Notes and Errata

Max Fleischer
Yijia Liu

January 28, 2021

All notations below follow from [1], which we used to implement our code. Throughout the document, we assume that the modular unit used is $[N]-N[1]$, for any prime N. Note that for $N>3$, we can remove all occurrences of a factor of 12 in the algorithms.

1 Basis

We show that $\left\{[\infty]-\left[\frac{i}{N}\right], i=1,2,\ldots,N-1\right\}$ form a $\Gamma_0(N)$-basis.

Proof: We can show this by a descent argument. Given $[\infty]-[\frac{a}{Nc}]$ where we can assume that $c>0$ and $c\neq 1$, consider the integer $0<d'<Nc$ such that $ad'\equiv 1 \pmod{Nc}$. Let $d=d'-Nc, b=\frac{ad-1}{Nc}$ and $x=\max\{N-\lceil d/c\rceil, 1\}$. Then

$$[\infty]-\left[\frac{a}{Nc}\right]=[\infty]-\left[\frac{ax+Nb}{Ncx+Nd}\right]-\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}\left([\infty]-\left[\frac{x}{N}\right]\right).$$

We check that $|cx+d|<|c|$, and by repeating this process we can write $[\infty]-[\frac{a}{Nc}]$ in terms of the basis elements.

2 Errata in paper

There is a sign error in Equation (43) of [1] and the next equation. It should read $d\bar{\mu}_{\gamma m_i}(u)$.

3 Discussion of $\sum n_d \neq 0$

For $[N]-N[1]$ in our program, the assumption that $\sum n_d \neq 0$ is no longer valid.

3.1 Proposition 3.1

The following proposition remains valid:

$$\mathcal{F}_k(U)=\int_U x_p^{k-1} d\mathcal{F}_1(x).$$

Proof: The equivalence at Equation (18) and Equation (19) in [1] yields

$$\mathcal{F}_k(U) \equiv -\sum_{d|N} \left(n_d a^{k-1} \left[\frac{da}{ep^n} \right] + \frac{n_d}{2} a^{k-1} \right) \equiv \frac{N-1}{2} a^{k-1} + a^{k-1}\mathcal{F}(U) \pmod{p^{n-\epsilon}\mathbf{Z}_p}.$$

Thus for $U = a + ep^n Z$, we can write

$$\begin{aligned}\mathcal{F}_k(U) &= \lim_{m\to\infty} \sum_{t=0}^{p^m-1} \mathcal{F}_k(a + ep^n \cdot t + ep^{m+n} \cdot Z)^k \\ &= \lim_{m\to\infty} \sum_{t=0}^{p^m-1} \left(\frac{N-1}{2}(a + ep^n \cdot t)^{k-1} + a^{k-1}\mathcal{F}(a + ep^n \cdot t + ep^{m+n} \cdot Z) \right)\end{aligned}$$

(expanding $(a + ep^n \cdot t)^{k-1}$ gives for fixed c_i, $\sum_{t=0}^{p^m-1}(a + ep^n \cdot t)^{k-1} = \sum_{i=0}^{k-1} c_i \sum_{t=0}^{p^m-1} t^i \to 0$ as $m \to \infty$)

$$= \int_U x_p^{k-1} d\mathcal{F}_1(x).$$

3.2 Proposition 3.2

Following Proposition 3.1, we can deduce that the formulas for Proposition 3.2 are still correct when $\sum n_d \neq 0$.

3.3 Modification to ord_p formula

From Equation (4.1) of [2], we add $\frac{N-1}{4}$ to the formula at Step 1 of Algorithm 4.3 in [1].

4 Binary Quadratic Forms Representatives

We can calculate the representatives based on [3], such that Equation (12) of [1] is satisfied.

5 Speeding up the computations in Algorithm 4.3

The formula for Step 1 and Step 2 run in $O(c)$ time, which can be large. We can make use of the basis representation of $[\infty] - [\frac{a}{Nc}]$ to significantly speed up these steps.

- Step 1: While using the basis representation to compute ord_p, we must take note of sign changes. i.e. $[\infty] - [\frac{-x}{Ny}]$ gives a different ord_p as compared to $[\infty] - [\frac{x}{-Ny}]$. This is due to the introduction of an error term (see Section 3.3).
- Step 2: We can proceed in the same fashion as Step 3.

See the comments in the code at [4] for more details of the implementation.

References

[1] Samit Dasgupta, Computations of Elliptic Units for Real Quadratic Fields, *Canadian Journal of Mathematics.* 59 (3):553-74, 2007.

[2] Don Zagier, A Kronecker limit formula for real quadratic fields, *Mathematische Annalen.* 213 (2):153-184, 1975.

[3] Henri Darmon, *Heegner points, Heegner cycles, and congruences*, Elliptic curves and related topics, Vol. 4, 2007.

[4] https://github.com/liuyj8526/Computation-of-Elliptic-Units.