Problem Tutorial: "Exercise"

Let's take a random prime p around $\sqrt{n}$.

For each pair of $(x_1 \mod p, y_1 \mod p, x_2 \mod p)$ with $y_1 \mod p > 0$ let's find $y_2 \mod p$ with needed value of $(x_1 \cdot y_1 + x_2 \cdot y_2) \mod p$, let's save it in f_{x_1,y_1,x_2}

After that, for fixed i with $y_i \mod p > 0$ let's fix $x_j \mod p$, and check all points with such x modulo and $y_j \mod p = f_{x_i,y_j,x_j}$.

For points with $y_i \mod p$ check all points with $(x_j \cdot x_i) \mod p = k \mod p$.

Why is it working fast? Let's look at fixed pair $x_i \cdot x_j + y_i \cdot y_j \neq k$, but correct value of it $\mod p$. There are $O(1)$ $p's$ for which it will be that because if it is equal $\mod p$ for lots of big modules, it will mean that it is equal to k. So, the probability that a fixed pair will give correct value for random modulo is something like $(\frac{1}{\sqrt{n}/logn})$. Which implies that the expected number of pairs is $n^2 \cdot (\sqrt{n} \log n) = n \cdot \sqrt{n} \log$.

So for not random points, we can solve this problem in $n \cdot \sqrt{n} \log$.

But points are random, so $(x_i \cdot x_j + y_i \cdot y_j) \mod p$ is random which means that there are around $n \cdot \sqrt{n}$ pairs of points with fixed $\mod$ value.

So we can solve the whole problem in $n \cdot \sqrt{n}$.