

The first two problems could have been assigned on Day 12, but you already had a lot of programming work assigned, so here they are on Day 13.

A. The Bernstein-Vazirani problem is not a special case of the Simon problem, and the Simon problem is not a special case of the Bernstein-Vazirani problem. But what is the intersection of these two problems? In other words, what is the largest problem that can be viewed as a special case of both? Be thorough, precise, and specific. For example, Bernstein-Vazirani has 2^n possible answers, and Simon has $2^n - 1$ possible answers. How many possible answers does the intersection problem have?

B. In the Simon problem, why is it impossible to find more than $n - 1$ independent γ s? If we did manage to find n independent γ s, then what would that imply?

C. Find the periods of all elements in $(\mathbb{Z}/11\mathbb{Z})^*$.

D. In $(\mathbb{Z}/16\mathbb{Z})^*$, what is $\log_5 13$ and what is $\log_5 11$?