EXERCISE SHEET 2

————*Day 3*————

Exercise 2-1.(a) Show that a smooth curve of genus 0 or 1 over a finite field $\mathbb{F}$ always has an $\mathbb{F}$-rational point.

(b) What about curves of genus 2? Find q_0 such that over fields $\mathbb{F}_q$ of cardinality $q \geq q_0$, curves of genus 2 always have points.

Exercise 2-2.(a) Count the number of smooth plane conics over $\mathbb{F}_p$ directly (instead of subtracting the number of reducible conics from the total number). You should not need to treat $p = 2$ separately. *Hint: count triangles.*

(b) Count the number of (absolutely) reducible plane conics over $\mathbb{F}_p$ of each type (split lines, conjugate lines, double line) subject to each of the side conditions "point" (exclude those which contain one fixed point) and "line" (exclude those whose intersections with one fixed line are not $\mathbb{F}_p$-rational).

Exercise 2-3. Let $N = |\mathrm{PGL}(3, \mathbb{F}_p)|$. Show that the number of irreducible plane cubics over $\mathbb{F}_p$ with a node is Nm and the number with a cusp is $N/(p-1)$.
Hint: WLOG the node/cusp is at $(0,0,1)$. Homogenise to get an affine equation of the form $C_3(X,Y) + C_2(X,Y) = 0$ where the C_j are coprime forms of degree j.

Exercise 2-4. Let p be any prime, fix $j \in \mathbb{F}_p$ and consider the set $\mathcal{E}(j)$ of $\mathbb{F}_p$-isomorphism classes of elliptic curves $E/\mathbb{F}_p$ with j-invariant $j(E) = j$. We aim to show that

$$\sum_{E \in \mathcal{E}(j)} (\#\operatorname{Aut} E)^{-1} = 1,$$

where $\mathrm{Aut}(E)$ is the group of automorphisms of E defined over $\mathbb{F}_p$.

(i) For $j \neq 0, 1728$ show that $\#\mathcal{E}(j) = \#\operatorname{Aut}(E) = 2$ for all $E \in \mathcal{E}(j)$.

(ii) Let $j = 1728$ and suppose $p \neq 2, 3$. Show that $\#\mathcal{E}(j) = \#\operatorname{Aut}(E) = \#(\mathbb{F}_p^*/(\mathbb{F}_p^*)^4) \in \{2, 4\}$ (depending on $p \pmod 4$) for all $E \in \mathcal{E}(j)$.

(iii) Let $j = 0$ and suppose $p \neq 2, 3$. Show that $\#\mathcal{E}(j) = \#\operatorname{Aut}(E) = \#(\mathbb{F}_p^*/(\mathbb{F}_p^*)^6) \in \{2, 6\}$ (depending on $p \pmod 6$) for all $E \in \mathcal{E}(j)$.

(iv) [Harder] If $p = 2$, $j = 1728 = 2$ then $\#\mathcal{E}(j) = 3$ and $\#\operatorname{Aut}(E) = 2, 4, 4$ for the three isomorphism classes.

(v) [Harder] If $p = 3$, $j = 1728 = 2$ then $\#\mathcal{E}(j) = 4$ and $\#\operatorname{Aut}(E) = 2, 6, 6, 6$ for the four isomorphism classes.
Hence deduce the result in each case.
The previous result is a special case of a more general phenomenon!

Exercise 2-5. Consider long Weierstrass equations

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

(a) The number of these with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_p$, including singular equations, is obviously p^5. Count how many define *singular* curves over $\mathbb{F}_p$ and hence how many are smooth.

(b) Hence find the probability that a random long Weierstrass equation with coefficients in $\mathbb{Z}_p$ has good reduction at p, in the sense that its discriminant is in $\mathbb{Z}_p^*$.
Is this the same as the probability that a random long Weierstrass equation over $\mathbb{Z}_p$ defines an elliptic curve over $\mathbb{Q}_p$ which has good reduction at p?

(c) Find the probability that a random long Weierstrass equation over $\mathbb{Z}_p$ has (i) split multiplicative, (ii) non-split multiplicative, (iii) additive reduction at p. Exercise 7 may help.
If you must, assume $p \geq 5$ and use short Weierstrass equations $Y^2 = X^3 + aX + b$, but done the right way this is not necessary.