Exercise 1. Let $b_1, \ldots, b_n$ be an LLL-reduced basis of a lattice $\Lambda$ for parameter $\delta \in (1/4, 1)$. Set $\alpha := (\delta - 1/4)^{-1}$. Show the following:

(a) $||b_i||^2 \leq \alpha^{i-1} ||b_i^*||^2$ for all $i$.
(b) $||b_j|| \leq \alpha^{(i-1)/2} ||b_i^*||$ for all $j \leq i$.
(c) $||b_i|| \leq \alpha((n-1)/2) \lambda_i(\Lambda)$ for all $i$.
(d) $||b_1|| \leq \alpha^{(n-1)/4} d(\Lambda)^{1/n}$.

Exercise 2. Compute an LLL reduced basis with $\delta = 3/4$ for the lattice defined by the rows of

$$
\begin{pmatrix}
1 & 1 & 1 \\
-1 & 0 & 2 \\
3 & 5 & 6
\end{pmatrix}
$$

Exercise 3. Show that $p = 10^{400} + 69$ is a pythagorean prime number and find $a, b \in \mathbb{N}$ with $p = a^2 + b^2$. (Hint: This can be translated into a lattice problem in $\mathbb{R}^2$. Exercise 1d will be helpful.)

Exercise 4. Let $L$ be a field and let $\mu \subseteq L^*$ be a finite subgroup of the multiplicative group of $L$. Show that $\mu$ is cyclic.

---

1 Part of this is showing that $1 + \frac{1}{4} \alpha^2 \leq \alpha^{-1}$.

2 Prove (and use) the following: let $w_1, \ldots, w_i \in \Lambda$ be linearly independent. Write $w_j = \sum_k a_{j,k} b_k$. For each $j$ let $k(j)$ be the largest index $k$ such that $a_{j,k} \neq 0$. Then $||w_j|| \geq ||b_{k(j)}^*||$. 