Upper half-plane formulas

We want to explain the derivation of formulas for two types of objects on the upper half plane: the Atkin-Lehner involutions and Heegner points. Both of these are treated somewhat briefly in Gross-Zagier. The explicit description characterizing those $\tau \in \mathfrak{h}$ which correspond to Heegner points relative to the "standard model" of $Y_0(N)$ is a somewhat involved exercise with imaginary quadratic fields, and the formulas obtained (or rather, asserted) on p. 236 of G-Z have some sign errors (which we fix below). The discussion in Chapter 8, §1–2 of Lang's *Elliptic Functions* was helpful for efficiently working out the details in the case of Heegner points.

Throughout this discussion, we fix the following running hypotheses. We let $N \geq 1$ be an integer, $K \subseteq \mathbf{C}$ an imaginary quadratic field with odd discriminant $D < 0$ where $(N, D) = 1$ (in particular, $D \equiv 1 \bmod 4$ and $\mathscr{O}_K = \mathbf{Z}[(1+\sqrt{D})/2] = \mathbf{Z}[(D+\sqrt{D})/2]$), and we assume that all primes $p|N$ are split in K. We let $\mathscr{O}$ denote the ring of integers of K. Here and always we let $\sqrt{D}$ denote the unique square root of D in the upper half-plane with which we're working.

We let s denote the number of prime factors of N, and we denote by $\mathfrak{n}$ an integral ideal with norm N which is not divisible by any rational integer > 1 (so $\mathfrak{n}$ is a product of "half" of the prime-power factors of N, with one choice of prime from each pair of primes over each $p|N$). Such $\mathfrak{n}$ will be called *primitive divisors of* N, and these are exactly the ideals in $\mathscr{O}$ for which $\mathscr{O}/\mathfrak{n} \simeq \mathbf{Z}/N$ as abelian groups.

1. Involutions

Fix a positive integer $d|N$ with $(d, N/d) = 1$. We have a (set-theoretic) involution

$$w_d : Y_0(N) \to Y_0(N)$$

given by

$$(E, C = C_d \times C_{N/d}) \to (E/C_d, C_{N/d} \times E[d]/C_d)$$

where C_d denotes the "d-part" of the cyclic group C of order N. For a point (or rather, isomorphism class)

$$(\mathbf{C}/[1, z], \langle 1/N \rangle) \in Y_0(N)$$

applying the w_d construction yields the pair

$$(\mathbf{C}/[1/d, z], \langle d/N, z/d \rangle) \simeq (\mathbf{C}/[1, d \cdot z], \langle d^2/N, z \rangle)$$

using multiplication by d on $\mathbf{C}$.

In order to (hopefully) "compute" $w_d(z)$ in terms of a linear fractional transformation applied to z, we need to put this final expression in standard form. That is, we seek to find a matrix

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$$

such that the multiplication map

$$(\gamma d \cdot z + \delta)^{-1} : \mathbf{C}/[1, d \cdot z] = \mathbf{C}/[\alpha d \cdot z + \beta, \gamma d \cdot z + \delta] \simeq \mathbf{C}/[1, A(d \cdot z)]$$

carries the cyclic subgroup $\langle d^2/N, z \rangle$ over to $\langle 1/N \rangle \bmod [1, A(d \cdot z)]$. Now since we are dealing with an isomorphism and two groups which we know a priori to be cyclic of order N, for counting reasons it is necessary and sufficient for our map to merely carry the first of these two cyclic groups *into* the second.

That is, we need the existence of integers r, s such that

$$\frac{d^2}{N(\gamma d \cdot z + \delta)} \equiv \frac{r}{N} \bmod [1, A(d \cdot z)], \quad \frac{z}{\gamma d \cdot z + \delta} \equiv \frac{s}{N} \bmod [1, A(d \cdot z)].$$

Multiplying the congruences through by $N(\gamma d \cdot z + \delta)$, this is the same as

$$d^2 \equiv r(\gamma d \cdot z + \delta) \bmod [N, Nd \cdot z], \quad Nz \equiv s(\gamma d \cdot z + \delta) \bmod [N, Nd \cdot z].$$

Comparing coefficients of 1 and z, this translates into the congruence conditions

$$r\gamma \equiv 0 \bmod N/d, \quad d^2 \equiv r\delta \bmod N, \quad s\delta \equiv 0 \bmod N, \quad N/d \equiv s\gamma \bmod N.$$

Since d and N/d are relatively prime we can break these conditions (for existence of r and s) into congruences modulo d and N/d. We get

$$r\gamma \equiv 0,\ d^2 \equiv r\delta,\ s\delta \equiv 0,\ s\gamma \equiv 0 \bmod N/d$$

and

$$r\delta \equiv 0,\ s\delta \equiv 0,\ s\gamma \equiv N/d \bmod d.$$

Since d^2 is a unit mod N/d, we see r, γ must be units mod N/d, so then the vanishing of $r\gamma$ and $s\delta$ mod N/d forces $\gamma, s \equiv 0 \bmod N/d$. Meanwhile, with $s\gamma \equiv N/d \bmod d$ where N/d is a unit mod d, we see that s, γ are units mod d, so the vanishing of $s\delta$ mod d says exactly $\delta \equiv 0 \bmod d$.

To summarize, the necessary and sufficient conditions on our original matrix A are that $\gamma \equiv 0 \bmod N/d$ with γ a unit mod d, while $\delta \equiv 0 \bmod d$ and δ is a unit mod N/d. That is,

$$A = \begin{pmatrix} \alpha & \beta \\ (N/d)x & dy \end{pmatrix}$$

with determinant 1 (which forces x to be a unit mod d and y to be a unit mod N/d, as is certainly necessary). But then $w_d(z) = A(d \cdot z)$ is described by applying the linear fractional transformation

$$\begin{pmatrix} \alpha & \beta \\ (N/d)x & dy \end{pmatrix} \cdot \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} d \cdot \alpha & \beta \\ Nx & d \cdot y \end{pmatrix}$$

with arbitrary $x, y, \alpha, \beta \in \mathbf{Z}$ and determinant d.

This shows that the set of matrices which can be used to represent the action of w_d is exactly the set of matrices of the form

$$\begin{pmatrix} d\mathbf{Z} & \mathbf{Z} \\ N\mathbf{Z} & d\mathbf{Z} \end{pmatrix}$$

with determinant d, exactly as asserted by Gross and Zagier on the top of p. 235.

2. Heegner points

We have described Heegner points in terms of diagrams

$$(\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1})$$

where $\mathfrak{a}$ is a fractional ideal of K and $\mathfrak{n}$ is a primitive divisor of N. Such a description is parameterized by the 2^s choices of $\mathfrak{n}$ and the elements of the class group (as the isomorphism class of the above Heegner data depends on $\mathfrak{a}$ only up to its image in the class group).

We want to give an exhaustive list of points $\tau \in \mathfrak{h}$ which represent all of the Heegner points for K on $Y_0(N)$. For our later purposes we will want τ to encode the data of a specific $\mathfrak{a}$ as well as a specific $\mathfrak{n}$. To do this, it is simpler to begin by first presenting a description of the 2^s possibilities for $\mathfrak{n}$ in "upper half-plane" terms.

Consider $\beta \in \mathbf{Z}/2N$. Its square $\beta^2 \in \mathbf{Z}/4N$ is well-defined, and we wish to consider the condition that $\beta^2 \equiv D \bmod 4N$. Note that since D is odd and relatively prime to N, in particular this forces β to be a unit mod $2N$. For any odd prime $p|N$ the condition $\beta^2 \equiv D \bmod 4N$ determines $\beta \bmod p^{\mathrm{ord}_p(N)}$ up to sign, while the fact that β^2 is specified modulo $4 \cdot 2^{\mathrm{ord}_2(N)}$ implies that $\beta \bmod 2 \cdot 2^{\mathrm{ord}_2(N)}$ is also unique up to sign (such a sign issue arising from $2|N$ iff $2 \cdot 2^{\mathrm{ord}_2(N)}$ is divisible at least by 4). In other words, the number of such β's is exactly 2^s, since we choose one sign for each $p|N$. Of course, this all rests on the fact that the equation $x^2 \equiv D \bmod 4N$ admits *some* solution, which is to say that D mod 4 must be a square and D mod p must be a square for all $p|N$. But $D \equiv 1 \bmod 4$, so there's no problem at 2, and for odd $p|N$ we have p split in $K = \mathbf{Q}(\sqrt{D})$ (with D the odd discriminant of K), so indeed D is a square mod p.

In summary, the set of $\beta \in \mathbf{Z}/2N$ satisfying $\beta^2 \equiv D \bmod 4N$ is of size 2^s, which is exactly the same as the size of the set of possible $\mathfrak{n}$'s. Now for each such β, we define the $\mathscr{O}$-ideal

$$\mathfrak{n}_\beta = (N, (\widetilde{\beta} + \sqrt{D})/2) = N\mathbf{Z} + \frac{\widetilde{\beta} + \sqrt{D}}{2} \cdot \mathbf{Z}$$

where $\widetilde{\beta} \in \mathbf{Z}$ is a representative of $\beta \in \mathbf{Z}/2N$, the choice of which doesn't affect the underlying $\mathscr{O}$-ideal. The reason the indicated elements form a $\mathbf{Z}$-basis of the $\mathscr{O}$-ideal $\mathfrak{n}_\beta$ is because the *oddness* of $\widetilde{\beta}$ (D is odd!) ensures that 1 and $(\widetilde{\beta} - \sqrt{D})/2$ form a $\mathbf{Z}$-basis of $\mathscr{O}$ and

$$\frac{\widetilde{\beta} - \sqrt{D}}{2} \cdot \frac{\widetilde{\beta} + \sqrt{D}}{2} = \frac{\widetilde{\beta}^2 - D}{4} \in N\mathbf{Z}.$$

It is the appearance of expressions like $(\widetilde{\beta} + \sqrt{D})/2$ which leads us to view this as an "upper half-plane" description of $\mathfrak{n}_\beta$. We now state the classification of primitive divisors $\mathfrak{n}$ of N in such "upper half-plane" terms.

Theorem 2.1. *For each $\beta \in \mathbf{Z}/2N$ satisfying $\beta^2 \equiv D \bmod 4N$, the integral ideal $\mathfrak{n}_\beta$ is a primitive divisor of N, and every primitive divisor of N is of this form for a unique such β.*

For a primitive divisor $\mathfrak{n}$ of N, we will refer to the element $\beta \in \mathbf{Z}/2N$ from the theorem with $\mathfrak{n}_\beta = \mathfrak{n}$ as the *β-invariant* of $\mathfrak{n}$ (this is somewhat abusive terminilogy, but it is convenient).

Proof. If $\mathfrak{n}_\beta = \mathfrak{n}_{\beta'}$ then

$$(\widetilde{\beta} - \widetilde{\beta}')/2 \in \mathfrak{n}_\beta \cap \mathbf{Z} = N\mathbf{Z},$$

so $\beta = \beta'$ in $\mathbf{Z}/2N$. Thus, once we check that $\mathfrak{n}_\beta$ is a primitive divisor of N then this construction is injective and so by mere counting we get the bijectivity. It should be possible to prove the surjectivity directly, but it may be slightly unpleasant to do so (e.g., recall that our counting argument rests on the fact that D is a square modulo all $p|N$, a property which is slightly awkward to use directly).

Due to the description

$$\mathfrak{n}_\beta = \mathbf{Z} \cdot N \oplus \mathbf{Z} \cdot \frac{B + \sqrt{D}}{2}$$

with $B \in \mathbf{Z}$ a representative of $\beta \in \mathbf{Z}/2N$, as well as the fact that (via oddness of B)

$$\mathscr{O} = \mathbf{Z} \oplus \mathbf{Z} \cdot \frac{B + \sqrt{D}}{2},$$

we see that $\mathfrak{n}_\beta$ is not divisible by any rational integers > 1. Thus, we just need to check that $\mathfrak{n}_\beta \overline{\mathfrak{n}}_\beta = N\mathscr{O}$.

By cross-multiplying generators, we get

$$\mathfrak{n}_\beta \overline{\mathfrak{n}}_\beta = N \cdot (N, (B + \sqrt{D})/2, (B - \sqrt{D})/2, (B^2 - D)/4).$$

Since the last term is a multiple of N, it can be dropped. Thus, we are reduced to showing

$$I \stackrel{\text{def}}{=} (N, (B + \sqrt{D})/2, (B - \sqrt{D})/2) = 1.$$

This ideal certainly contains N, so it divides $N\mathscr{O}$. Thus, if this ideal is not the unit ideal then it is divisble by some prime factor $\mathfrak{p}$ of $N\mathscr{O}$. But this ideal is visibly $\mathrm{Gal}(K/\mathbf{Q})$-invariant, so it is then also divisible by $\overline{\mathfrak{p}}$. But the prime factors of $N\mathscr{O}$ are split over $\mathbf{Z}$, so we conclude that I would be divisible by a rational prime p. But I contains elements such as $(B \pm \sqrt{D})/2$ which are part of a $\mathbf{Z}$-basis of $\mathscr{O}$, so I cannot be divisible by a rational prime p.

∎

With the descriptions of the $\mathfrak{n}$'s settled, we now turn to a description of Heegner points. That is, we choose $\tau \in \mathfrak{h}$ and we seek to give necessary and sufficient conditions on τ in order that $y_\tau = (\mathbf{C}/[1, \tau], \langle 1/N \rangle) \in Y_0(N)$ be a Heegner point for K (with CM by $\mathscr{O}$), and in such terms we will explicitly compute both an $\mathfrak{a}$ and $\mathfrak{n}$ such that $y_\tau = ([\mathfrak{a}], \mathfrak{n})$.

Certainly $\tau \in K$ with τ not in $\mathbf{Q}$, so τ satisfies a unique quadratic polynomial

$$A\tau^2 - B\tau + C = 0$$

where $A, B, C \in \mathbf{Z}$, $A > 0$, and $\gcd(A, B, C) = 1$. The relative primality condition will be crucial in the proof that is to follow (e.g., it is certainly necessary if one wants $B^2 - 4AC = D$, since D is squarefree). By the quadratic formula, the positivity of A, and the fact that $\tau, \sqrt{D} \in \mathfrak{h}$, we deduce that

$$\tau = \frac{B + \sqrt{D'}}{2A},$$

where $D' = B^2 - 4AC$ is the discriminant of our poynomial. We put the sign in the linear term of the quadratic polynomial to avoid a sign in the description of τ. This will be convenient later (and fixes a mistake in Gross-Zagier, as we shall explain).

We will eventually show $D' = D$ is the fundamental discriminant of K, but for now all we know is that $D' = Dm^2$ for some positive integer m. In particular, we do not yet know if D' is even or odd.

In order to determine when

$$\mathfrak{a} = [\tau, 1]$$

is a fractional $\mathscr{O}$-ideal, we will generally compute the ring of endomorphisms of this lattice (arising from homotheties by $\lambda \in \mathbf{C}^\times$) and then we'll see that the condition this ring equal $\mathscr{O}$ requires exactly $D' = D$. We will then go on to determine further conditions on A, B, C which make $\mathbf{C}/[1/N, \tau]$ also have CM by $\mathscr{O}$.

Let $\mathscr{O}_\tau$ denote the ring consisting of elements $\lambda \in \mathbf{C}$ for which multiplication by λ maps the lattice $[1, \tau]$ back into itself (i.e., $\mathscr{O}_\tau$ is the endomorphism ring of the elliptic curve $\mathbf{C}/[1, \tau]$).

Lemma 2.2. *With notation as above, the ring $\mathscr{O}_\tau$ is equal to*

$$\mathbf{Z}[(D' + \sqrt{D'})/2] = \mathbf{Z} \cdot 1 + \mathbf{Z} \cdot \frac{D' + \sqrt{D'}}{2} \cdot = \mathbf{Z} \cdot 1 + \mathbf{Z} \cdot \frac{\pm B + \sqrt{D'}}{2}$$

Note that $D' = B^2 - 4AC \equiv B^2 \equiv B \bmod 2$, so D' and B are either both even or both odd. In particular, the equality of the two lattices is clear, and general nonsense shows that the indicated ring is equal to the lattice on the basis 1 and $(D' + \sqrt{D'})/2$.

Proof. We check inclusion in both directions. Let L denote the common lattice which we want to show is equal to $\mathscr{O}_\tau$. Since

$$\frac{B + \sqrt{D'}}{2} = A\tau - B \in L, \quad \frac{-B + \sqrt{D'}}{2} \cdot \tau = -C \in L,$$

is it clear that $L \subseteq \mathscr{O}_\tau$.

To get the reverse inclusion, we will need to use the condition that A, B, C have no common factor > 1. Let $L' = [\overline{\tau}, 1]$. We compute

$$L \cdot L' = \left[\frac{B^2 - D'}{4A^2}, \frac{B + \sqrt{D'}}{2A}, \frac{B - \sqrt{D'}}{2A}, 1 \right] = \frac{1}{A}[C, B, A, (-B + \sqrt{D'})/2],$$

and this is exactly $(1/A)[1, (-B + \sqrt{D'})/2] = (1/A)\mathscr{O}_\tau$ since $\gcd(A, B, C) = 1$.

Thus, if $\lambda \in \mathbf{C}$ is such that $\lambda \cdot L \subseteq L$, then

$$\lambda \cdot L \cdot L' \subseteq L \cdot L',$$

which is to say that multiplication by λ takes $(1/A)\mathscr{O}_\tau$ back into $(1/A)\mathscr{O}_\tau$. In other words, $\lambda\mathscr{O}_\tau \subseteq \mathscr{O}_\tau$. This forces $\lambda \in \mathscr{O}_\tau$.

■

We deduce from this lemma that *by the hypothesis* $\mathscr{O}_\tau = \mathscr{O}_K$, necessarily the sublattice $\mathbf{Z} \cdot 1 + \mathbf{Z} \cdot \frac{D' + \sqrt{D'}}{2} \subseteq \mathbf{Z}[(1 + \sqrt{D})/2] = \mathscr{O}$ coincides with the entire ring $\mathscr{O}$. This forces $D' = D$, so $B \equiv D' \equiv 1 \bmod 2$, which is to say that B is odd. We therefore have

$$\tau = \frac{B + \sqrt{D}}{2A}$$

with some odd B.

So far we have argued with lattices of the form $[\tau,1]$ where we only assumed $\mathbf{C}/[1,\tau]$ has CM by the full ring of integers $\mathscr{O}$ in $K=\mathbf{Q}(\sqrt{D})$, and from this we deduced that if

$$A\tau^2-B\tau+C=0$$

with $A,B,C\in\mathbf{Z}$, $A>0$, and $\gcd(A,B,C)=1$, then $B^2-4AC=D$, $\tau=(B+\sqrt{D})/2A$, and

$$[\tau,1]\cdot[\overline{\tau},1]=\frac{1}{A}\mathscr{O}.$$

Now we apply these arguments to classify Heegner points in the upper half-plane. The following is a corrected version of Gross-Zagier, p. 236 (the mistakes are noted in the remark following the theorem).

Theorem 2.3. *Choose an element $\alpha\in\mathrm{Cl}_K$ in the class group of K and a primitive divisor $\mathfrak{n}$ of N. Let $\beta\in\mathbf{Z}/2N$ be the β-invariant of $\mathfrak{n}$. Choose a representative $\mathfrak{a}$ of α with $\mathfrak{a}\mathfrak{n}^{-1}$ an integral ideal prime to $\overline{\mathfrak{n}}$ and not divisible by any rational integer >1; this can be done thanks to Cebotarev. In particular, $\mathfrak{a}=(\mathfrak{a}\mathfrak{n}^{-1})\mathfrak{n}$ is an integral ideal divisible by $\mathfrak{n}$ but not divisible by any rational integer, and also $A=\mathrm{Norm}_{\mathbf{Q}}^{K}\mathfrak{a}\in N\mathbf{Z}^{+}$.*

We then have

$$\mathfrak{a}=\mathbf{Z}\cdot A+\mathbf{Z}\cdot\frac{B+\sqrt{D}}{2}$$

for some $B\equiv\beta \bmod 2N$ and

$$\mathfrak{a}\mathfrak{n}^{-1}=\mathbf{Z}\cdot(A/N)+\mathbf{Z}\cdot\frac{B+\sqrt{D}}{2}.$$

The point $\tau=(B+\sqrt{D})/2A\in\mathfrak{h}$ gives rise to the Heegener point $(\mathbf{C}/\mathfrak{a}\to\mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1})$ and satisfies $A\tau^2-B\tau+C=0$, where $B^2-4AC=D$ (so $\gcd(A,B,C)=1$).

Conversely, if $\tau\in\mathfrak{h}$ satisfies an equation of the form $A\tau^2-B\tau+C=0$ with integers A,B,C satisfying

- *$A\in N\mathbf{Z}^{+}$,*
- *$B^2-4AC=D$ (so $B^2\equiv D \bmod 4N$)*

then $\tau=(B+\sqrt{D})/2A$, $\mathfrak{a}=\mathbf{Z}\cdot A+\mathbf{Z}\cdot\frac{-B+\sqrt{D}}{2}$ is an integral $\mathscr{O}$-ideal with norm A, and $\mathfrak{a}\mathfrak{n}_{\beta}^{-1}$ is an integral $\mathscr{O}$-ideal not divisible by any rational integer >1 and relatively prime to $\overline{\mathfrak{n}}_{\beta}^{-1}$, with $\beta=B \bmod 2N$. Moreover, the point $(\mathbf{C}/[1,\tau],\langle 1/N\rangle)\in Y_0(N)$ is the Heegner point $([\mathfrak{a}],\mathfrak{n}_{\beta})$.

Remark 2.4. Recall that if B' is a representative of $\beta\in\mathbf{Z}/2N$, then $\mathfrak{n}_{\beta}=\mathbf{Z}\cdot N+\mathbf{Z}\cdot(B'+\sqrt{D})/2$. Also observe that the equation $B^2-4AC=D$ and the square-free property of D automatically force $\gcd(A,B,C)=1$.

Gross-Zagier forgot to mention the additional constraints that $\mathfrak{a}\mathfrak{n}^{-1}$ and $\mathfrak{a}$ not be divisible by any rational integer >1 (which is obviously necessary to get the asserted formulas). They also lost the minus sign when describing the linear coefficient of the polynomial for τ (alternatively one could negate the roles of B and β in the descriptions of various ideals, but since it presumably simplifies matters to have $B\equiv\beta \bmod 2N$ rather than $B\equiv-\beta \bmod 2N$, it seems we'd get a lot more sign interference if we had chosen a different "fix").

Proof. For any non-zero integral ideal I of $\mathscr{O}$, the intersection $I\cap\mathbf{Z}$ is a non-zero ideal, say of the form $n_I\mathbf{Z}$ for a unique positive integer n_I, so $n_I\mathbf{Z}$ is a direct summand of I as a $\mathbf{Z}$-module (as $I/n_I\mathbf{Z}$ is torsion-free). Thus, $(1/n_I)I$ has 1 as part of a $\mathbf{Z}$-basis.

Applying this to $\mathfrak{a}\mathfrak{n}^{-1}$, we get a positive integer c such that $(1/c)\mathfrak{a}\mathfrak{n}^{-1}$ contains 1 as part of a $\mathbf{Z}$-basis. By the discussion preceding the theorem, we can write

$$\frac{1}{c}\mathfrak{a}\mathfrak{n}^{-1}=[1,\tau]$$

where $\tau=(B'+\sqrt{D})/2A'$ with $B'^2-4A'C'=D$ for some $A',B',C'\in\mathbf{Z}$ with $A'>0$. In particular, B' is odd. Clearly now we get

$$\frac{A'}{c}\mathfrak{a}\mathfrak{n}^{-1}=\mathbf{Z}\cdot A'+\mathbf{Z}\cdot\frac{B'+\sqrt{D}}{2}.$$

Since the right side is visibly not divisible by any rational integers >1 and $\mathfrak{a}\mathfrak{n}^{-1}$ is integral, the reduced form fraction of A'/c cannot have non-trivial factors in the numerator. But likewise by the assumption (!) that

$\mathfrak{a}\mathfrak{n}^{-1}$ is not divisible by any rational integer > 1, we deduce that the reduced form fraction of c/A' cannot have non-trivial fractions in the numerator. Thus, $A'/c = \pm 1$. Since $A', c > 0$, we get $c = A'$ and

$$\mathfrak{a}\mathfrak{n}^{-1} = \mathbf{Z} \cdot A' + \mathbf{Z} \cdot \frac{B' + \sqrt{D}}{2}.$$

But the right side visibly has index A' in $\mathscr{O}$ (as B' is odd, so $\mathscr{O} = \mathbf{Z} + \mathbf{Z} \cdot (B' + \sqrt{D})/2$), so we conclude $A' = A/N$.

Since $\mathfrak{a}$ is also an integral ideal not divisible by any rational integer > 1, the same method gives

$$\mathfrak{a} = \mathbf{Z} \cdot A + \mathbf{Z} \cdot \frac{B + \sqrt{D}}{2}$$

where $B^2 - 4AC = D$, $A > 0$, $C \in \mathbf{Z}$, so $\mathfrak{a} = A[1, \tau]$ where $\tau = (B + \sqrt{D})/2 \in \mathfrak{h}$ satisfies $A\tau^2 - B\tau + C = 0$.

We will now show that $B \equiv \beta \bmod 2N$, where we recall that $\mathfrak{n} = \mathfrak{n}_\beta$ with a chosen $\beta \in \mathbf{Z}/2N$. To do this we observe that

$$\mathbf{Z} \cdot N + \mathbf{Z} \cdot \frac{\widetilde{\beta} + \sqrt{D}}{2} = \mathfrak{n} = (A/N)^{-1}\mathfrak{a} \cdot \overline{\mathfrak{a}\mathfrak{n}^{-1}},$$

where $\widetilde{\beta}$ is any desired lift of β. Thus, it suffices to "compute" the right side and to express it in the form $I + \mathbf{Z} \cdot (B + \sqrt{D})/2$ with an ideal I of $\mathbf{Z}$ (i.e., this will force $B \equiv \beta \bmod 2N$, as desired). We have

$$\begin{aligned}
(A/N)^{-1}\mathfrak{a} \cdot \overline{\mathfrak{a}\mathfrak{n}^{-1}} &= (A/N)^{-1}\left(A, \frac{B + \sqrt{D}}{2}\right)\left(A/N, \frac{B' - \sqrt{D}}{2}\right) \\
&= \left(A, N \cdot \frac{B' - \sqrt{D}}{2}, \frac{B + \sqrt{D}}{2}, (A/N)^{-1}\left(\frac{B' - B}{2} \cdot \frac{B + \sqrt{D}}{2} + \frac{B^2 - D}{4}\right)\right) \\
&= \left(A, N(B' + B)/2 - N\frac{B + \sqrt{D}}{2}, \frac{B + \sqrt{D}}{2}, \frac{B' - B}{2A/N} \cdot \frac{B + \sqrt{D}}{2} + NAC\right) \\
&= \left(A, N(B' + B)/2, \frac{B + \sqrt{D}}{2}, \frac{B' - B}{2A/N} \cdot \frac{B + \sqrt{D}}{2}\right)
\end{aligned}$$

However, this equals $\mathfrak{n}_\beta$ and so in particular must lie inside of $\mathbf{Z} + \mathbf{Z}(B + \sqrt{D})/2$.

We conclude that $B' \equiv B \bmod 2A/N$ and $A = N(A/N), N(B' + B)/2 \in \mathbf{Z}$ generate $N\mathbf{Z}$. That is, A/N and $(B' + B)/2$ are relatively prime. In any case, this ideal has to contain N (as $\mathfrak{n}_\beta$ always does) and we have explicitly exhibited $(B + \sqrt{D})/2$ as an element, so it follows that the above displayed ideal (which is $\mathfrak{n}_\beta$ in disguise) contains $\mathfrak{n}_{B \bmod 2N}$. A consideration of norms then shows that the inclusion

$$\mathfrak{n}_{B \bmod 2N} \subseteq \mathfrak{n}_\beta$$

must be an equality, so $B \bmod 2N = \beta$ as desired. Note also that since we obtained $B' \equiv B \bmod 2A/N$ along the way, we have

$$\mathfrak{a}\mathfrak{n}^{-1} = \mathbf{Z} \cdot A/N + \mathbf{Z} \cdot \frac{B' + \sqrt{D}}{2} = \mathbf{Z} \cdot A/N + \mathbf{Z} \cdot \frac{B + \sqrt{D}}{2}.$$

This description of both $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{n}^{-1}$ in terms of A, B, C now enables us to see that for

$$\tau = \frac{B + \sqrt{D}}{2} \in \mathfrak{h},$$

we have the point $(\mathbf{C}/[1, \tau], \langle 1/N \rangle) \in Y_0(N)$ equal to our original Heegner point

$$(\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1}).$$

Indeed, if we consider this cylic N-isogeny and multiply on universal covers of both source and target by $1/A$ (i.e., we change the representative $\mathfrak{a}$ of our class group element) then we arrive at the (isomorphic!) cyclic N-isogeny

$$\mathbf{C}/[1, \tau] \to \mathbf{C}/[1/N, \tau]$$

which is exactly what is needed.

Now we turn to the converse implication. We pick $A, B, C \in \mathbf{Z}$ with $A \in N\mathbf{Z}^+$ and $B^2 - 4AC = D$. In particular, B is odd and $\beta = B \bmod 2N \in \mathbf{Z}/2N$ satisfies $\beta^2 = D$ in $\mathbf{Z}/2N$. We define

$$\mathfrak{a} = \mathbf{Z} \cdot A + \mathbf{Z} \cdot \frac{B + \sqrt{D}}{2}, \quad \mathfrak{n} = \mathbf{Z} \cdot N + \mathbf{Z} \cdot \frac{B + \sqrt{D}}{2},$$

both of which are trivially checked to be ideals since

$$\left(\frac{B + \sqrt{D}}{2}\right)^2 = \frac{D - B^2}{4} + B \cdot \frac{B + \sqrt{D}}{2} = -AC + B \cdot \frac{B + \sqrt{D}}{2}$$

and $A \in \mathbf{Z} \cdot N$. It is obvious that $\mathscr{O}/\mathfrak{a}$ has size A, so $\mathfrak{a}$ has norm A. By its definition, clearly $\mathfrak{a}$ is not divisible by any rational integers > 1. For the unique root $\tau = (B + \sqrt{D})/2A$ to $Ax^2 - Bx + C = 0$ in the upper half plane, we have $\mathfrak{a} = A[1, \tau]$. Since A is divisible by N, when we form the quotient $\mathbf{C}/[1/N, \tau] \simeq \mathbf{C}/[1, N\tau]$ we have that $N\tau = (B + \sqrt{D})/2(A/N)$ is a root of

$$(A/N)x^2 - Bx + NC = 0$$

with $B^2 - 4(A/N)(NC) = B^2 - 4AC = D$, so $\mathbf{C}/[1, N\tau]$ also has CM by $\mathscr{O}$ (thanks to the lemma which preceded this theorem). Hence, τ gives rise to a Heegner point $([\mathfrak{a}], \mathfrak{n}')$ for some primitive divisor $\mathfrak{n}'$ of N. It remains to show $\mathfrak{n}' = \mathfrak{n}$ as defined above.

Since $\mathfrak{a}\mathfrak{n}'^{-1} = A[1/N, \tau] = [A/N, A\tau]$, in order to prove $\mathfrak{n}' = \mathfrak{n}$ it suffices to show $\mathfrak{n}[A/N, A\tau] = \mathfrak{a}$. Since both sides are a priori (integral) fractional ideals with the same norm $N(A/N) = A$, we just have to check

$$\mathfrak{n}[A/N, A\tau] \subseteq \mathfrak{a}.$$

Since $\mathfrak{n}$ is generated over $\mathbf{Z}$ by N and $(B + \sqrt{D})/2$ while $A\tau = (B + \sqrt{D})/2$ and $\mathfrak{a}$ is generated over $\mathbf{Z}$ by A and $(B + \sqrt{D})/2$, we again just need to note the identity

$$\left(\frac{B + \sqrt{D}}{2}\right)^2 = -AC + B \cdot \frac{B + \sqrt{D}}{2}.$$

■