Dartmouth College
Mathematics 17

Assignment 2
due Wednesday, January 18

1. Another use for calculus. In our discussion of the Bachet problem, we assumed that a tangent to the cubic intersected in one other point. Solving simultaneously gave a cubic whose roots were the x-coordinates of the points of intersection. You assumed that the point of tangency occurred with multiplicity two. The means by which we prove this relies on the following problem,

   Let f be a polynomial of degree n over a field F (e.g., the real or complex numbers), and let $a \in F$. We say that f has a **zero of order $k \geq 0$ at $x = a$**, if $f(x) = (x-a)^k g(x)$ for some polynomial g with coefficients in F and satisfying $g(a) \neq 0$.

   (a) Establish the following generalization of what is needed in the Bachet problem. Show that f has a zero of order k at $x = a$ if and only if $f(a) = f'(a) = \cdots = f^{(k-1)}(a) = 0$ and $f^{(k)}(a) \neq 0$. *Hint:* Taylor polynomials are your friend.

   (b) Generalizing the Bachet problem, consider $y^2 = g(x)$ where g is a cubic. Suppose we find the equation of the tangent line to the curve at the point (a, b). Assuming a non-vertical tangent, it will have the form $y - b = m(x - a)$ where m is the slope we get by implicit differentiation (your answer will be in terms of g').

   The cubic we obtained was $f(x) = g(x) - (m(x-a)+b)^2 = (x-a)^2(x-x_0)$. Show that this assumption is valid by showing f has at least a double root at a, i.e., by verifying that $f(a) = f'(a) = 0$.

2. One of our goals is to describe a group law for the points on an elliptic curve. In the short term, let's see why the obvious association does not make a viable candidate.

   Since we have not yet formally introduced groups, let's simply look for some sort of structure we can impose on a set with nice properties. So our set will be the set of points on a cubic curve, C. As we have observed in class, a line and a cubic should intersect in at most three points, so given points P and Q on C consider the line through P and Q. If $P = Q$, we consider the tangent line to the curve at P. Let $P * Q$ denote the third point of intersection which may on occasion be either P or Q.

   (a) (easy) Explain why the operation $*$ is commutative, that is why is $P * Q = Q * P$.

   (b) Prove that there is no identity element for this operation, that is there is no point P_0 on C so that $P_0 * P = P$ for all points P on C.

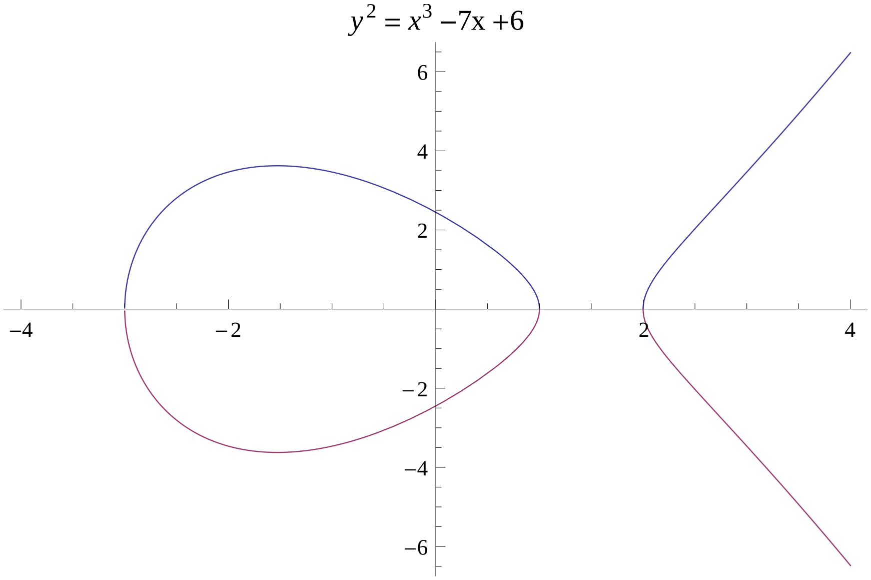
   (c) Explain why $P * (P * Q) = Q$. There are several cases to consider.

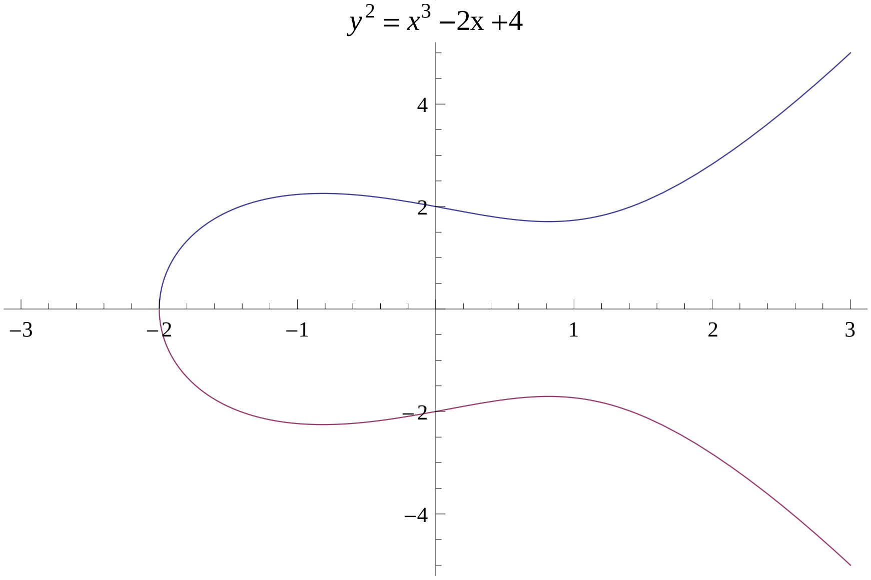
   (d) Prove that the operation $*$ is not associative, that is in general, that $P*(Q*R) \neq (P * Q) * R$. You can do this by picture if you like; I have included a couple of reasonable graphs on the last page of the assignment.

3. Analogous to what we did in class and projecting from the rational point $(1, 1)$, find a parametrization for the points on the conic $x^2 + y^2 = 2$. Note: projecting onto the x or y-axis does not work as expected, as not all lines from $(1, 1)$ to points on the circle intersect those axes. As we did in class, explain the correspondence of rational points on the line versus the conic.

4. Now consider the issue of rational points on $x^2 + y^2 = 3$. In contrast to the example above and the one in class, prove that there are no rational points on this curve, and describe the crucial difference between this example and the one before.

5. Find a square-free congruent number not in the list provided on the web site, showing all work to obtain it.


$y^2 = x^3 - 7x + 6$
6
4
2
−2
−4
−6
−4
−2
2
4


$y^2 = x^3 - 2x + 4$
4
2
−2
−4
−3
−2
−1
1
2
3