

Homework 36, due December 8

- (1) (Page 390, problem 3) Let $v_1, \dots, v_n$ be linearly independent row vectors in $\mathbb{R}^n$. Form the matrix M whose rows are the vectors v_i . Let $\mathbf{a} = (a_1, \dots, a_n)$ be a row vector with integer entries. Show that $\mathbf{a}M$ is a vector in the lattice generated by $v_1, \dots, v_n$, and show that every vector in the lattice can be written in this way.
- (2) (Page 390, problem 4) Let $\{v_1, v_2\}$ be a basis of a lattice. Let a, b, c, d be integers with $ad - bc = \pm 1$, and let

$$w_1 = av_1 + bv_2, \quad w_2 = cv_1 + dv_2.$$

- (a) Show that

$$v_1 = \pm(dw_1 - bw_2), \quad v_2 = \pm(-cw_1 + aw_2).$$

- (b) Show that $\{w_1, w_2\}$ is also a basis of the lattice.

- (3) (Page 391, problem 7)

- (a) In the NTRU cryptosystem, suppose we ignore q and let

$$c = 3hr + m \pmod{x^N - 1}.$$

Show how the attacker can obtain the message quickly.

- (b) In the NTRU cryptosystem, suppose q is a multiple of 3. Show how an attacker can obtain the message quickly.