These problems are related to the material covered in Lectures 27-29. I have made every effort to proof-read them, but some errors may remain. The first person to spot each error will receive 1-5 points of extra credit.

The problem set is due by 11:59pm on 11/20/2020 and should be submitted electronically as a pdf-file e-mailed to zzyzhang@mit.edu and roed@mit.edu (please include "18.782" in the subject of the email). You can use the latex source for this problem set as a template for writing up your solutions; be sure to include your name in your solutions and to identify collaborators and any sources not listed in the syllabus.

As usual, a *curve* is a smooth projective (irreducible) variety of dimension one.

Problem 1. A genus 1 curve with no rational points (30 points)

Consider the homogeneous polynomial

$$f(x, y, z) = x^3 + 2y^3 + 4z^3.$$

(a) Prove that the zero locus of f is a plane curve $C/\mathbb{Q}$.

(b) Prove that C has genus one.

(c) Prove that C has no $\mathbb{Q}$-rational points (so it is not an elliptic curve over $\mathbb{Q}$).

Problem 2. Hyperelliptic curves (70 points)

A *hyperelliptic curve* C/k is a curve of genus $g \geq 2$ whose function field is a separable quadratic extension of the rational function field $k(x)$. The non-trivial element of $\mathrm{Gal}(k(C)/k(x))$ is called the *hyperelliptic involution*. In this problem we consider hyperelliptic curves over a perfect field k whose characteristic is not 2 (so every quadratic extension of $k(x)$ is separable).

(a) Let C/k be a hyperelliptic curve of genus g. Prove that C can be defined by an affine equation of the form $y^2 = f(x)$, where $f \in k[x]$ is a polynomial of degree $2g+1$ or $2g+2$ (so C is the desingularization of the projective closure of this affine variety). (hint: consider the Riemann-Roch spaces $\mathcal{L}(nD)$ where D is the pole divisor of x, and proceed along the lines of the first part of the proof of Theorem 23.3; as a first step, figure out what the degree of D must be).

(b) Prove that the polynomial f in part (a) can be made squarefree, and that $y^2 - f(x)$ is irreducible in $\overline{k}[x, y]$. Then show that if k is algebraically closed one can make f monic and of degree $2g + 1$.

(c) Let f be any squarefree polynomial in $k[x]$ of degree $d \geq 5$. Prove that the curve defined by $y^2 = f(x)$ is a hyperelliptic curve of genus $g \leq (d - 1)/2$.

(d) Let C/k be a hyperelliptic curve of genus g defined by $y^2 = f(x)$ with f squarefree of degree d, where k is algebraically closed. Prove that there are at least d distinct places of $k(C)$ that are fixed by the hyperelliptic involution, but not every place of $k(C)$ is fixed by the hyperelliptic involution.

(e) Let C/k be a hyperelliptic curve of genus g over an algebraically closed field k, and let σ be an automorphism of $k(C)$ that fixes k. Prove that if σ does not fix every place of $k(C)$ then it fixes at most $2g + 2$ places. (hint: show that there is a nonconstant function $x \in \mathcal{L}((g+1)P)$, where P is a place not fixed by σ, and then show that every place fixed by σ corresponds to a zero of $\sigma(x) - x$).

(f) Using (b-e), prove that every equation of the form $y^2 = f(x)$ with $f \in k[x]$ a squarefree polynomial of degree $d \geq 5$ defines a hyperelliptic curve C/k of genus $g = \lfloor \frac{d-1}{2} \rfloor$. Your proof should work whether or not k is algebraically closed.

(g) Prove that every curve of genus 2 is hyperelliptic (hint: first show there exists an effective canonical divisor W, then consider a non-constant $x \in \mathcal{L}(W)$).

Problem 3. Survey

Complete the following survey by rating each problem on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			

Feel free to record any additional comments you have on the problem sets or lectures; in particular, how you think they might be improved.