due-02-12.sagews

February 6, 2014

Contents

1 Homework 4 Due Feb 12, 2014

1.1 Instructions

- Put your solutions in the empty space below the problem.
- When youre done, open the worksheet, and copy/paste the URL to this worksheet into an email to wstein@gmail.com with the subject math 480: homework 02-12.

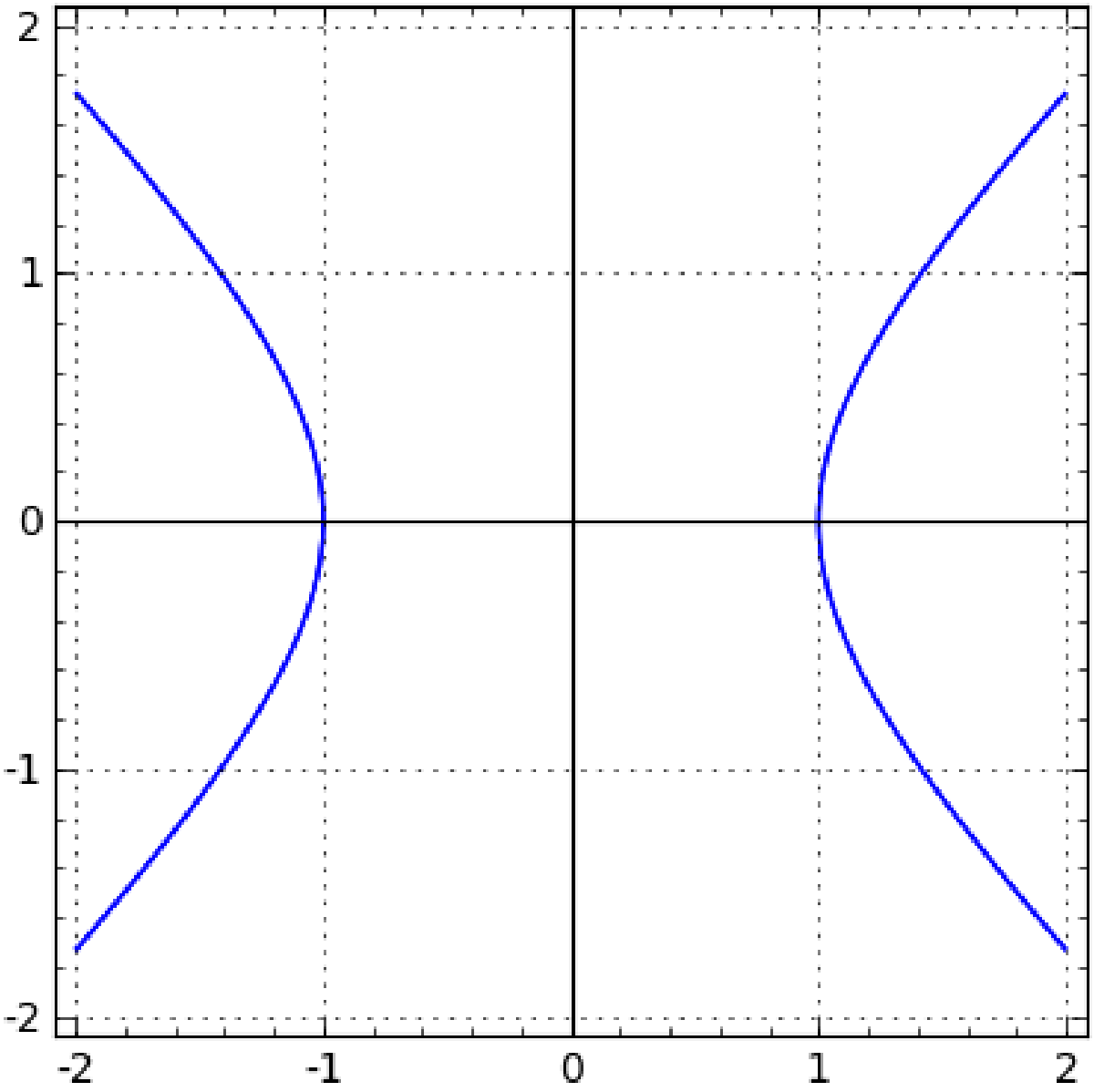
1.2 Problems

1.2.1 Problem 1: Rational Points on Conics (i.e., Pythagorean triples)

(If you want, you can do this problem entire with pencil and paper, like people did thousands of years ago. A computer isnt needed.)

1. Derive an explicit parametrization of all rational points on the unit circle $x^2 + y^2 = 1$, i.e., a function $f(t) = (?, ?, ?)$ so that there is a 1-1 correspondence between $t \in \mathbf{Q} \cup \{\infty\}$ and rational points on the circle. (Hint: This should be pretty easy to find online if you get stuck. The idea is to draw a line of slow t through $(-1, 0)$ and look at the other point of intersection.)
2. Use a similar method to derive an explicit parametrization of all rational points on the hyperbola $x^2 - y^2 = 1$.

```
#Here's a plot of that hyperbola
%var x,y
implicit_plot(x^2-y^2==1,(x,-2,2),(y,-2,2), axes=True, gridlines=True)
```



1.2.2 Problem 2: NO Rational Points on Conics

1. Prove that there are no rational numbers x, y such that $2x^2 + 3y^2 + 5 = 0$.
2. Prove that there are no rational numbers x, y such that $x^2 + y^2 = 3$. (Hint: write $x = a/b$ and $y = c/d$ with a, b, c, d integers, clear denominators, make sure there are no common factors, and work modulo 3.)
3. Prove that there are no rational numbers x, y such that $x^2 - 2y^2 = 3$.

1.2.3 Problem 3: Archimedes Cattle Problem

Read Sections 1 and 2 of Solving the Pell equation by Hendrik W. Lenstra, Jr.
`http://www.math.leidenuniv.nl/~psh/ANTproc/01lenstra.pdf`

1. Basic reading question: The total number of cattle is some number with n digits. What is n?

1.2.4 Problem 4: Group law problem

1. Make up an elliptic curve over $\mathbf{Q}$ with at least two distinct nonzero rational points P and Q on it, and add them together, i.e., compute $P + Q$.

2. Let E be the elliptic curve $y^2 = x^3 + 2x + 3$ over the finite field $\mathbf{F}_p$, where $p = 2^{61} - 1$. Consider the point $P = (1338935335744614844, 1658805286949476255)$. What is $P + P$? What is $2014P$?

1.2.5 Problem 5: Your Project

1. Write enough of a rough draft of your project that it is at least 3 pages long and actually says something.

2. Get somebody else in this class (of your choosing) to read what you wrote and write a paragraph of feedback about it. Paste that feedback below.