EXERCISE SHEET 1

————Day 1————

Exercise 1-1. *Hensel lifting of smooth points on curves.*
Let $f(X,Y,Z) \in \mathbb{Z}[X,Y,Z]$ or $\mathbb{Z}_p[X,Y,Z]$ be homogeneous of degree $d \geq 1$ with coprime coefficients. Let $(x_0,y_0,z_0) \in \mathbb{Z}^3$ be coprime integers such that

(i) $f(x_0,y_0,z_0) \equiv 0 \pmod p$;

(ii) not all of $f_X(x_0,y_0,z_0) \equiv 0, f_Y(x_0,y_0,z_0) \equiv 0, f_Z(x_0,y_0,z_0) \equiv 0 \pmod p$.

Show that there exists $(x,y,z) \in \mathbb{Z}_p^3$ such that $f(x,y,z) = 0$ and $(x,y,z) \equiv (x_0,y_0,z_0) \pmod p$.

Exercise 1-2. *Real densities for quadratics*
Show that

(i) $vol(\{(a,b,c) \in [0,1]^3 \mid b^2 \leq 4ac\}) = (31 - 6\log 2)/36$.

(ii) $vol(\{(a,b,c) \in [0,1]^3 \mid b^2 \leq ac\}) = 4/9$.

Deduce that the (real) density of quadratics $f(X) = aX^2 + bX + c$ which have a real root is $(41 + 6\log 2)/72$ and the similar density for quadratics $f(X) = aX^2 + 2bX + c$ is $7/9$. (Use the uniform density distribution on $\mathbb{R}^3$ which is constant on $[-1,1]^3$ and zero outside.)

Exercise 1-3.(a) Show that the squares in $\mathbb{Z}_2$ have density $1/6$.

(b) Show that for random $(b,c) \in \mathbb{Z}_p^2$, the probability that $b^2 - 4c$ is a p-adic square is $p/(2(p+1))$ for *all* primes p (including $p = 2$!). Compare this to the probability of a random element of $\mathbb{Z}_p$ being a p-adic square.
Hint: for fixed b, when $p \neq 2$ the map $c \mapsto b^2 - 4c$ is a measure-preserving bijection $\mathbb{Z}_p \to \mathbb{Z}_p$. When $p = 2$, consider even and odd b separately.

Exercise 1-4. Find the density of cubes in $\mathbb{Z}_p$. (The answer depends on p mod 3.)

————Day 2————

Exercise 1-5. Let G be an abelian group of order n and let a, b be coprime integers. Show that the number of solutions to $x^a = y^b$ in G is exactly n.

Exercise 1-6.(a) Show that for all $k \geq 1$, the density of $\{(x,y) \in \mathbb{Z}_p^2 \mid x,y \in \mathbb{Z}_p^*$ and $x^3 \equiv y^2 \pmod{p^k}\}$, as a subset of $\mathbb{Z}_p^2$, is $p^{-k}(1 - 1/p)$.

(b) For $k = 0, 1$ find the density of the subset $\{(x,y) \in \mathbb{Z}_p^2 \mid v(x^3 - y^2) = k\}$ of $\mathbb{Z}_p^2$.
Hence find the probability that $x^3 - y^2$ is square-free (for random $x, y \in \mathbb{Z}_p$).

(c) For $p \geq 5$, deduce that a random cubic of the form $X^3 + aX + b \in \mathbb{Z}_p[X]$ has square-free discriminant with probability $1 - 2/p + 1/p^3$.

Exercise 1-7.(a) Count the number of monic quadratics $X^2 + bX + c \in \mathbb{F}_p[X]$ which factor as
(i) the square of a linear polynomial;
(ii) the product of two distinct linear polynomials over $\mathbb{F}_p$;
(iii) the product of two conjugate polynomials over $\mathbb{F}_{p^2}$.
Check that your counts add up to p^2.

(b) Repeat (a) for (nonzero) binary quadratic forms $aX^2 + bXY + cY^2 \in \mathbb{F}_p[X,Y]$, counting how many factor in each of the three possible ways (i), (ii), (iii) (up to a constant factor). Check that your counts add up to $p^3 - 1$.

(c) If you found (a) and (b) too easy, write down all possible ways a cubic in $\mathbb{F}_p[X]$ or a cubic form in $\mathbb{F}_p[X,Y]$ can factor, taking into account multiplicities and the field of definition of the factors. (There are five possibilities.) Count how many there are of each type and check that your counts add up to p^3 and $p^4 - 1$ respectively.

(d) If that was too easy (or if it was too hard), write a computer program to enumerate and count all possible factorizations of a polynomial or form of general degree d over a finite field.