 10)		I^*_0	6	$c'_4 c'_6 \equiv 3\ (4)$
$(\geqslant 7, 8, 10)$		I^*_0	6	$c'_6 \equiv 1\ (4)$
(4, 6, 11)	$c'_6 \equiv 1\ (4)$	I^*_3	4	$+1$
(4, 6, 11)	$c'_6 \equiv 3\ (4)$	II*	3	$c'_6 \equiv 3\ (8)$

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

DEFINITION. A triplet of integers (a, b, c) is *p-admissible* if

(1) there is a minimal elliptic curve $E/\mathbf{Q}_p$ such that $v_p(c_4, c_6, \Delta) = (a, b, c)$;
(2) for every nonzero integer k, there is no minimal elliptic curve $E/\mathbf{Q}_p$ such that $v_p(c_4, c_6, \Delta) - (a, b, c) = (4k, 6k, 12k)$.

(c_4, c_6 and Δ being the invariants associated with the given Weierstrass equation.) We say that (a, b, c) is *semi-admissible* if it satisfies the first condition.

Remark 4. If (a, b, c) is semi-admissible it is clear that the three values are non-negative. If $p > 3$, then it is well known (cf. [13], Ex. VII.7.1) that semi-admissibility implies $a \leqslant 4$, $b \leqslant 6$ or $\Delta \leqslant 12$: in particular, semi-admissibility implies admissibility. If $p = 3$, we can read the list of admissible values in Table III of [7]: in particular, semi-admissibility still implies admissibility. If $p = 2$, we can read the list of admissible values in Table IV of [7]: in particular, only $(0, 0, \geqslant 0)$, $(4, 6, \geqslant 12)$, $(\geqslant 4, 3, 0)$, $(\geqslant 8, 9, 12)$ are semi-admissible but not admissible.

Let $p = 2$; let $E/\mathbf{Q}_2$ be an elliptic curve such that $v_2(c_4, c_6, \Delta) = (a, b, c)$ is semi-admissible but not admissible. After a change of coordinates with u power of 2, we get a minimal equation E: we say that $v_2\big(c_4(\mathsf{E}), c_6(\mathsf{E}), \Delta(\mathsf{E})\big)$ is the *minimal triplet* of E. It is clear that this triplet is well defined; it actually depends only on (c_4, c_6, Δ):

PROPOSITION 5. *Fix a prime p and let $E/\mathbf{Q}_p$ be a Weierstrass equation for an elliptic curve. If E is in minimal form then $v_p(c_4, c_6, \Delta)$ is (at least) semi-admissible. Vice versa,*

(1) *suppose $v_p(c_4, c_6, \Delta)$ is admissible, then after a change of coordinates that leaves (c_4, c_6, Δ) fixed, E becomes minimal.*
(2) *Suppose $v_p(c_4, c_6, \Delta)$ is semi-admissible but not admissible (thus $p = 2$), then*
   (a) *if $v_2(c_4, c_6, \Delta) = (0, 0, \geqslant 0)$ or $(4, 6, \geqslant 12)$, then the minimal triplet is the former if $c_6/2^{v(c_6)} \equiv 3 \bmod 4$, the latter otherwise;*
   (b) *if $v_2(c_4, c_6, \Delta) = (\geqslant 4, 3, 0)$ or $(\geqslant 8, 9, 12)$, then the minimal triplet is the former if $c_6/2^{v(c_6)} \equiv 1 \bmod 4$, the latter otherwise.*

Proof. If E is minimal then Tate algorithm applied to E as in [7] (i.e., using only c_4, c_6 and Δ rather than the coefficients a_i) will stop and give one of the (semi-) admissible cases.

(1) Suppose that $v_p(c_4, c_6, \Delta)$ is admissible. As above, we can suppose the equation integral; thus we can apply Tate's algorithm to find, after some change of coordinates of the form (2), a minimal equation E. By definition, we must have $(c_4(\mathsf{E}), c_6(\mathsf{E}), \Delta(\mathsf{E})) = (c_4, c_6, \Delta)$.
(2) Suppose now that $v_p(c_4, c_6, \Delta)$ is semi-admissible but not admissible. Arguing as above, there is a change of coordinates with u a power of 2 that will give us an

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

integral equation with $v_2(c_4, c_6, \Delta) = (4, 6, \geqslant 12)$ or $v_2(c_4, c_6, \Delta) = (\geqslant 8, 9, 12)$. We will analyze the two cases separately.

(a) Suppose that $v(c_4, c_6, \Delta) = (4, 6, \geqslant 12)$; we claim that the equation is minimal if and only if $c_6/2^{v(c_6)} \equiv 1 \bmod 4$. Following [7], we are at least in Tate's case (7). In particular $v(a_1) \geqslant 1$, $v(a_2) \geqslant 1$, $v(a_3) \geqslant 2$, $v(a_4) \geqslant 3$ and $v(a_6) \geqslant 4$. It follows that $c_6 = -a_1^6 + 4a_1^4 a_2 + O(2^8)$; thus $v(a_1) = 1$ while $v(a_2) = 1$ if and only if $c_6/2^6 \equiv 1 \bmod 4$. By Proposition 4 of [7], we are in Tate's case (7) if and only if the equation $a_2 \equiv sa_1 + s^2 \bmod 4$ has no solution s; i.e., if and only if $c_6/2^6 \equiv 1 \bmod 4$. This proves the claim.

Suppose that the equation is not minimal, then Tate's algorithm rolls over with a change of coordinates of the form 2 with $u = 2$, so that the new invariants are $(0, 0, 0)$: this time the algorithm must terminate, so we have a minimal equation (possibly after another change of coordinates with $u = 1$).

(b) Suppose that $v(c_4, c_6, \Delta) = (\geqslant 8, 9, 12)$; then we are at least in Tate's case (10). In particular $v(a_i) \geqslant i$ for $i = 1, 2, 3, 4$, while $v(a_6) \geqslant 5$. It follows that $c_4 = a_1^4 + 8a_1^2 a_2 + 8a_1 a_3 + O(2^8)$; since $v(c_4) \geqslant 8$, this implies that $v(a_1) \geqslant 2$. Therefore, $v(b_2) \geqslant 4$, $v(b_4) \geqslant 5$, $v(b_6) \geqslant 6$, $v(b_8) \geqslant 8$ and proposition 6 of [7] becomes E is minimal if and only if the equation $b_6 \equiv s^2 \bmod 2^8$ has no solution s. Since $c_6 = 8b_6 + O(2^{11})$ and $v(c_6) = 9$, we have that $v(b_6) = 6$ and the equation can be solved if and only if $c_6/2^9 \equiv 1 \bmod 4$, which proves our claim. □

1.3. PROOF OF THE TABLES

Using Proposition 5, we can remove the minimality assumption from Halberstadt's tables by introducing additional special conditions to distinguish between the semi-admissible but not admissible cases. So, by Fact 3, the only thing left to do is to show how to deduce the reduction type from the triplet (c_4, c_6, Δ). We recall some well known facts, which we apply to Papadopolous' list of possible triplets.

FACT 6. For any prime p, if $E/\mathbf{Q}_p$ is in minimal Weierstrass form, then its reduction is: good if and only if $v_p(\Delta) = 0$. Multiplicative if and only if $v_p(\Delta) > 0$ and $v_p(c_4) = 0$. Additive if and only if $v_p(\Delta) > 0$ and $v_p(c_4) > 0$; in this case, it is potentially multiplicative if and only if $v_p(\Delta) > 3v_p(c_4)$.

If $p > 3$, the results in Table I follow at once from Fact 6 and Table I of [7], except for the following lemma.

LEMMA 7. *For any prime p, an elliptic curve $E/\mathbf{Q}_p$ in minimal Weierstrass form has multiplicative reduction if and only if $v_p(c_4, c_6, \Delta) = (0, 0, \geqslant 1)$. Suppose so; then, if $p = 2$, the reduction is split if and only if $c_6 \equiv 7 \bmod 8$, if $p > 2$, the reduction is split if and only if $-c_6$ is a square modulo p.*

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

Proof. The first statement is obvious. Suppose then that E has multiplicative reduction; let $\tilde{E}$ be its reduction modulo p. Moving the node onto the origin, we may assume that the equation for $\tilde{E}$ is

$$y^2 + \bar{a}_1 xy = x^3 + \bar{a}_2 x^2, \tag{3}$$

where $\bar{a}_i$ is the reduction of a_i modulo p (cf. Section III.1 of [13]). In particular, $c_6 = -(a_1^2 + 4a_2)^3 + O(p)$.

If $p = 2$, then $v(c_6) = 0$ implies $v(a_1) = 0$ and Equation (3) is split if and only if $a_2 \equiv 0 \bmod 2$. Since $v_2(a_3) > 0$, we have $v_2(b_4) > 0$ and $c_6 \equiv -b_2^3 \equiv -a_1^6 + 4a_1^4 a_2 \bmod 8$. Given that $a_1^2 \equiv 1 \bmod 8$, this shows that $a_2 \equiv 0 \bmod 2$ if and only if $c_6 \equiv 7 \bmod 8$, as we claimed.

If instead $p > 2$, Equation (3) is split if and only if $a_1^2 + 4a_2$ is a square; since its valuation is zero, this is equivalent to $-c_6$ being a square, as we claimed. □

If instead $p \leqslant 3$, we need another couple of lemmata, which are easily proved using Papadopolous' tables, Proposition 5 and Fact 6. Let c_4, c_6, Δ be the invariants of a Weierstrass equation E over $\mathbf{Q}_p$.

LEMMA 8. *Let $p = 3$ and let (a, b, c) be the smallest triplet of nonnegative integers such that $(a, b, c) \equiv v_3(c_4, c_6, \Delta) \bmod (4, 6, 12)$. Then*

(1) *E has good reduction if and only if $(a, b, c) = (0, 0, 0)$ or $(1, \geqslant 3, 0)$; in this case, $W_3(E) = 1$.*
(2) *E has additive, potentially multiplicative reduction if and only if $(a, b, c) = (2, 3, \geqslant 7)$; in this case, $W_3(E) = -1$.*

LEMMA 9. *Let $p = 2$ and let (a, b, c) be the smallest triplet of nonnegative integers such that $(a, b, c) \equiv v_2(c_4, c_6, \Delta) \bmod (4, 6, 12)$. Then*

(1) *E has good reduction if and only if $(a, b, c) = (0, 0, 0)$ with $c_6' \equiv 3 \bmod 4$ or $(a, b, c) = (\geqslant 4, 3, 0)$ with $c_6' \equiv 1 \bmod 4$; in this case, $W_2(E) = 1$.*
(2) *E has additive, potentially multiplicative reduction if and only if $(a, b, c) = (0, 0, \geqslant 7)$ with $c_6' \equiv 1 \bmod 4$ or $(a, b, c) = (2, 3, \geqslant 7)$; in this case, $W_2(E) = 1$ if and only if $c_6' \equiv 3 \bmod 4$.*

2. Washington's Family

Let E_t be as in Theorem 1 and let $f(t) = t^2 + 3t + 9$. Then $c_4(t) = 16f(t)$, $c_6(t) = -32(2t + 3)f(t)$, $\Delta(t) = 16f^2(t)$.

PROPOSITION 10. *We have, for every integer t,*

$$W_2(t) = \begin{cases} +1 & \text{if } t \equiv 0, 1 \bmod 4, \\ -1 & \text{if } t \equiv 2, 3 \bmod 4 \end{cases} \equiv f(t) \bmod 4;$$

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

$$W_3(t) = (-1)^{v_3 f(t)} = \begin{cases} +1 & \text{if } t \not\equiv 3 \bmod 9, \\ -1 & \text{if } t \equiv 3 \bmod 9; \end{cases}$$

$$W_p(t) = \left(\frac{-1}{p}\right)^{v_p f(t)}, \quad \text{for every } p > 3.$$

Proof. Notice that, independently from the characteristics, if t is integral then all the coefficients of E_t are integral. Suppose $p = 2$; then $f(t) \equiv 1 \bmod 2$ for every $t \in \mathbf{Z}_2$. Thus $v_2(c_4, c_6, \Delta) = (4, 5, 4)$. Moreover, $c_4' \equiv 1 \bmod 4$ if and only if $t \equiv 0, 1 \bmod 4$ and $c_6' \equiv 1 \bmod 4$ if and only if $t \equiv 1, 2 \bmod 4$. We can now read $W_2(t)$ from Table III, exception made for the case $t \equiv 0 \bmod 4$; nevertheless, we can easily check that $c_4'(t)c_6'(t) \equiv 1 \bmod 8$ for every such t.

Suppose $p = 3$; then

$$v_3 f(t) = \begin{cases} 0 & \text{if } t \equiv \pm 1 \ (3), \\ 2 & \text{if } t \equiv 0, 6 \ (9), \\ 3 & \text{if } t \equiv 3 \ (9); \end{cases} \qquad v_3(2t+3) = \begin{cases} 0 & \text{if } t \equiv \pm 1 \ (3), \\ 1 & \text{if } t \equiv 0, 6 \ (9), \\ 2 & \text{if } t \equiv 3, 21 \ (27), \\ \geqslant 3 & \text{if } t \equiv 12 \ (27). \end{cases}$$

Thus,

$$v_3(c_4, c_6, \Delta) = \begin{cases} (0, 0, 0) & \text{if } t \equiv \pm 1 \bmod 3, \\ (2, 3, 4) & \text{if } t \equiv 0, 6 \bmod 9, \\ (3, 5, 6) & \text{if } t \equiv 3, 21 \bmod 27, \\ (3, \geqslant 6, 6) & \text{if } t \equiv 12 \bmod 27. \end{cases}$$

Notice that, if $t \equiv 3 \bmod 9$, then $c_4'(t) \equiv 1 \bmod 3$. We can now read $W_3(t)$ from Table II.

Finally let $p > 3$. Write $v_p f(t) = 6\omega + \tau$, where $0 \leqslant \tau < 6$; then

$$v_p(c_4, c_6, \Delta) = (2\omega + \tau, \tau + v_p(2t+3), 2\tau) \bmod (4, 6, 12).$$

The right hand side is minimal, since $2\tau < 12$. Moreover, notice that, if $v_p(2t+3) > 0$, then $v_p f(t) = 0$. Therefore, we can read from Table I:

$$W_p(t) = \begin{cases} +1 & \text{if } v_p f(t) \equiv 0 \bmod 6, \\ \left(\frac{-1}{p}\right) & \text{if } v_p f(t) \equiv 1 \bmod 2, \\ \left(\frac{-3}{p}\right) & \text{if } v_p f(t) \equiv 2, 4 \bmod 6. \end{cases}$$

On the other hand, if $v_p f(t) > 0$ for some $t \in \mathbf{Z}_p$, then $f(t)$ splits over $\mathbf{F}_p$; its discriminant being -27, this is equivalent to $(-3/p) = +1$. This proves our claim.

Proof of Theorem 1. if p is an odd prime, then $(-1/p) \equiv p \bmod 4$. Since $v_2 f(t) = 0$ for every t, thanks to Proposition 10 we have

$$(-1)^{v_3 f(t)} \prod_{p \geqslant 5} W_p(t) = \prod_{p \geqslant 3} \left(\frac{-1}{p}\right)^{v_p f(t)} \equiv f(t) \equiv W_2(t) \bmod 4.$$

Hence, for every integer t,

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

$$W(t) = -\prod_p W_p(t) = -(-1)^{v_3 f(t)} \prod_{p \neq 3} W_p(t) = -W_2(t)^2 = -1.$$

3. Specializing Halberstadt–Rohrlich

Let E_t be as in Theorem 2. In order to apply the tables of Section 1, we need to find, for each parameter t and each prime p, a minimal nonnegative triplet (a, b, c) such that $(a, b, c) \equiv v_p(c_4, c_6, \Delta) \bmod (4, 6, 12)$. We have

$$c_4(t) = \frac{t^3}{t - 1728}, \qquad c_6(t) = -\frac{t^4}{t - 1728}, \qquad \Delta(t) = \frac{t^8}{(t - 1728)^3}. \tag{4}$$

Thus, letting $\tau = v_p(t)$, we need to find an integer ω such that

$$(a, b, c) = \tau(3, 4, 8) - \omega(4, 6, 12) - v(t - 1728)(1, 1, 3) \geqslant 0 \tag{5}$$

is minimal. The computations are similar to those in the previous section and are not too difficult; moreover, they can be easily verified with a computer algebra system. On the other hand, they are quite long, so we prefer to omit them: nevertheless, they can be found in an earlier version of this paper [10].

PROPOSITION 11. *Let p be a prime > 3: notice that we cannot have both $v_p(t)$ and $v_p(t - 1728)$ strictly positive. Then W_p is given by Table IVa if $v_p(t) > 0$ and by Table IVb if $v_p(t - 1728) > 0$.*

PROPOSITION 12. *Let $t \in \mathbf{Z}_3$; let $t' = t/3^{v(t)}$. Then we have*

- *If $v_3(t) \neq 3$, then W_3 is as in Table Va if $v_3(t) < 3$ and as in Table Vb if $v_3(t) > 3$.*
- *If $v_3(t) = 3$ and $t \not\equiv 1728 \bmod 3^7$, then $W_3 = +1$ if and only if $t' \equiv \pm 2, \pm 4 \bmod 9$, $\equiv 19 \bmod 27$. If $v(t) = 3$ and $t \equiv 1728 \bmod 3^7$, then $W_3 = +1$ if and only if $v(t - 1728) \not\equiv 2 \bmod 4$.*

PROPOSITION 13. *Let $t \in \mathbf{Z}_2$ and write $t' = t/2^{v(t)}$. Then we have*

- *If $v_2(t) \neq 6$, then W_2 is as in Table VIa.*
- *If $v_2(t) = 6$ and $t \not\equiv 1728 \bmod 2^{11}$, then $W_2 = 1$ if and only if $t' \equiv 9, 13, 15 \bmod 16$, $t' \equiv 7, 23, 35, 51 \bmod 64$, or $t' \equiv 43, 187, 235, 251 \bmod 256$. If $v(t) = 6$ and $t \equiv 1728 \bmod 2^{11}$, then W_2 is as in Table VIb.*

Table IVa. $v_p(t) > 0$

$v_p(t)$	$W_p(E_t)$
$0 \bmod 3$	$+1$
$\pm 1 \bmod 3$	$\left(\frac{-3}{p}\right)$

Table IVb. $v_p(t - 1728) > 0$

$v_p(t - 1728)$	$W_p(E_t)$
$0 \bmod 4$	$+1$
$\pm 1 \bmod 2$	$\left(\frac{-2}{p}\right)$
$2 \bmod 4$	$\left(\frac{-1}{p}\right)$

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

Table Va. $v_3(t) < 3$

$v(t)$	W_3
0	$+1$
1	-1
2	$t' \equiv 2\ (3)$

Table Vb. $v_3(t) > 3$

$v(t) > 3$	W_3
$0 \bmod 3$	$t' \not\equiv \pm 1(9)$
$1 \bmod 3$	$+1$
$2 \bmod 3$	-1

Table VIa. $v_2(t) \neq 6$

$v_2(t)$	W_2
0, 1, 4, 8,	$t' \equiv 1 \bmod 4$
2	$t' \not\equiv 5 \bmod 8$
3, 5, 9	$t' \equiv 3 \bmod 4$
7	$t' \equiv 1, 3 \bmod 8$
$\geqslant 10$	-1

Table VIb. $v_2(t) = 6, t = 1728 \bmod 2^{11}$

$v_2(t - 1728)$	W_2
$0 \bmod 4$	$t'' \equiv 7, 11 \bmod 16$
$1 \bmod 4$	$t'' \equiv 1, 3 \bmod 8$
$2 \bmod 4$	$t'' \equiv 5, 9 \bmod 16$
$3 \bmod 4$	$t'' \equiv 5, 7 \bmod 8$

4. Locally Constant Multiplicative Functions

Let us consider the root number $W(t) = W(E_t)$ as a function of the parameter t; then we can write $W(t) = \prod W_p(t)$, where each W_p is a 'nice' p-adic function. Our goal is to express the *average value* of W in terms of the average values of all the W_p, which turn out to be standard integrals over $\mathbf{Z}_p$. Our idea of niceness is the following:

DEFINITION. Given a prime p, we say that a function $f\colon \mathbf{Z} \to \mathbf{R}$ is a *p-uniformly locally constant multiplicative function* if there exist a positive integer η such that $f(x)$ depends only on $v_p(x)$ and on the first η digits of the p-adic expansion of x; i.e., f factors through the map $\mathbf{Z} \to \mathbf{Z}^{\geqslant 0} \times (\mathbf{Z}/p^\eta\mathbf{Z})^*$ given by $x \mapsto (v_p(x), xp^{-v_p(x)} \bmod p^\eta)$.

By abuse of notation we will write $f(dp^e)$ with $d \in (\mathbf{Z}/p^\eta\mathbf{Z})^*$ and e a nonnegative integer to mean $f(x)$, where x is any integer $\equiv dp^e \bmod p^{e+\eta}$. We say that η is a *uniformity constant* of f.

DEFINITION. Given a finite set of primes $\mathbf{p} = \{p_1, \ldots, p_s\}$, we say that f is a *$\mathbf{p}$-uniformly locally constant multiplicative function* if $f = \prod_{i=1}^s f_i$, where each f_i is p_i-uniformly locally constant multiplicative. A *uniformity constant* for f is an integer η which is such for every factor f_i.

Remark 14. Clearly, $W(t)$ does not satisfy the above conditions. Nonetheless, we will show in Section 5 that it can be approximated closely enough by uniformly locally constant multiplicative functions.

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

4.1. *p*-ADIC INTEGRALS

Suppose that f is a p-uniformly locally constant function with a uniformity constant η. Then we can define, for every $e \geqslant 0$,

$$\int_{v_p(t)=e} f(t)\mathrm{d}t = \sum_{d\in(\mathbf{Z}/p^{\eta}\mathbf{Z})^*} \frac{f(dp^e)}{p^{e+\eta}}. \tag{6}$$

It is easy to verify that the sum is indipendent of the choice of η. We can, henceforth, give the following:

DEFINITION. Suppose that f is a p-uniformly locally constant function. Then let

$$\int_{\mathbf{Z}_p} f(t)\mathrm{d}t = \sum_{e=0}^{\infty} \int_{v_p(t)=e} f(t)\mathrm{d}t,$$

assuming the sum converges absolutely. In this case we say that $f \in L^1(\mathbf{Z}_p)$.

Notice that this definition induces the standard Haar measure on $\mathbf{Z}_p$ and that the measure of $\{t \in \mathbf{Z}_p : v_p(t) = e\}$ is $(p-1)/p^{e+1}$. In particular, by the compactedness of $\mathbf{Z}_p$, any continuous and uniformally locally constant function $f\colon \mathbf{Z}_p \to \mathbf{R}$ belongs to $L^1(\mathbf{Z}_p)$.

4.2. AVERAGING

Given $\mathbf{p} = \{p_1, \ldots, p_s\}$, write P for $\prod p_i$.

DEFINITION. The average value of a function $f\colon \mathbf{Z} \to \mathbf{R}$ is

$$\mathrm{Av}_{\mathbf{Z}} f(t) = \lim_{T\to\infty} \frac{\sum_{|t|\leqslant T} f(t)}{2T},$$

provided that the limit exists. In this case we say that $f \in L^1(\mathbf{Z})$.

LEMMA 15. *Let f be a $\mathbf{p}$-uniformly locally constant function, bounded by some $F > 0$ and with uniformity constant η. Then, for any integers r and k with $r \geqslant \eta$, we have*

$$\left| \sum_{t=(k-1)P^r+1}^{kP^r} \frac{f(t)}{P^r} - \prod_{p\in\mathbf{p}} \int_{v_p(t)\leqslant r-\eta} f_p(t)\mathrm{d}t \right| \leqslant \frac{F}{2^r} \sum_{p\in\mathbf{p}} p^{\eta-1} = \mathrm{O}\left(\frac{1}{2^r}\right).$$

Proof. Let J be the set of integers in $((k-1)P^r, kP^r]$. Define

$$J_0 = \{t \in J \cap \mathbf{Z} : \forall p \in \mathbf{p},\, v_p(t) \leqslant r - \eta\}$$

and J_1 as its complement in J. Then

$$\left| \sum_{t\in J_1} \frac{f(t)}{P^r} \right| \leqslant F\frac{\#J_1}{P^r} \leqslant \frac{F}{P^r} \sum_{p\in\mathbf{p}} \{t \in J : p^{r-\eta+1} | t\} \leqslant \frac{F}{2^r} \sum_{p\in\mathbf{p}} p^{\eta-1} \tag{7}$$

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

Remark that, if $t \in J_0$, then $f(t + sP^r) = f(t)$ for any integer s. hence

$$\sum_{t \in J_0} f(t)/P^r = \sum_{t \in \bar{J}_0} \prod_{p \in \mathbf{p}} f_p(t)/p^r,$$

where $\bar{J}_0 = \{t \in \mathbf{Z}/P^r\mathbf{Z} : \forall p \in \mathbf{p},\ v_p(t) \leqslant r - \eta\}$. We claim that

$$\sum_{t \in \bar{J}_0} \prod_{p \in \mathbf{p}} \frac{f_p(t)}{p^r} = \prod_{p \in \mathbf{p}} \int_{v_p(t) \leqslant r-\eta} f_p(t)\mathrm{d}t.$$

We will prove the claim by induction on the number of primes in $\mathbf{p}$: suppose that $P = p$; then, by the well-definedness of Equation (6),

$$\sum_{t \in \bar{J}_0} \frac{f_p(t)}{p^r} = \sum_{e=0}^{r-\eta} \sum_{d \in (\mathbf{Z}/p^{r-e}\mathbf{Z})^*} \frac{f_p(dp^e)}{p^r} = \int_{v_p(t) \leqslant r-\eta} f_p(t)\mathrm{d}t.$$

If $q \in \mathbf{p}$, let $P' = P/q$ and factor $\mathbf{Z}/P\mathbf{Z}$ as $\mathbf{Z}/q\mathbf{Z} \oplus \mathbf{Z}/P'\mathbf{Z}$. Then,

$$\sum_{t \in \bar{J}_0} \frac{1}{P^r} \prod_{p|P} f_p(t) = \sum_{\substack{t \in \mathbf{Z}/q^r\mathbf{Z} \text{ s.t.} \\ v_q(t) \leqslant r-\eta}} \left(\frac{f_q(t)}{q^r} \sum_{\substack{t \in \mathbf{Z}/P'^r\mathbf{Z} \text{ s.t.} \\ \forall p|P', v_p(t) \leqslant r-\eta}} \prod_{p|P'} \frac{f_p(t)}{p^r} \right),$$

which, by the induction hypothesis, is

$$= \prod_{p|P} \int_{v_p(t) \leqslant r-\eta} f_p(t)\mathrm{d}t;$$

which proves the claim. By Equation (7), this suffices to prove the lemma. □

NOTATION. For every positive integer T let $T = T_0 + T_1 P + \cdots + T_r P^r$ be the P-adic expansion of T; i.e., $r = \lfloor \log_P T \rfloor$ and $0 \leqslant T_e < P$ for every $e = 0, \ldots, r$. Moreover, we will write $\hat{T}_e$ for $T_e P^e + \cdots + T_r P^r$.

LEMMA 16. *Suppose that the series $\sum a_e$ converges absolutely. Then*

$$\lim_{T \to \infty} \sum_{e=0}^{\log_P T} \frac{\hat{T}_e}{T} a_e = \sum_{e=0}^{\infty} a_e.$$

Proof. Since $0 \leqslant 1 - \hat{T}_e/T < P^e/T$ if $e \geqslant 0$, we have

$$\left| \lim_{T \to \infty} \sum_{e=0}^{\log_P T} \left(1 - \frac{\hat{T}_e}{T}\right) a_e \right| < \lim_{T \to \infty} \sum_{e=0}^{\log_P T} \frac{P^e}{T} |a_e| = \lim_{x \to \infty} \sum_{e=0}^{x} P^{e-x} |a_e|,$$

where $x = \log_P T$. Fix now an arbitrary $\varepsilon > 0$, then there is an η such that $\sum_{e > \eta} |a_e| < \varepsilon$. Noting that $|P^{e-x}| \leqslant 1$ for every $e \leqslant x$, we get

$$\lim_{x \to \infty} \sum_{e=0}^{x} P^{e-x} |a_e| < \varepsilon + \lim_{x \to \infty} \frac{1}{P^x} \sum_{e=0}^{\eta} P^e |a_e| = \varepsilon.$$

The constant ε being arbitrary, the lemma follows. □

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

NOTATION. Given $\mathbf{p}$ as above, let $\mathbf{i}$ be a multi-index $\mathbf{p} \to \mathbf{Z}^{\geqslant 0}$. We will write i_p for $\mathbf{i}(p)$ and $\|\mathbf{i}\|$ for $\max_{p\in\mathbf{p}}\{i_p\}$.

LEMMA 17. *For every $p \in \mathbf{p}$, suppose given a sequence $\{S_p(i)\}_{i=0}^{\infty}$. Then, for every positive T,*

$$\sum_{e=0}^{\log_P T} T_e P^e \prod_{p|P} \sum_{i=0}^{e} S_p(i) = \sum_{e=0}^{\log_P T} \hat{T}_e \sum_{\|\mathbf{i}\|=e} \prod_{p|P} S_p(i_p).$$

In particular, if the series $\sum_i S_p(i)$ converge absolutely for every $p \in \mathbf{p}$, then

$$\lim_{T\to\infty} \sum_{e=0}^{\log_P T} \frac{T_e P^e}{T} \prod_{p|P} \sum_{i=0}^{e} S_p(i) = \prod_{p|P} \sum_{i=0}^{\infty} S_p(i).$$

Proof. We have, for every $e > 0$,

$$\prod_{p|P} \sum_{i=0}^{e} S_p(i) = \sum_{i=0}^{e} \sum_{\|\mathbf{i}\|=i} \prod_{p|P} S_p(i_p).$$

Thus

$$\begin{aligned}\sum_{e=0}^{\log_P T} T_e P^e \prod_{p|P} \sum_{i=0}^{e} S_p(i) &= \sum_{e=0}^{\log_P T} \sum_{i=0}^{e} T_e P^e \sum_{\|\mathbf{i}\|=i} \prod_{p|P} S_p(i_p) \\ &= \sum_{i=0}^{\log_P T} \sum_{e=i}^{\log_P T} T_e P^e \sum_{\|\mathbf{i}\|=i} \prod_{p|P} S_p(i_p) \\ &= \sum_{i=0}^{\log_P T} \hat{T}_i \sum_{\|\mathbf{i}\|=i} \prod_{p|P} S_p(i_p),\end{aligned}$$

as we claimed. Suppose now that every $\sum_i S_p(i)$ converges absolutely. Then

$$\lim_{T\to\infty} \sum_{e=0}^{\log_P T} \frac{T_e P^e}{T} \prod_{p|P} \sum_{i=0}^{e} S_p(i) = \lim_{T\to\infty} \sum_{i=0}^{\log_P T} \frac{\hat{T}_i}{T} \sum_{\|\mathbf{i}\|=i} \prod_{p|P} S_p(i_p)$$

which, by Lemma 16 and rearrangement,

$$= \sum_{i=0}^{\infty} \sum_{\|\mathbf{i}\|=i} \prod_{p|P} S_p(i_p) = \sum_{\mathbf{i}\geqslant 0} \prod_{p|P} S_p(i_p) = \prod_{p|P} \sum_{i=0}^{\infty} S_p(i),$$

which concludes the proof. □

THEOREM 18. *Suppose that $f\colon \mathbf{Z} \to \mathbf{R}$ is a bounded, $\mathbf{p}$-uniformly locally constant function. Then $f \in L^1(\mathbf{Z})$ and*

$$\mathrm{Av}_{\mathbf{Z}} f(t) = \prod_{p\in\mathbf{p}} \int_{\mathbf{Z}_p} f_p(t)\mathrm{d}t.$$

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

Proof. Let η be the uniformity constant of f and F a bound for $|f(t)|$; then we claim that, for T large,

$$\sum_{t=-T}^{T} \frac{f(t)}{2T} = \prod_{p\in\mathbf{p}} \left(\int_{v_p(t) \leqslant \log_P(T)-\eta} f_p(t)\mathrm{d}t \right) + \mathrm{o}(1). \tag{8}$$

Since each f_p is integrable, the equation passes to the limit proving the theorem. Therefore, it suffices to prove Equation (8). Let $r = \log_P T$; define, for $e \leqslant r$, $\check{T}_e = \sum_{i=e}^{r} T_i$ and, for $n \leqslant \check{T}_\eta$,

$$\lambda(n) = \begin{cases} 0 & \text{if } n = 0, \\ P^r & \text{if } 0 < n \leqslant \check{T}_r, \\ P^e & \text{if } \check{T}_{e+1} < n \leqslant \check{T}_e, \text{ where } \eta \leqslant e < r(T); \end{cases}$$

$$I_0 = [-T, -\hat{T}_\eta) \cup \{0\} \cup (\hat{T}_\eta, T],$$

$$I_n = \left(\sum_{i=0}^{n-1} \lambda(i), \sum_{i=0}^{n} \lambda(i) \right], \quad \text{for } 0 < n \leqslant \check{T}_\eta;$$

last, let $I_{-n} = -I_n$. Clearly, $\bigcup_{n=-\check{T}_\eta}^{\check{T}_\eta} I_n$ is a partition of $[-T, T] \cap \mathbf{Z}$. We have

$$\#I_0 \leqslant 2P^\eta - 1 \quad \text{and} \quad \#I_n = \#I_{-n} = \lambda(n), \quad \text{for} \quad n > 0$$

Thus,

$$\left| \sum_{t\in I_0} \frac{f(t)}{T} \right| \leqslant F\frac{\#I_0}{T} \leqslant F\frac{2P^\eta - 1}{T} = \mathrm{O}\left(\frac{1}{T}\right);$$

while, by Lemma 15, if $n \neq 0$,

$$\begin{aligned} \sum_{t\in I_n} \frac{f(t)}{T} &= \frac{\lambda(n)}{T} \sum_{t\in I_n} \frac{f(t)}{\lambda(n)} \\ &= \frac{\lambda(n)}{T} \prod_{p|P} \left(\int_{v_p(t) \leqslant \log_P \lambda(n)-\eta} f_p(t)\mathrm{d}t \right) + \mathrm{O}\left(\frac{1}{T}\right). \end{aligned}$$

Therefore,

$$\sum_{t=-T}^{T} \frac{f(t)}{2T} = \sum_{e=\eta}^{\log_P T} \frac{2T_e P^e}{2T} \prod_{p|P} \int_{v_p(t) \leqslant e-\eta} f_p(t)\mathrm{d}t \quad + \quad \mathrm{O}\left(\frac{\ln T}{T}\right).$$

Applying Lemma 17 with $S_p(i) = \int_{v_p(t)=i-\eta} f_p(t)\mathrm{d}t$ if $i \geqslant \eta$ and $S_p(i) = 0$ if not, we get $\lim_{T\to\infty} \sum_{t=-T}^{T} f(t)/2T = \prod_{p|P} \int_{\mathbf{Z}_p} f_p(t)\mathrm{d}t$, as we claimed. □

4.3. APPROXIMATIONS

For our goals, we will have to deal with functions which are not exactly locally constant, so we need to state an analogous of Lebesgue's Dominated Convergence Theorem. Given a bounded function $f\colon \mathbf{Z} \to \mathbf{R}$, we write

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

$$\underline{\mathrm{Av}}_{\mathbf{Z}} f(t) = \liminf_{T\to\infty} \sum_{t=-T}^{T} \frac{f(t)}{2T}, \qquad \overline{\mathrm{Av}}_{\mathbf{Z}} f(t) = \limsup_{T\to\infty} \sum_{t=-T}^{T} \frac{f(t)}{2T}.$$

Moreover, if $\mathcal{I} \subset \mathbf{Z}$, we say that its *density* is

$$\mu(\mathcal{I}) = \limsup_{T\to\infty} \frac{\#\{t \in \mathcal{I} : |t| \leqslant T\}}{2T}.$$

Clearly, $\underline{\mathrm{Av}}_{\mathbf{Z}} f \leqslant \overline{\mathrm{Av}}_{\mathbf{Z}} f$ and equality holds if and only if $f \in L^1(\mathbf{Z})$.

Suppose that $\phi(t) \in L^1(\mathbf{Z})$. Let $f(t)$ be a function $\mathbf{Z} \to \mathbf{R}$ and suppose that $|\phi(t)|$ and $|f(t)|$ are bounded by some $F < \infty$. Let $\mathcal{I} = \{t \in \mathbf{Z} : f(t) \neq \phi(t)\}$. Then it is easy to show that

$$\mathrm{Av}_{\mathbf{Z}} \phi(t) - 2F\mu(\mathcal{I}) \leqslant \underline{\mathrm{Av}}_{\mathbf{Z}} f(t) \leqslant \overline{\mathrm{Av}}_{\mathbf{Z}} f(t) \leqslant \mathrm{Av}_{\mathbf{Z}} \phi(t) + 2F\mu(\mathcal{I}). \tag{9}$$

THEOREM 19. *Let f: $\mathbf{Z} \to \mathbf{R}$ be a bounded function (say by F). Suppose that there is a real number Φ and a family $\{\phi_n\} \subset L^1(\mathbf{Z})$ such that $|\phi_n(t)| < F$, $\lim_{n\to\infty} \mathrm{Av}_{\mathbf{Z}} \phi_n = \Phi$ and $\lim_{n\to\infty} \mu(\mathcal{I}_n) = 0$, where $\mathcal{I}_n = \{t \in \mathbf{Z} : f(t) \neq \phi_n(t)\}$. Then $f \in L^1(\mathbf{Z})$ and $\mathrm{Av}_{\mathbf{Z}} f(t) = \Phi$.*

Proof. Fix $\varepsilon > 0$. Then, by hypothesis, there is a v such that, for every $n \geqslant v$, $|\Phi - \mathrm{Av}_{\mathbf{Z}} \phi_n| < \varepsilon/2$ and $\mu(\mathcal{I}_n) < \varepsilon/4F$. By Equation (9), we have

$$\left|\overline{\mathrm{Av}}_{\mathbf{Z}} f(t) - \Phi\right| \leqslant |\overline{\mathrm{Av}}_{\mathbf{Z}} f(t) - \mathrm{Av}_{\mathbf{Z}} \phi_n| + |\mathrm{Av}_{\mathbf{Z}} \phi_n - \Phi| \leqslant \varepsilon, \quad \text{for } n \geqslant v;$$

and similarly for $\underline{\mathrm{Av}}_{\mathbf{Z}} f(t)$. Since ε is arbitrary, $\underline{\mathrm{Av}}_{\mathbf{Z}} f(t) = \Phi = \overline{\mathrm{Av}}_{\mathbf{Z}} f(t)$, as we claimed. □

5. Proof of Theorem 2

Since we have 'nice' formulæ for the local root numbers, we would like to use Theorems 18 and 19 to approximate $\mathrm{Av} W(E_t)$ by computing, for P large, $\prod_{p<P} \int_{\mathbf{Z}_p} W_p(t)\mathrm{d}t$. The problem is, $\sum_{p>P} 1/p$ does not converge: the approximation is not good enough for Theorem 19. On the other hand, $\sum_{p>P} 1/p^2$ does converge! hence, our plan is to rewrite $W(E_t)$ as a product of local factors ω_p such that $\omega_p(t) = 1$ whenever t is not divisible by p^2.

5.1. THE ROOT NUMBERS REVISITED

Let

$$\tilde{W}_3(t) = \mathrm{sgn}(t) \prod_{p>3} \left(\frac{-3}{p}\right)^{v_p(t)}. \quad \tilde{W}_2(t) = \mathrm{sgn}(t - 1728) \prod_{p>2} \left(\frac{-2}{p}\right)^{v_p(t-1728)}$$

Notice that $\tilde{W}_3(t)$ and $\tilde{W}_2(t + 1728)$ are completely multiplicative functions; in particular, they are monoid maps $\mathbf{Z}^{\neq 0} \to (\mathbf{Z}/3\mathbf{Z})^*$. Recall that we write x'_p to mean $x/p^{v_p(x)}$.

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

LEMMA 20. *We have that*

$$\tilde{W}_3(t) \equiv (-1)^{v_2(t)} t'_3 \bmod 3. \tag{10}$$

$$\tilde{W}_2(t) = \begin{cases} +1 & \text{if } (t-1728)'_2 \equiv 1, 3 \bmod 8, \\ -1 & \text{if } (t-1728)'_2 \equiv 5, 7 \bmod 8; \end{cases} \tag{11}$$

Proof. By quadratic reciprocity, we have that, for every prime $p \neq 3$, $(-3/p) \equiv p \bmod 3$. Thus, Equation (10) follows from

$$\tilde{W}_3(t) = \operatorname{sgn}(t)(-1)^{v_2(t)} \prod_{p \neq 3} \left(\frac{-3}{p}\right)^{v_p(t)} \equiv (-1)^{v_2(t)} t'_3 \bmod 3.$$

Let now w: $\mathbf{Z}^{\neq 0} \to (\mathbf{Z}/3\mathbf{Z})^*$ be the monoid map defined by $w(-1) = -1$, $w(2) = 1$, $w(p) = (-2/p)$ for every $p > 2$. Thus, $\tilde{W}_2(t) = w(t - 1728)$. For every odd prime p we have, by quadratic reciprocity, $w(p) = -1$ if and only if $p \equiv 5, 7 \bmod 8$. Therefore, ω factors through $(\mathbf{Z}/8\mathbf{Z})^*$; i.e., $\omega = \beta \circ \alpha$, where $\alpha(t) \equiv t'_2 \bmod 8$ and $\beta(5) = \beta(-1) = -1$. Since $\alpha(t - 1728) \equiv (t - 1728)'_2 \bmod 8$, we have proved Equation (11). □

DEFINITION. Let

$$\omega_p(t) = W_p(t) \left(\frac{-2}{p}\right)^{v_p(t-1728)} \left(\frac{-3}{p}\right)^{v_p(t)};$$

$$\omega_3(t) = \begin{cases} W_3(t) & \text{if } t'_3 \equiv 1 \bmod 3, \\ -W_3(t) & \text{if } t'_3 \equiv 2 \bmod 3; \end{cases}$$

$$\omega_2(t) = \begin{cases} (-1)^{v_2(t)} W_2(t) & \text{if } (t-1728)'_2 \equiv 1, 3 \bmod 8, \\ (-1)^{v_2(t)+1} W_2(t) & \text{if } (t-1728)'_2 \equiv 5, 7 \bmod 8; \end{cases}$$

Remark 21. If $t \notin [0, 1728]$, then Lemma 20 and the definitions give

$$\begin{aligned} -\prod_{p \geqslant 2} \omega_p(t) &= -\prod_{p=2,3} \tilde{W}_p(t) W_p(t) \cdot \prod_{p>3} W_p(t) \left(\frac{-2}{p}\right)^{v_p(t-1728)} \left(\frac{-3}{p}\right)^{v_p(t)} \\ &= -\prod_{p \geqslant 2} W_p(t) = W(t). \end{aligned}$$

Moreover, for every $p > 3$, Proposition 11 implies that $\omega_p(t) \neq 1$ only if $v_p(t) \geqslant 2$ or $v_p(t - 1728) \geqslant 2$. □

Applying some tedious but straightforward computations to Propositions 13 and 12 we can prove the two following results. (Where, in the left column, if ω_p is not constant in the mentioned case, a necessary and sufficient condition for ω_p to be equal to 1 is given.)

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

PROPOSITION 22. *Let* $t \in \mathbf{Z}_3$. *Then we have*

- *If* $t \not\equiv 1728 \bmod 3^7$*; i.e.,* $v_3(t) \neq 3$ *or* $v_3(t) = 3$ *but* $t'_3 \not\equiv 64 \bmod 81$*, then* ω_3 *is as in Table VII.*
- *If* $t \equiv 1728 \bmod 3^7$*, then* $\omega_3(t) = +1$ *if and only if* $v_3(t - 1728) \not\equiv 2 \bmod 4$.

Table VII. $t \not\equiv 1728 \bmod 3^7$

$v_3(t)$	ω_3
0	$t \equiv 1 \bmod 3$
1	$t'_3 \equiv -1 \bmod 3$
2	-1
3	$t_3 \equiv 4, 7, 8 \bmod 9$, $\equiv 19 \bmod 27$
$> 3, \equiv 0 \bmod 3$	$t'_3 \equiv 4, 7, 8 \bmod 9$
$> 3, \equiv 1 \bmod 3$	$t'_3 \equiv 1 \bmod 3$
$> 3, \equiv 2 \bmod 3$	$t'_3 \equiv 2 \bmod 3$

PROPOSITION 23. *Let* $t \in \mathbf{Z}_2$. *Then we have*

- *If* $v_2(t) \neq 6$*, then* ω_2 *is as in Table VIIIa.*
- *If* $v_2(t) = 6$ *and* $t \not\equiv 1728 \bmod 2^{12}$ *(i.e.,* $t'_2 \not\equiv 27 \bmod 64$*), then* $w_2 = 1$ *if and only if* $t'_2 \equiv 3, 5, 13 \bmod 16$, $\equiv 31 \bmod 32$, $\equiv 7, 55 \bmod 64$ *or* $\equiv 11 \bmod 128$. *If* $t \equiv 1728 \bmod 2^{12}$*, let* $t'' = (t - 1728)'_2$*; then* ω_2 *is as in Table VIIIb.*

Table VIIIa. $t \not\equiv 1728 \bmod 2^{12}$

$v_2(t)$	ω_2
0, 3, 7	$t'_2 \equiv 1, 7 \bmod 8$
1, 4	$t'_2 \equiv 3, 5 \bmod 8$
2	$t'_2 \equiv 1, 3, 5 \bmod 8$
5	$t'_2 \equiv 1, 3 \bmod 8$
8	$t'_2 \equiv 1 \bmod 4$
9	$t'_2 \equiv 3 \bmod 4$
$\geqslant 10$	$v_2(t) \equiv 0 \bmod 2$

Table VIIIb. $t \equiv 1728 \bmod 2^{12}$

$v_2(t - 1728)$	ω_2
$0 \bmod 4$	$t'' \equiv 5, 11, 13, 15$ (16)
$1 \bmod 4$	$+1$
$2 \bmod 4$	$t'' \equiv 7, 9, 13, 15$ (16)
$3 \bmod 4$	-1

5.2. PARTIAL INTEGRALS

PROPOSITION 24. *We have that*

$$\int_{\mathbf{Z}_3} \omega_3(t)\, \mathrm{d}t = -\frac{1027}{14580} \quad \textit{and} \quad \int_{\mathbf{Z}_2} \omega_2(t)\, \mathrm{d}t = \frac{977}{15360}.$$

Proof. Let $\mathcal{I} = \{t \in \mathbf{Z}_3 : v_3(t) = 3, t \not\equiv 1728 \bmod 3^7\}$ and, for $n \geqslant 2$, let $\mathcal{I}_n = \{t \in \mathbf{Z}_3 : 4n - 1 \leqslant v_3(t - 1728) \leqslant 4n + 2\}$. Then,

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

$$\int_{\mathbf{Z}_3} \omega_3(t)\ \mathrm{d}t = \sum_{\substack{e=0\\ e\neq 3}}^{\infty} \int_{v_3(t)=e} \omega_3(t)\ \mathrm{d}t\ + \int_{\mathcal{I}} \omega_3(t)\ \mathrm{d}t + \sum_{n=2}^{\infty} \int_{\mathcal{I}_n} \omega_3(t)\ \mathrm{d}t. \tag{12}$$

If $e \neq 2, 3$, then Proposition 22 implies that $\int_{v_3(t)=e} \omega_3(t)\mathrm{d}t = 0$. If $e = 2$, we get $\int_{v_3(t)=2} \omega_3(t)\ \mathrm{d}t\ = -2/27$. Suppose now that $e = 3$: on one hand, $\int_{\mathcal{I}} = 7/3^7$; on the other, $\int_{\mathcal{I}_n} \omega_3(t)\ \mathrm{d}t = 76/3^{4n+3}$; thus

$$\sum_{n=2}^{\infty} \int_{\mathcal{I}_n} \omega_3(t)\ \mathrm{d}t = \sum_{n=2}^{\infty} \frac{76}{3^{4n+3}} = \frac{19}{43740}.$$

Putting all together, Equation (12) becomes $\int_{\mathbf{Z}_3} \omega_3(t)\ \mathrm{d}t = -1027/14580$, as we claimed.

Define now, as above, $\mathcal{I} = \{t \in \mathbf{Z}_2 : v_2(t) = 6,\ t \not\equiv 1728 \bmod 2^{12}\}$ and, for $n \geqslant 3$, let $\mathcal{I}_n = \{t \in \mathbf{Z}_2 : 4n \leqslant v_2(t - 1728) \leqslant 4n + 3\}$. Then,

$$\int_{\mathbf{Z}_2} \omega_2(t)\ \mathrm{d}t\ = \sum_{\substack{e=0\\ e\neq 6}}^{\infty} \int_{v_2(t)=e} \omega_2(t)\ \mathrm{d}t + \int_{\mathcal{I}} \omega_2(t)\ \mathrm{d}t + \sum_{n=3}^{\infty} \int_{\mathcal{I}_n} \omega_2(t)\ \mathrm{d}t. \tag{13}$$

If $e \in \{0, 1, 3, 4, 5, 7, 8, 9\}$, then $\int_{v_2(t)=e} \omega_2(t)\ \mathrm{d}t = 0$ by Proposition 23. If $e = 2$, by the definition of the p-adic integral (cf. § 4.1) and by Proposition 23, we have

$$\int_{v_2(t)=2} \omega_2(t)\,\mathrm{d}t = \sum_{d\in(\mathbf{Z}/8\mathbf{Z})^*} \frac{\omega_2(4d)}{2^{2+3}} = \frac{3-1}{32} = \frac{1}{16}.$$

If $e \geqslant 10$, we have $\int_{v_2(t)=e} \omega_2(t)\,\mathrm{d}t = (-1)^e \mu(\{v_2(t) = e\})$; thus,

$$\sum_{e=10}^{\infty} \int_{v_2(t)=e} \omega_2(t)\,\mathrm{d}t = \sum_{e=10}^{\infty} \frac{(-1)^e}{2^{e+1}} = \frac{1}{3072}.$$

Suppose now that $e = 6$; then, arguing as above we find $\int_{\mathcal{I}} \omega_2(t)\,\mathrm{d}t = 3/2^{12}$. On the other hand, if $n \geqslant 3$, it is not difficult to check that $\int_{\mathcal{I}_n} \omega_2(t)\,\mathrm{d}t = 3/2^{4n+4}$; hence, $\sum_{n=3}^{\infty} \int_{\mathcal{I}_n} \omega_2(t)\ \mathrm{d}t = 1/20480$. Putting all together, Equation (13) gives $\int_{\mathbf{Z}_2} \omega_2(t)\,\mathrm{d}t = 977/15360$, as we claimed. □

PROPOSITION 25. *For every $p \geqslant 5$, we have*

$$\int_{\mathbf{Z}_p} \omega_p(t)\ \mathrm{d}t = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 12,\\ 1 - \dfrac{2p}{(p^3+1)}, & \text{if } p \equiv 5 \bmod 12,\\ 1 - \dfrac{2p}{(p^3+p^2+p+1)}, & \text{if } p \equiv 7 \bmod 12,\\ 1 - \dfrac{2p}{(p^3+1)} - \dfrac{2p}{(p^3+p^2+p+1)}, & \text{if } p \equiv 11 \bmod 12. \end{cases}$$

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

Proof. Recall that, if both $v_p(t)$ and $v_p(t-1728)$ are zero, then $\omega_p(t)=1$; hence,

$$\int_{\mathbf{Z}_p}\omega_p(t)\,\mathrm{d}t=\mu\big(\{t\in\mathbf{Z}_p : t\neq 0,\,1728 \bmod p\}\big)+ \\ +\int\limits_{v_p(t)>0}\omega_p(t)\,\mathrm{d}t+\int\limits_{v_p(t-1728)>0}\omega_p(t)\,\mathrm{d}t. \tag{14}$$

Notice that, by definition and by Proposition 11, if $v_p(t)=e>0$ (resp. $v_p(t-1728)=e>0$), then $\omega_p(t)=\omega_p(p^e)$ (resp. $\omega_p(t)=\omega_p(p^e+1728)$). Moreover, for every $e\geqslant 1$,

$$\omega_p(p^e)=\begin{cases}-1 & \text{if } p\equiv 2 \bmod 3 \text{ and } e\equiv 2,3,4 \bmod 6,\\ +1 & \text{otherwise;}\end{cases}$$
$$\omega_p(p^e+1728)=\begin{cases}-1 & \text{if } p\equiv 1 \bmod 4 \text{ and } e\equiv 2 \bmod 4,\\ +1 & \text{otherwise.}\end{cases}$$

In particular, $\int_{v_p(t)>0}\omega_p(t)\,\mathrm{d}t=1/p$ if $p\equiv 1 \bmod 3$, while if $p\equiv 3 \bmod 4$, $\int_{v_p(t-1728)>0}\omega_p(t)\,\mathrm{d}t=1/p$.

Suppose now that $p\equiv 2 \bmod 3$, then

$$\int\limits_{v_p(t)>0}\omega_p(t)\,\mathrm{d}t \\ =\mu(\{t\in\mathbf{Z}_p : v_p(t)>0\})-2\sum_{e\equiv 2,3,4\ (6)}\mu(\{t\in\mathbf{Z}_p : v_p(t)=e\}) \\ =\frac{1}{p}-2\left(\frac{1}{p^2}-\frac{1}{p^5}\right)\sum_{e=1}^{\infty}\frac{1}{p^{6e}}=\frac{1}{p}-\frac{2p}{p^3+1}.$$

Finally, if $p\equiv 1 \bmod 4$, by Theorem 19,

$$\int\limits_{v_p(t-1728)>0}\omega_p(t)\mathrm{d}t=\sum_{e=1}^{\infty}\omega_p(p^e+1728)\mu(\{t\in\mathbf{Z}_p : v_p(t-1728)=e\}) \\ =\frac{1}{p}-2\sum_{e\equiv 2\ (4)}\mu(\{t\in\mathbf{Z}_p : v_p(t-1728)=e\}) \\ =\frac{1}{p}-\frac{2p}{p^3+p^2+p+1}.$$

The proposition now follows easily from Equation (14). □

5.3. FINAL STEPS

From now on, we will suppose that $t\notin[0,1728]$: clearly, throwing away a finite number of cases will not make any difference. Hence, $W(E_t)=-\prod_{p=2}^{\infty}\omega_p(t)$ by Remark 21. Let $\Omega(t)=\prod_{p=5}^{\infty}\omega_p(t)$ and, for every prime $P\geqslant 5$, let $\Omega_P(t)=\prod_{p=5}^{P}\omega_p(t)$

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

PROPOSITION 26. *For every prime $P \geqslant 5$ we have that*

$$\mu(\{t \in \mathbf{Z} : \Omega_P(t) \neq \Omega(t)\}) < 2/P.$$

Proof. For every $T > 0$ let $I(T) = [-T, T] \cap \mathbf{Z}$; we have

$$\{t \in I(T) : \Omega_P(t) \neq \Omega(t)\} \subset \{t \in I(T) : \exists p > P : \omega_p(t) = -1\}.$$

Since, by definition, $\omega_p(t) = 1$ whenever $v_p(t), v_p(t - 1728) \leqslant 1$, we get

$$\begin{aligned}
&\#\{t \in I(T) : \Omega_P(t) \neq \Omega(t)\} \\
&\quad < \sum_{P<p<\infty} \#\{t \in I(T) : v_p(t) \geqslant 2 \text{ or } v_p(t - 1728) \geqslant 2\} \\
&\quad = \sum_{p=P+1}^{\sqrt{T}} \left(\frac{4T}{p^2} + \mathrm{O}(1)\right) = \frac{4T}{P} + \mathrm{O}\left(\sqrt{T}\right).
\end{aligned}$$

The proposition follows by considering the limit as $T \to \infty$. □

Proof of Theorem 2. Write Σ_p for $\int_{\mathbf{Z}_p} \omega_p(t)$. Then, by Proposition 26, we can apply Theorems 18 and 19 to $W(t) = -\prod \omega_p(t)$ to get the estimate $\mathrm{Av}_{\mathbf{Z}} W(E_t) = -\prod_{p=2}^{\infty} \Sigma_p$; in particular $W(E_t) \in L^1(\mathbf{Z})$. Moreover, since $|\omega_p| \leqslant 1$,

$$\left|\prod_{p=5}^{\infty} \Sigma_p - \prod_{p=5}^{P} \Sigma_p\right| < 4/P;$$

therefore,

$$\left|\mathrm{Av}_{\mathbf{Z}} W(E_t) + \prod_{p=2}^{P} \Sigma_p\right| < \left|\frac{4\Sigma_2\Sigma_3}{P}\right|.$$

Take $P = 900{,}001$. Using PARI and Propositions 24 and 25, we can compute

$$\prod_{p=2}^{900{,}001} \Sigma_p = -0.003, 718, 27\ldots$$

(We actually computed the result as a rational number, to avoid rounding errors in the product; having the resulting fraction 776,263 figures, we content ourselves with a decimal approximation.) Since $2|\Sigma_2\Sigma_3|/900{,}001 = 0.000, 000, 009\ldots$, the theorem follows. □

Appendix. Numerical Notes

The family (1) was found by computing $\sum_{|t|<T} W(E_t)$ for various families E_t and T large enough; the computations were made using the PARI implementations of the Rohrlich–Halberstadt tables. In Figure 1 we see the graph of $\sum_{|t|<T} W(E_t)/2$ with T

https://doi.org/10.1023/A:1022669121502 Published online by Cambridge University Press

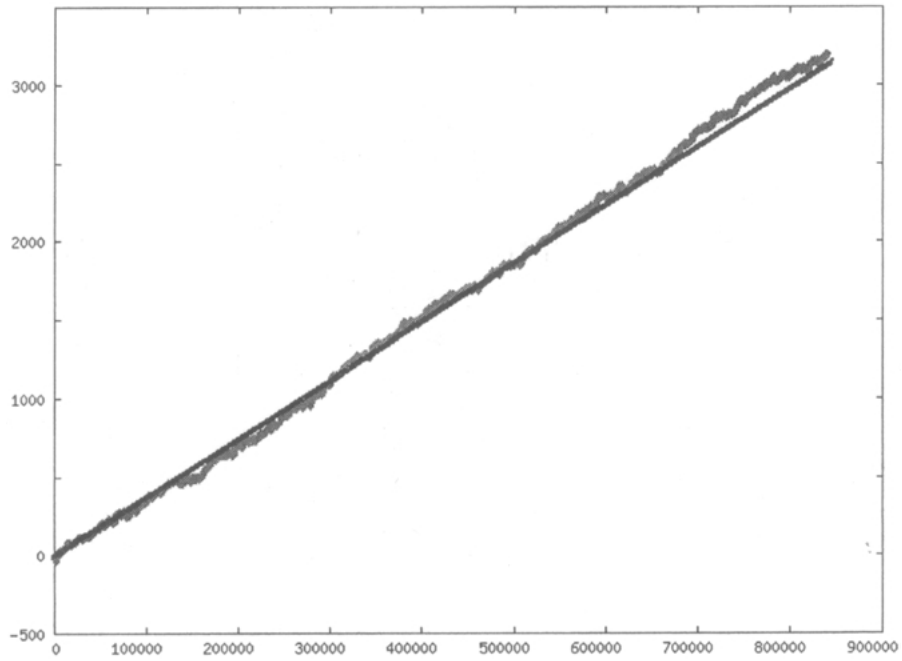

Figure 1. $\frac{1}{2}\sum_{|t|<T} W(E_t)$.

that varies between 0 and 839,447, and the line of slope 0.003,718,2; this 'validates' the proof of Theorem 2.

Acknowledgements

This paper was written in great part while I held a E.U. post-doc position in the 'equipe de Géométrie Algébrique' of the University of Rennes 1, which I want to thank for their warm hospitality; in particular, I am thankful to Bas Edixhoven for many helpful conversations and suggestions. I also thank Henri Cohen for pointing out to me the example of Theorem 1, for developing PARI and for making it free for all to use.

References

1. Cassels, J. W. S. and Schinzel, A.: Selmer's conjecture and families of elliptic curves, *Bull. London Math. Soc.* **14**(4) (1982), 345–348.
2. Connell, I.: Calculating root numbers of elliptic curves over **Q**. *Manuscripta Math.* **82** (1994), 93–104.
3. Diamond, F. and Im, J.: Modular forms and modular curves. In: V. K. Murty (ed.), *Seminar on Fermat's Last Theorem*, CMS Conf. Proc. 17, Amer. Math. Soc., Providence, 1994, pp. 39–133.

4. Duquesne, S.: Integral points on elliptic curves defined by simplest cubic fields, *Experiment Math.* **10**(1) (2001), 91–102.
5. Edixhoven, B.: Rational elliptic curves are modular (after Breuil, Conrad, Diamond and Taylor), *Séminaire Bourbaki* **871** (2000). In: *Astérisque* **276** (2002), 161–188.
6. Halberstadt, E.: Signes locaux des courbes elliptiques en 2 et 3, *C.R. Acad. Sci. Paris, Sér. I Math.* **326** (1998), 1047–1052.
7. Papadopoulos, I.: Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3, *J. Number Theory* **44**(2) (1993), 119–152.
8. Rizzo, O. G.: On the variation of root numbers in families of elliptic curves, PhD thesis, Brown University, Providence, Rhode Is, 1997.
9. Rizzo, O. G.: Average root numbers in families of elliptic curves, *Proc. Amer. Math. Soc.* **127**(6) (1999), 1597–1603.
10. Rizzo, O. G.: Average root numbers for a non-constant family of elliptic curves, Prépublication 00-24, IRMAR, Université de Rennes 1, 2000.
11. Rohrlich, D. E.: Variation of the root number in families of elliptic curves, *Compositio Math.* **87**(2) (1993), 119–151.
12. Rohrlich, D. E.: Elliptic curves and the Weil–Deligne group. In: H. Kisilevsky and M. R. Murty (eds), *Elliptic Curves and Related Topics*, CRM Proc. Lecture Notes 4, Amer. Math. Soc., Providence, 1994, pp. 125–157.
13. Silverman, J. H.: *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer-Verlag, New York, 1986.
14. Silverman, J. H.: The average rank of an algebraic family of elliptic curves, *J. Reine Angew. Math.* **504** (1998), 227–236.
15. Washington, L. C.: Class numbers of the simplest cubic fields. *Math. Comp.* **48**(177) (1987), 371–384.
16. Zagier, D. and Kramarz, G.: Numerical investigations related to the *L*-series of certain elliptic curves, *J. Indian Math. Soc.* **52** (1987), 51–69.