Math 5020 - Elliptic Curves
Homework 1 (1.3, 1.6, 2.3, and 2.6, plus additional exercises)

Preliminary Exercises

1 *Let $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ be a polynomial with integer coefficients, and $a_n \neq 0$. Suppose that a rational number $x_0 = \frac{s}{t}$, with $s, t \in \mathbb{Z}$ and $t \neq 0$, is a root of f, that is $f(x_0) = 0$. Show that s divides a_0, and t divides a_n.*

2 *Let a, b, c be non-zero integers. Show that the line $L : ax + by = c$ has integral points if and only if $\gcd(a, b)$ is a divisor of c.*

3 (The Hundred Fowls Problem.) *One rooster is worth 5 qian, one hen 3 qian, and 3 chicks are worth 1 qian. If we bought 100 fowls with 100 qian, how many roosters, hens and chicks did we buy?*

4 *Find all the rational points on the conic $x^2 - 3xy + y^2 = 5$, given as a 1-parameter family.*

5 *A natural number n is said to be a triangular number if it n objects (dots) that can be arranged in an equilateral triangle configuration (such as 1, 3, 6, etc). Similarly, a number n is a square number if n objects can be arranged as a square (e.g., 1, 4, 9, etc.). Find the first 5 square-triangular numbers, that is, the first five numbers that are both triangular and square numbers. Can you find a way to characterize all the square-triangular numbers?*

6 (This problem involves elliptic curves, so you may want to come back to it later, after we learn some theory... or find an elementary solution!) *Find all sets of three consecutive integers such that their product is a square.*

7 (This problem requires a familiarity with the p-adics.) *Let p be a prime such that $p \equiv 2 \bmod 3$. Show that $3x^3 + 4y^3 + 5z^3 = 0$ has a non-trivial solution over $\mathbb{Q}_p$.*

Problems from Silverman's Book

1.3 *Let $V \subset \mathbb{A}^n$ be a variety given by a single equation. Prove that a point $P \in V$ is nonsingular if and only if $\dim_{\overline{K}} \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim V$, where $\mathfrak{m}_P$ is the maximal ideal of P in the affine ring of V.*

1.6 *Let V be the variety*

$$V : Y^2 Z = X^3 + Z^3.$$

The map $\phi : V \to \mathbb{P}^2$ defined by $\phi([X, Y, Z]) = [X^2, XY, Z^2]$ is a morphism.

2.3 (a) *Prove Proposition 2.6 for the special case of a non-constant map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$.*

(b) *Prove the Riemann-Roch theorem for $\mathbb{P}^1$.*

(c) *Prove Hurwitz' theorem (a.k.a. the Riemann–Hurwitz formula) for $\phi : \mathbb{P}^1 \to \mathbb{P}^1$.*

2.6 *Let C be a curve of genus 1. Fix a basepoint $\mathcal{O} \in C$.*

(a) *For all $P, Q \in C$, there exists a unique $R \in C$ such that $(P) + (Q) \sim (R) + (\mathcal{O})$. Denote this R by $\sigma(P, Q)$.*

(b) *The map $\sigma : C \times C \to C$ makes C into an abelian group with identity $\mathcal{O}$.*

(c) *Define a map $\kappa : C \to Pic^0(C)$ by sending P to the divisor class of $(P) - (\mathcal{O})$. Then κ is a bijection of sets, and hence κ can be used to make C into a group by $P + Q = \kappa^{-1}(\kappa(P) + \kappa(Q))$.*

(d) *The group operations defined in (b) and (c) are the same.*