Experiments with Canonical Height on Elliptic Curves

Many breakthroughs in pure mathematics, and therefore in science and technology have emerged from the study of elliptic curves. Elliptic curves with rational points (points whose coordinates are rational), form the foundation of fields like Elliptic Curve Cryptography. This cryptography helps with keeping our passwords and bank details safe while enabling us to make secure online transactions. Elliptic curves also played a key role in Andrew Wiles' famous proof of Fermat's Last Theorem. However, this is not the endpoint of their potential; elliptic curves can advance beyond our current imagination.

Just as humans have measurable characteristics like height and weight, elliptic curves have properties such as rank and discriminant. While the discriminant is easy to compute, the rank remains mysterious for mathematicians. Despite many conjectures, no universal formula has ever been found to calculate the rank for all elliptic curves. The rational points on an elliptic curve have a characteristic called the "canonical height". Calculating this height by hand is challenging when it is non-zero; as if, in the world of elliptic curves, points are reluctant to reveal a non-zero canonical height.

In the study of elliptic curves, we are particularly interested in the points with a non-zero canonical height. These points have a deep relationship with rank. In other words, the canonical height is a characteristic that helps us restrict our focus to rational points that are related to the rank. These relationships help us understand the importance of Lang's height conjecture, the primary direction of this project.

The characteristics of focus for this conjecture were the discriminant and the canonical height. This resulted in analysing large data sets and hence using Microsoft Excel and coding languages for this purpose. A sudden encounter revealed an interesting but known pattern between two elliptic curves and this turned the focus of the project into searching for patterns in different families of elliptic curves. These searches led to finding a family in which the rank could be determined using the equation of the elliptic curve. It later turned out that a similar pattern was already found in a similar family. This suggests the idea of grouping these families together and I am exploring this further.

Out of all the gifts from this project, an invaluable was the insight into how experiments and theory can contribute to one another. This serves as a reminder of how central searching for patterns is in the study of elliptic curves and generally in mathematics. An encounter can sometimes open the gate to discovering patterns and even shift our perspective to a new direction.