COMPUTING A HEEGNER POINT p-ADIC HEIGHT, (MOTIVATED BY A CONJECTURE OF MAZUR-RUBIN)

JENNIFER BALAKRISHNAN, MIRELA ÇIPERIANI, AND WILLIAM STEIN

Abstract.

1. Introduction

2. Example (first layer)

Let $p = 5$, let E be the elliptic curve 57a1, and let $K = \mathbb{Q}(\sqrt{-2})$. Let $K[c]$ denote the ring class field extension of K associated to the conductor c. Let $x_{25} \in X_0(57)(K[25])$ be the Heegner point for $c = 25$ and via the modular parametrization $\pi : X_0(57) \to E$, let $y_{25} = \pi(x_{25}) \in E(K[25])$ be its image.

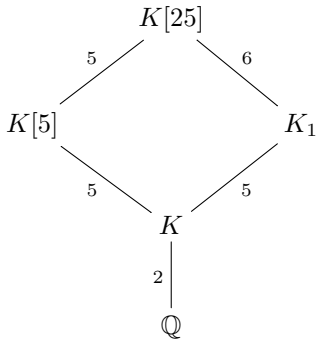
We have $K[1] = K$ (i.e., class number 1), and

$$\mathrm{Gal}(K[25]/K) \cong (\mathcal{O}_K/25\mathcal{O}_K)^*/(\mathbb{Z}/25\mathbb{Z})^* \approx \mathbb{P}^1(\mathbb{Z}/25\mathbb{Z}),$$

which is cyclic of order $5 \cdot 6$. Thus we have the tower

$$K \subset K_1 \subset K[25]$$

fitting into the following diagram



where K_1/K is cyclic of degree 5 and $K[25]/K_1$ is cyclic of degree 6.

Let σ be a generator of $\mathrm{Gal}(K[25]/K_1)$, so σ is of order 6. The points we're interested in are

$$z = \mathrm{Tr}_{K[25]/K_1}(y_{25}) = \sum_{i=0}^{5} \sigma^i(y_{25}),$$

and its Galois conjugates.

Question 2.1 (Mazur)**.** What are the 5-adic heights (i.e., mod 5^n, with n not too large being perfectly OK for us, and here we mean standard p-adic heights—related to the p-cyclotomic extension) of the conjugates of z?

2.1. **Computing z.** How this is done:

(1) Using the fact that conjugates of x_c correspond to binary quadratic forms of discriminant $\mathrm{disc}(O_c)$, we begin by enumerating the 30 primitive binary quadratic forms up to equivalence of discriminant $\mathrm{disc}(\mathcal{O}_c) = D{\cdot}c^2 = -8{\cdot}5^4$ that correspond to Heegner points of this conductor, i.e., *for which $N \mid A$ and* $\gcd(A/N, B, CN) = 1$ *(see prop 2.2 of* [**?**]*).* **Actually, this needs William's generalization of Prop 2.2 of Watkins.**

(2) For each of these 30 primitive binary quadratic forms $Q = Ax^2 + Bxy + Cy^2$, we compute the ideal $I = (A, (-B + c\sqrt{D})/2)\mathcal{O}_K$ and find a generator α_Q of this principal ideal. Then we compute the multiplicative order of the class of α_Q in $(\mathcal{O}_K/25\mathcal{O}_K)^*/(\mathbb{Z}/25\mathbb{Z})^*$. We find an element with multiplicative order 6.

(3) Now we have $\alpha = \alpha_Q$ whose class has multiplicative order 6, so it corresponds to the σ of order 6 chosen above. To compute $\sigma^i(y_{25})$ for $i = 0, \ldots, 5$ we proceed as follows:
   (a) Binary quadratic forms correspond to conjugates of x_{25} as follows. The form $f = Ax^2 + Bxy + Cy^2$ corresponding to $[\tau_f] \in X_0(N)$, where $f(\tau_f, 1) = 0$ and $\tau_f \in \mathfrak{h}$; explicitly, $\tau_f = (-B + c\sqrt{D})/(2A)$.
   (b) Choose any $[\alpha_0] \in (\mathcal{O}_K/25\mathcal{O}_K)^*/(\mathbb{Z}/25\mathbb{Z})^*$ corresponding to some $\sigma_0 \in G$, and let $y'_{25} = \sigma(y_{25})$.
   (c) Then $\sigma^i(y'_{25})$ is the point corresponding to $[\alpha^i\alpha_0]$. Since our group is abelian, we can thus compute a conjugate of z by computing
   $$\sum \sigma^i(y'_{25}) = \sum \sigma^i\sigma_0(y_{25}) = \sigma_0(z),$$
   and that is good enough for our application.

(4) Recognize the x-coordinate of $z \in E(\mathbb{C})$ using algdep, and get a y-coordinate. Make sure that z is defined over a Galois dihedral field of degree 10 that is ramified exactly at 2 and 5, by checking that discriminant of defining poly of x coordinate is divisible by 2 and 5 and the coprime to 10 part is a perfect square.

The x-coordinate of z satisfies

$$18034072681x^5 - 126430131580x^4 + 352783410220x^3 - 489834319200x^2 + 338504989540x - 93144838864.$$

The point z is defined over

$$L := \mathbb{Q}(b_3),$$

where b_3 is a root of

$$x^{10} - 10x^8 - 20x^7 + 165x^6 - 12x^5 - 760x^3 + 2220x^2 + 5280x + 7744.$$

(This is not a **theorem** because there are no proven error bounds on our computations; but it's inconceivable that this is wrong.)

Explicitly, we will compute with z with x-coordinate

$$\begin{aligned} x(z) = {} & \frac{96698852571685}{2145672615243325696}b_3^9 + \frac{2472249905907}{195061146840302336}b_3^8 + \frac{916693155514421}{2145672615243325696}b_3^7 + \frac{1348520950997779}{2145672615243325696}b_3^6 \\ & - \frac{82344497086595}{12191321677518896}b_3^5 + \frac{2627122040194919}{536418153810831424}b_3^4 - \frac{452199105143745}{48765286710075584}b_3^3 \\ & + \frac{4317002771457621}{536418153810831424}b_3^2 + \frac{2050725777454935}{67052269226353928}b_3 + \frac{3711967683469209}{3047830419379724}. \end{aligned}$$

2.2. **Computing p-adic Heights.** By the work of Mazur-Stein-Tate [**?**], we have that the cyclotomic p-adic height of P can be computed as

$$h_p(P) = \frac{1}{p} \cdot \left(\sum_{v|p} \log_p(N_{K_v/\mathbb{Q}_p}(\sigma_v(P))) - \sum_{w\nmid p} \mathrm{ord}_w(d_w(P)) \cdot \log_p(\#k_w) \right).$$

We will return to this formula later[1], but for now, we use the following:

If we assume that P lies in a sufficiently small (finite index) subgroup of $E(K)$ (see [**?**, Prop. 2]), then there will be a global choice of denominator $d(P)$, and the formula simplifies to

$$h_p(P) = \frac{1}{p} \cdot \log_p \left(\prod_{v|p} N_{K_v/\mathbb{Q}_p} \left(\frac{\sigma_v(P)}{d(P)} \right) \right). \tag{2.1}$$

More precisely, since our point z does not necessarily lie in this sufficiently small subgroup of $E(K)$, we compute an appropriate n such that nz does lie in the subgroup, compute the height of nz by (2.1), then use the fact that the height pairing is a quadratic form to recover the height of our original point.

We begin by computing the denominator $d(nz)$ of nz, which in turn requires that we compute the denominator $d := d(z)$ of z. Note that this requires that we work over a PID, since we wish to write each coordinate of z as the ratio of two integral elements. The goal then is to write $z = (x, y)$ as $(\frac{a}{d^2}, \frac{b}{d^3})$, such that $(a, d) = (b, d) = 1$ and $a, b, d \in \mathcal{O}_L$.

2.2.1. *Computing $d(z)$.*

(1) We start with $z = (x, y)$ as a point on the elliptic curve, where $x, y \in L$. We begin by writing the ideal I generated by (x, y), and compute its GCD by writing it as a principal ideal $I = (g)$ and reading off the generator g. In our case,

$$\begin{aligned} g = {} & \frac{123984834273901806131}{45238689824261707813521152} b_3^9 + \frac{18086333051389614235}{41126081658419734375928 32} b_3^8 \\ & - \frac{2034338252029802812739}{45238689824261707813521152} b_3^7 - \frac{1210137739879154041477}{45238689824261707813521152} b_3^6 \\ & + \frac{45162732628910301745}{25703801036512333984955 2} b_3^5 + \frac{20860129147970487107559}{11309672456065426953380288} b_3^4 \\ & - \frac{5232862309605254732233}{10281520414604935939820 8} b_3^3 + \frac{73696187951449076337469}{11309672456065426953380288} b_3^2 \\ & - \frac{11829570856332514083089}{14137090570081783691725 36} b_3 + \frac{2848093589238986978981}{64259502591280834962388}. \end{aligned}$$

(2) Read off the integer denominator $d(g)$ of g, and re-express the coordinates of z in terms of a numerator (ideal) over this integer denominator (ideal). In our example,

$$d(g) = 45238689824261707813521152.$$

(3) Simplify the coordinates of z by canceling common prime ideals in the numerator and denominator ideals.

(4) What is left in the factored denominator ideal is a perfect cube of prime ideals in the ring of integers of L, and a cube root of this is the desired denominator $d(z)$. In our example, we find that

$$\begin{aligned} d(z) = {} & -\frac{170066107}{18679674112} b_3^9 + \frac{46616573}{1698152192} b_3^8 + \frac{3760482603}{18679674112} b_3^7 - \frac{11188479427}{18679674112} b_3^6 - \frac{263947335}{106134512} b_3^5 \\ & + \frac{40187214425}{4669918528} b_3^4 + \frac{1074830385}{424538048} b_3^3 - \frac{67626028101}{4669918528} b_3^2 - \frac{15616668599}{583739816} b_3 + \frac{738093651}{26533628}. \end{aligned}$$

[1]TODO: It'd be another good numerical consistency check to compute the height directly this way...

2.2.2. *Computing $d(nz)$.* One could repeat the above process for nz, but this would be slightly tedious due to the numerical explosion in the coordinates of nz. Instead, we make use of n-division polynomials to write $d(nz)$ in terms of $d(z)$.

Lemma 2.2. *Let f_n be the nth division polynomial of E. Then*

$$d(nz) = f_n(x(z))d(z)^{n^2}.$$

2.2.3. *An algorithm for the height of z.*

(1) Compute z.
(2) Compute n and nz. This n is a positive integer such that nz reduces[2] to $\mathcal{O} \in E(\mathbb{F}_p)$ (resp. $E(\mathbb{F}_{p^2})$) and to the connected component of $\mathcal{E}_{\mathbb{F}_\ell}$ at all bad primes ℓ. If the torsion subgroup of E is trivial, then as P is a Heegner point, by a theorem of Gross-Zagier, this second condition is automatic, so n can be taken to be $\#E(\mathbb{F}_p)$ (resp. $\#E(\mathbb{F}_{p^2})$). (Note that in practice, one wants n to be as small as possible, to reduce numerical explosion in the coordinates.)
(3) Compute $d(z)$ and $d(nz)$.
(4) Compute $\sigma_v(t)$ the v-adic σ function above p as in [**?**]. Note that p is *a priori* totally ramified in L, so there is just one v above p.
(5) Let $t_n = -\frac{x(nz)}{y(nz)}$. Evaluate $\sigma_v(t_n)$ and compute

$$h_p(z) = \frac{1}{n^2 p} \log_p \left(N_{K_v/\mathbb{Q}_p} \left(\frac{\sigma_v(t_n)}{d(nz)} \right) \right).$$

For our example, we may take $n = 3$. Indeed, the point z reduces to $(4, 1) \in E(\mathbb{F}_5)$, and we see that $3z = \mathcal{O} \in E(\mathbb{F}_5)$.

Moreover, we have

$$\begin{aligned}\sigma_5(t) = {} & \left(1 + O(5^{10})\right) t + O(5^9)t^2 + \left(1 + 2 \cdot 5 + 2 \cdot 5^3 + 4 \cdot 5^5 + 4 \cdot 5^6 + O(5^8)\right) t^3 \\ & + \left(3 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 2 \cdot 5^6 + O(5^7)\right) t^4 \\ & + \left(1 + 4 \cdot 5 + 3 \cdot 5^3 + 4 \cdot 5^4 + O(5^6)\right) t^5 + \left(1 + 3 \cdot 5 + 3 \cdot 5^3 + O(5^5)\right) t^6 \\ & + \left(5^2 + 5^3 + O(5^4)\right) t^7 + \left(3 + 4 \cdot 5 + 3 \cdot 5^2 + O(5^3)\right) t^8 \\ & + \left(2 + 2 \cdot 5 + O(5^2)\right) t^9 + \left(1 + O(5)\right) t^{10} + O(t^{11}).\end{aligned}$$

Then substituting the appropriate parameters into (2.1), we find that

$$h_5(z) = 2 + 4 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 5^4 + 3 \cdot 5^5 + O(5^6).$$

Repeating the computation with $n = 9$ serves as a numerical consistency check.

3. Example: twisting

We take the previous example and take a quadratic twist by $\sqrt{41}$. This gives us the elliptic curve

$$E_{41} : y^2 + y = x^3 + x^2 - 3922x + 102712.$$

We have that E_{41} has rank 1 over $\mathbb{Q}$ as well as over K. A generator P of E_{41} has height divisible by $p = 5$ as well. So we repeat the computation as above.

We find that a traced Heegner point z in K_5 has x-coordinate

...

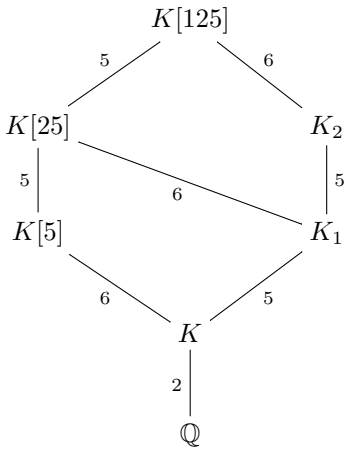
[2]depending on which is relevant; since p is inert, this amounts to how complex conjugation $\tau \in \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ acts. In our case, since E has rank 1, $\varepsilon = -1$, and $(nz)^\tau = -\varepsilon nz = nz$. So $nz \in E(\mathbb{F}_p)$.

with denominator $d(z) =$.
As z reduces to in $E(\mathbb{F}_5)$, we have that $n =$, and we use this to compute

$$h(z) = .$$

4. Example (second layer)

We could try to compute with the next layer of the anti-cyclotomic tower.
For convenience, here are the relevant fields in the tower along with their relative degrees:



The idea is very similar to before: we use a generator of $\mathrm{Gal}(K[125]/K_2)$ (again, of order 6) to compute the trace of y_{125} from $K[125]$ to K_2, then use algebraic dependency to recognize the extension K_2/K, which we then write as a degree 50 extension over $\mathbb{Q}$.

Remark 4.1. We have gotten as far as finding the x-coordinate of the Heegner point as an element of a field that has the right properties (degree 50 over $\mathbb{Q}$ and with discriminant divisible by $(\mathrm{disc}(K_1/\mathbb{Q}))^5$)

5. Example: fixing E, p, varying K

Let E be the elliptic curve 89a1, and fix $p = 5$. We have the fields with discriminants $D = -8, -11, -67$ satisfying the necessary hypotheses.

We have that the height of a Mordell-Weil generator P is

$$h_p(P) = 2 \cdot 5 + 5^2 + 3 \cdot 5^3 + 2 \cdot 5^4 + 3 \cdot 5^5 + 3 \cdot 5^6 + 4 \cdot 5^8 + O(5^{10}).$$

5.1. $D = -8$.

$$K_1 = \mathbb{Q}[b_3]/(b_3^{10} - 10b_3^8 - 20b_3^7 + 165b_3^6 - 12b_3^5 - 760b_3^3 + 2220b_3^2 + 5280b_3 + 7744)$$

$$d(z) = -\frac{184960682133}{583739816}b_3^9 + \frac{201372405891}{106134512}b_3^8 - \frac{4427090691257}{1167479632}b_3^7 + \frac{2576122895483}{1167479632}b_3^6 - \frac{1047171187695}{106134512}b_3^5 + \frac{3808621305257}{145934954}b_3^4 - \frac{402890182961}{26533628}b_3^3 - \frac{13515253550229}{291869908}b_3^2 - \frac{50649651812995}{291869908}b_3 - \frac{123445723611}{6633407}$$

$$z = \left(\frac{1802706589}{409822531712}b_3^9 - \frac{64304775}{37256593792}b_3^8 - \frac{20879156681}{409822531712}b_3^7 - \frac{20852393943}{409822531712}b_3^6 + \frac{7470954657}{9314148448}b_3^5 - \frac{38479444339}{102455632928}b_3^4 - \frac{113}{93}\right.$$

which reduces to $(0,0)$ in $E(\mathbb{F}_5)$, and this point has order 7. We use $n = 7, 14$ to compute the p-adic height.

$$h_p(z) = 4 + 3\cdot 5 + 4\cdot 5^2 + 5^3 + 4\cdot 5^4 + 5^5 + 5^7 + 4\cdot 5^8 + O(5^9).$$

5.2. $D = -67$.

$$K_1 = \mathbb{Q}[b_3]/(b_3^{10} - 40b_3^8 + 480b_3^6 + 75b_3^4 - 43960b_3^2 + 309808)$$

$$\begin{aligned} d(z) = {} & \frac{7187590315133071453604830959059 5}{7117152} b_3^9 + \frac{611957950770485997621380538373 9}{145248} b_3^8 \\ & - \frac{135897523348126877771180458895081}{593096} b_3^7 - \frac{116638857276970229728554941831 41}{12104} b_3^6 \\ & + \frac{866117541122609648136522585991 0}{10591} b_3^5 + \frac{104811862809256350526264813259 99}{3026} b_3^4 \\ & + \frac{363911719634389635190699025329574 35}{2372384} b_3^3 + \frac{310826594839174268542876170977 4419}{48416} b_3^2 \\ & - \frac{314460166167253356319310621824691521}{1779288} b_3 - \frac{159299456824137460113650173418 3561}{2136} \end{aligned}$$

$$z = \Bigg(- \frac{285606751909510601256037145422 3181}{168301494714657394033607702572179150 24} b_3^8 + \frac{796049750033362909950071080944840 43}{168301494714657394033607702572179150 24} b_3^6 - \frac{438744543341}{1683014947146}$$

which reduces to $(2,0)$ in $E(\mathbb{F}_5)$, and we use $n = 7, 14$ to compute the p-adic height:

$$h_p(z) = 3 + 2\cdot 5 + 5^2 + 5^3 + 2\cdot 5^4 + 2\cdot 5^6 + 4\cdot 5^7 + O(5^8).$$

6. Going up the anti-cyclotomic tower

This has non-linear polynomial:
$E = 158b1, D = -7, p = 5$
Height of a MW generator P:

$$h_p(P) = 2\cdot 5 + 5^2 + 2\cdot 5^5 + 3\cdot 5^6 + 4\cdot 5^7 + 5^8 + 3\cdot 5^9 + O(5^{10})$$

We have

$$K_1 = \mathbb{Q}[b_4]/(b_4^{10} - 20b_4^8 - 25b_4^7 + 260b_4^6 + 49b_4^5 + 525b_4^4 - 200b_4^3 + 705b_4^2 - 85b_4 + 617).$$

We have

$$\begin{aligned} d(z) = {} & -\frac{6492339886}{3631485879} b_4^9 + \frac{3731642890}{3631485879} b_4^8 + \frac{136176671707}{3631485879} b_4^7 + \frac{1211499568}{57642633} b_4^6 - \frac{65643271261}{125223651} b_4^5 \\ & + \frac{2822926228}{14021181} b_4^4 - \frac{199895608687}{518783697} b_4^3 + \frac{104410975006}{1210495293} b_4^2 - \frac{444144852182}{1210495293} b_4 - \frac{903689351762}{3631485879} \end{aligned}$$

and

$$z = \Bigg(\frac{2591369386796327995028}{38000606630179530113601 3} b_4^9 + \frac{14888842387016594709925}{3800060663017953011360 13} b_4^8 - \frac{60132612773564347609430}{38000606630179530113601 3} b_4^7 - \frac{42044016343105}{42222896255755}$$

This reduces to $(1,0)$ in $E(\mathbb{F}_5)$, which has order 7. We use $n = 7, 14$ to compute the height:

$$h_p(z) = 3\cdot 5 + 4\cdot 5^2 + 2\cdot 5^3 + 4\cdot 5^4 + 4\cdot 5^5 + O(5^6).$$

So we'd like to go the next level up...

7. Higher valuation

$E = 214b1, D = -7, p = 5$
Height of MW gen:

$$h_p(P) = 4 \cdot 5^2 + 3 \cdot 5^3 + 3 \cdot 5^4 + 5^8 + 2 \cdot 5^{12} + 3 \cdot 5^{13} + 2 \cdot 5^{14} + 3 \cdot 5^{15} + 4 \cdot 5^{17} + 2 \cdot 5^{18} + O(5^{19})$$

We have

$$K_1 = \mathbb{Q}[b_4]/(b_4^{10} - 20b_4^8 - 25b_4^7 + 260b_4^6 + 49b_4^5 + 525b_4^4 - 200b_4^3 + 705b_4^2 - 85b_4 + 617).$$

$$\begin{aligned} d(z) = &-\frac{55207226496320}{2824489017}b_4^9 - \frac{21659558622586}{941496339}b_4^8 + \frac{425994429247118}{941496339}b_4^7 + \frac{2546474905061947}{2824489017}b_4^6 \\ &- \frac{561982398059725}{97396173}b_4^5 - \frac{566184447353632}{76337541}b_4^4 + \frac{1987085301419457}{313832113}b_4^3 - \frac{53653231928520598}{2824489017}b_4^2 \\ &+ \frac{33500836567973212}{2824489017}b_4 - \frac{55170079769161475}{2824489017} \end{aligned}$$

$$z = \left(-\frac{2078748072945839}{3434191491764983131}b_4^9 + \frac{16748042702008406}{3434191491764983131}b_4^8 + \frac{5136977149233923}{490598784537854733}b_4^7 - \frac{103545523100105017}{1144730497254994377}b_4^6 - \frac{2879}{11842}\right.$$

which reduces to $(0, 4)$ in $E(\mathbb{F}_5)$, which has order 7.
We use $n = 7, 14$ to compute the heights:

$$h_p(z) = 2 + 2 \cdot 5 + 3 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 3 \cdot 5^6 + O(5^7)$$