Problem 1. ***Week 3 - 4.)***

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$ and let p be a prime.

(a) If we reduce the coefficients of the equation of E modulo p, we get a curve $E : y^2 = x^3 + \overline{A}x + \overline{B}$ over $\mathbb{F}_p$. (The bar denotes reduction modulo p.) Is E necessarily an elliptic curve over $\mathbb{F}_p$? That is, is the discriminant of E nonzero in $\mathbb{F}_p$? (Hint: the answer is no; justify why.)

(b) The curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{Q}$ is said to have good reduction at p if the reduced curve E is an elliptic curve over $\mathbb{F}_p$. And E has a bad reduction at p if not. Prove that every elliptic curve over $\mathbb{Q}$ has finitely many primes of bad reduction.

Solution.

(a) For $E/\mathbb{Q}$ to be an elliptic curve, it must be the case that its discriminant is $\Delta_{\mathbb{Q}} \neq 0$. The same applies for an elliptic curve over $\mathbb{F}_p$, so we should check if $\Delta_{\mathbb{Q}} \neq 0 \implies \Delta_{\mathbb{F}_p} \neq 0$.

Let's take an example of $p = 3$.
We know that $\Delta_{\mathbb{Q}} = 4A^3 + 27B^2$ and that $\Delta_{\mathbb{F}_p} = 4\overline{A}^3 + 27\overline{B}^2$.
If we consider $A = 3$ and any $B \in \mathbb{Q}$, we can see that $\Delta_{\mathbb{Q}} = 4 * 27 + 27B^2 > 0$.
However, for our $p = 3$ and $A = 3$, we have that $\Delta_{\mathbb{F}_p} = 4 * 27 + 27B^2 = 0 \mod 3$.
This counter-example is enough to disprove the proposed implication that we wanted to check.

(b) Let $E : y^2 = x^3 + Ax + B$ over $\mathbb{Q}$ be some elliptic curve. As we know, $\Delta_{\mathbb{Q}} = 4A^3 + 27B^2$ is discriminant of the elliptic curve E and it is true that $\Delta_{\mathbb{Q}} \neq 0$. Let's consider prime p, such that $p \mid \Delta_{\mathbb{Q}}$. We can see that for a reduced curve E over $\mathbb{F}_p$, it holds that
$\Delta_{\mathbb{F}_p} \equiv 0 \mod p \iff p \mid \Delta_{\mathbb{Q}}$. As such, E has a bad reduction at p.

As the set of numbers that divide $\Delta_{\mathbb{Q}}$ is finite, every elliptic curve E has finitely many bad reductions.
□

Problem 2. ***Week 4 - 2.)***

There is no obvious analogue for the index calculus approach for the DLP in $E(\mathbb{F}_p)$. Why not? What step fails when you try to generalize it for $E(\mathbb{F}_p)$?

Solution.
In the index calculus algorithm, the critical part is choosing a factor base, a set of *prime* numbers, which are used in later stages while creating a system of equations (modulo p).

The mere notion of *prime* number is not defined over a $E(\mathbb{F}_p)$, so such an analogue is impossible to trivially generalize. $\square$