## 2.1 Exercise Sheet 1

### 2.1.A Numerical and Exploration

**Exercise 2.1.1.** Let $b, c \in \mathbb{R}$. When does the equation $x^3 + bx + c = 0$ have exactly one (resp. two, resp. three) real root(s)? (Hint: Play around on Desmos. A little calculus might come in handy.)

**Exercise 2.1.2.**

(a) Let $R$ be a UFD with fraction field $K$. State and prove the analog of the Rational Root Theorem (1.1.2) with $\mathbb{Z}$ replaced by $R$, and conclude that there is an algorithmic procedure (given the ability to find all factors of an element of $R$[1]) for finding roots in $K$ of single-variable polynomials with coefficients in $K$.

(b) Using (a), or otherwise, determine all solutions in the field $\mathbb{Q}(i)$ to

$$2ix^3 + (2 - 4i)x^2 - (2 - 5i)x - (2 - i) = 0.$$

**Exercise 2.1.3.**

(a) Find all integer solutions $(x, y)$ to $3x + 5y + 4 = 0$ (and prove you have found all of them!).

(b) Do the same for $4x + 6y + 5 = 0$.

(c) For $a, b, c \in \mathbb{Z}$, give a necessary and sufficient criterion for the equation $ax + by + c = 0$ to have (i) infinitely many solutions, (ii) a finite nonzero number of solutions, and (iii) no solutions $(x, y)$ in the integers.

(d) Generalize (c) to an arbitrary number of variables. More precisely, given any $n \in \mathbb{Z}_{\geq 1}$ and integers $a_1, \ldots, a_n, c \in \mathbb{Z}$, find necessary and sufficient conditions for the equation

$$a_1x_1 + \cdots + a_nx_n + c = 0$$

to have integer solutions $(x_1, \ldots, x_n)$ as in (i), (ii), and (iii).

**Exercise 2.1.4.**

(a) Find all rational solutions $(x, y)$ to $x^2 + 3y^2 = 2$.

(b) Let $p$ be a prime. Find all rational solutions $(x, y)$ to the equation $x^3 + py^3 = p^2$.

**Exercise 2.1.5.**

(a) Finish the computation started in class (1.1.6) to verify that the described procedure ("chord and tangent process") yields Bachet's formula 1.1.8.

(b) In the case $c = 1$, why does Bachet's formula get "stuck" at the points $(0, \pm 1)$?

**Exercise 2.1.6.**

(a) Find all rational solutions $(x, y)$ to $3x^2 - 2y^2 = 1$.

(b) $(**)$ Find all integer solutions $(x, y)$ to $3x^2 - 2y^2 = 1$.

**Exercise 2.1.7.**

(a) Find a prime at which the curve $x^2 + y^2 = 3$ is locally obstructed.

(b) $(*)$ Find *all* primes at which the curve $x^2 + y^2 = 3$ is locally obstructed.

**Exercise 2.1.8.** (Adapted from [2, Exercise 2.4].)

(a) Consider the plane curve $y^2 = x^3 + 1$. For each prime $p$, let $n_p$ be the number of solutions $(x, y)$ to this equation modulo $p$ (i.e., the number of $\mathbb{F}_p$-points on this affine curve). Using your favorite computer software, compute the values $n_p$ for all primes $p \leq 100$. Do you see any patterns? Make and prove conjectures. (Hint: Consider the cases $p \equiv \pm 1 \pmod 3$ separately.)

(b) Repeat the same procedure for the curve $y^2 = x^3 + x$. (Hint: Consider the cases $p \equiv \pm 1 \pmod 4$ separately.)

**Exercise 2.1.9** (Fisher). Let $E$ be the elliptic curve over $\mathbb{Q}$ defined by the equation $y^2 + y = x^3 - x$.

(a) Draw a graph of the real points of $E$.

[1] This is the same as having the ability to find *one* factorization of any element of $R$, along with the knowledge of all units of $R$.

(b) Let $P := (0,0) \in E(\mathbb{Q})$. Get Sage to compute $nP$ for $n = 0, 1, \ldots, 20$. What do you notice about the denominators? Make and prove conjectures. (Hint: Can you express the operation of adding $P$ formulaically?)

### 2.1.B PODASIPs

Prove or disprove and salvage if possible the following statements.

**Exercise 2.1.10** (Hasse-Minkowski for Quadratic Equations)**.** Let $b, c \in \mathbb{Q}$. The quadratic equation $x^2 + bx + c = 0$ has a root in $\mathbb{Q}$ iff it has a root in $\mathbb{Q}_p$ for all primes $p \leq \infty$. (For those not too familiar with $\mathbb{Q}_p$ yet, the only fact you will need is: if a $d \in \mathbb{Q}^\times$ is a square in $\mathbb{Q}_p$, then $v_p(d)$ is even. You may assume this for now.)

**Exercise 2.1.11** (Homogeneous Polynomials)**.** Let $K$ be a field, $d \in \mathbb{Z}_{\geq 0}$, and $F \in K[X, Y, Z]$. The following conditions are equivalent:

(a) Every monomial in $F$ has total degree $d$.
(b) We have the equality $F(WX, WY, WZ) = W^d F(X, Y, Z)$ in the polynomial ring $K[W, X, Y, Z]$.
(c) For all $\lambda \in K$, we have $F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z)$.
(d) We have that
$$X\frac{\partial F}{\partial X} + Y\frac{\partial F}{\partial Y} + Z\frac{\partial F}{\partial Z} = d \cdot F.$$

**Exercise 2.1.12.** (Adapted from [2] Exercise 1.15].) Let $K$ be a field, $g(u) \in K[u]$ be a monic quartic polynomial, and consider the curve
$$v^2 = g(u).$$

(a) Suppose we are given a root $\alpha \in K$ of $g$, and a $\beta \in K^\times$. The transformation
$$(x, y) := \left(\frac{\beta}{u - \alpha}, \frac{\beta^2 v}{(u - \alpha)^2}\right)$$
transforms $v^2 = g(u)$ to a curve of the form
$$y^2 = f(x)$$
for some cubic polynomial $f(x) \in K[x]$. This transformation is birational (i.e., a one-to-one correspondence between points of the two curves, except possibly for a finite number of points). Note that this birational transformation does not arise from a linear change of coordinates on (projective closures of) these curves.
(b) If $X, Y, Z \in K$ satisfy $X^4 + Y^4 = Z^4$ with $Z \neq X$, then
$$(x, y) := \left(2\left(\frac{Z + X}{Z - X}\right), \frac{4Y^2}{(Z - X)^2}\right)$$
lies on the curve
$$y^2 = x^3 + bx$$
for some $b \in K$. This $b$ is unique. (What is it?)

(Hint: You will need some condition on $g$ for (a) to work. What is this condition? What implications does this condition have for the roots of $f$? What do parts (a) and (b) have to do with each other? Part (b) is definitely not correct as stated.)

**Exercise 2.1.13.** Let $K$ be a field.

(a) Any two lines in $\mathbb{P}^2(K)$ meet in exactly one point. Any two points in $\mathbb{P}^2(K)$ simultaneously lie on exactly one line.
(b) Given any two ordered quadruples $(P_1, P_2, P_3, P_4)$ and $(Q_1, Q_2, Q_3, Q_4)$ of points of $\mathbb{P}^2(K)$, there is a unique linear change of coordinates $\varphi$ such that $\varphi(P_i) = Q_i$ for $i = 1, 2, 3, 4$. The same result holds for ordered pentuples.

**Exercise 2.1.14** (Fisher)**.** Let $C \subset \mathbb{P}^2_{\mathbb{Q}}$ be a smooth cubic curve. If $K/\mathbb{Q}$ is a quadratic or cubic number field, then $C(K) \neq \emptyset$ implies that $C(\mathbb{Q}) \neq \emptyset$.