Class pairings and elliptic curves

Ideal class pairings map the rational points an elliptic curve $E/\mathbb{Q}$ to the ideal class groups $\mathrm{CL}(-D)$ of certain imaginary quadratic fields, by means of explicit maps to $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integral binary quadratic forms. Such pairings have been studied by Buell, Call, Soleng and others.

In recent work with Ono and Tsai, we used such pairings to study the class group and give explicit lowers bounds on the class numbers. In the specific case $E:\ y^2 = x^3 - a$ is a curve of rank r, and the twist E_{-D} of the elliptic curve has a rational point with sufficiently small "y-height", we find that

$$h(-D) \geq \frac{1}{10} \cdot \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{\sqrt{R_{\mathbb{Q}}(E)}} \cdot \frac{\pi^{\frac{r}{2}}}{2^r \Gamma\left(\frac{r}{2}+1\right)} \cdot \frac{\log(D)^{\frac{r}{2}}}{\log\log D}.$$

Whenever the rank is at least 3, this represents an improvement to the classical lower bound of Goldfeld, Gross and Zagier.

Conversely, using the classical upper bound on the class number $\mathrm{CL}(-D)$ for some discriminant $-D$ represented by the equation of the elliptic curve, these pairing imply effective lower bounds for the canonical heights $\widehat{h}(P)$ of non-torsion points $P \in E(\mathbb{Q})$.

I will also discuss a recent impressive REU project wherein the authors prove instances where the torsion subgroup of an elliptic curve injects into the the class group $\mathrm{CL}(-D)$. Using this result, they are able to demonstrate several infinite families of class groups with subgroups isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}^2$, or whose orders are divisible by the primes $3, 5$, or 7.