WRITTEN HOMEWORK #5: HINTS FOR 3.2B

Exercise 3.2(b) is now optional and you can turn it in for extra credit at the end of the term. (A list of extra credit questions will be posted shortly, and we will add to it over the next two weeks.)

We want to show that

$$h(P-Q)+h(P+Q) \leqslant 2h(P)+2h(Q)+\kappa$$

for some constant κ which depends on E, but not $P, Q \in E(\mathbb{Q})$.

Recall that $P=(x_1,y_1), Q=(x_2,y_2), P+Q=(x_3,y_3), P-Q=(x_4,y_4)$. In part (a) you obtained expressions for x_3+x_4, x_3x_4, in terms of x_1, x_2. As a matter of fact, you can show (you should provide details in your solution) that these expressions are ratios of quadratics in x_1+x_2, x_1x_2. For example, you might have found that the denominators of these expressions is equal to $(x_2-x_1)^2$. We can rewrite this as $(x_1+x_2)^2-4x_1x_2$, which evidently is a quadratic expression in x_1+x_2, x_1x_2. The computations for the numerators are much more complicated.

At this point, it helps to define the height of points in projective space. Let $[r_0, r_1, \ldots, r_n] \in \mathbb{P}^n(\mathbb{Q})$ be a point in projective n-space with all rational coefficients. By multiplying this by the least common denominators of the r_i, we can write

$$[r_0, r_1, \ldots, r_n] = [x_0, \ldots, x_n]$$

where $x_i \in \mathbb{Z}$ and the x_i share no common denominator. Then define the height of $[r_0, r_1, \ldots, r_n]$ by

$$H([r_0, r_1, \ldots, r_n]) = \max_{0 \leqslant i \leqslant n}(|x_i|).$$

Notice that this definition is compatible with our definition of height for rational numbers, where $H(m/n) = H[m,n]$. We will be interested in the cases where $n=1,2$. For example, $H([4,12,6]) = 6$, since $[4,12,6] = [2,6,3]$, and 6 is the largest of these three coprime numbers.

The key to solving this problem is to prove the following:

Let r_1, r_2 be two rational numbers. Then

$$H(r_1)H(r_2) \ll H([1, r_1+r_2, r_1r_2]) \ll H(r_1)H(r_2). \tag{1}$$

As a matter of fact, we can make the constants explicit; you want to prove

$$\frac{1}{4}H(r_1)H(r_2) \leqslant H([1, r_1+r_2, r_1r_2]) \leqslant 4H(r_1)H(r_2).$$

This is useful because we can say

$$H(x_3)H(x_4) \ll H([1, x_3+x_4, x_3x_4]).$$

We can convert this to a statement about $H[1, x_1+x_2, x_1x_2]$, because we have expressions for x_3+x_4, x_3x_4, which are ratios of quadratics in x_1+x_2, x_1x_2. One can show (you would need to provide details) that

$$H([1, x_3+x_4, x_3x_4]) \ll H([1, x_1+x_2, x_1x_2])^2.$$

You then use the upper bound on Inequality (1) to convert this into an expression involving $H(x_1), H(x_2)$.

Actually proving Inequality (1) is somewhat difficult. The upper bound is relatively easy, but the lower bound involves some calculation and clever insights.

All this and much more general statements are proven in Chapter VII.5 and VII.6 of Silverman's *The Arithmetic of Elliptic Curves*, but is discussed using substantially more sophisticated terminology and techniques than what we've used so far.