# HAWK IN HASKELL: IMPLEMENTATION JOURNAL

DANIEL BARRERO

## 1. January 14 – ?

I was about to learn (in bird's eye view) the working of the `verify` subroutine. However, I started reviewing the norms and inner products.

**Question.** Are inner products closed under scalar multiplication? Yes, if and only if the scalar is positive.

## 2. NTRUSolve

The NTRU equation is

$$fG - gF = q \mod X^n + 1$$

where $f$ and $g$ are given, and the idea is to solve for $F$ and $G$. All the polynomials in the equation are in $\mathbb{Z}[X]/\langle X^n + 1\rangle$