1. Show that every nonsingular curve in $\mathbb{P}^2_C$ is irreducible.

2. (Owner: Jacob) Prove Eisenstein’s criterion using the theorem of the Newton polygon. In other words, suppose $p$ is a prime and $f(x) = a_0 + \cdots + a_n x^n$ is a polynomial with integer coefficients such that $p$ divides $a_0, \ldots, a_{n-1}$ but not $a_n$, and furthermore $p^2$ does not divide $a_0$. Then $f$ is irreducible over $\mathbb{Q}$.

3. (Owner: Barry and Nathan) Write a function in Macaulay2, or any computer algebra package you may prefer, implementing the group law on a smooth cubic curve

$$E = V(y^2 z = x^3 + axz^2 + bz^3)$$

over a finite field $\mathbb{F}_p$ for a specified prime $p \neq 2, 3$.

In other words, the input to your function is a prime $p$, two elements $a, b$ of $\mathbb{F}_p$ such that $E$ is nonsingular, and points $P_1 = (q : r : s)$ and $P_2 = (t : u : v)$ on $E$, and the output is the sum $P_1 + P_2 \in E$, with the point $(0 : 1 : 0)$ playing the role of the identity.

Please e-mail your function to both me and Michael. As always, you are welcome to collaborate with your classmates, on the condition that you type your own final solution and provide a brief description of how your function works.

Optional, ungraded: Use your function to publish a (very, very weak) ElGamal elliptic curve public key.

Here is some sample Macaulay2 code that may be helpful. Also, please consult the online document The Macaulay2 Language for programming basics in Macaulay2.

```macaulay2
groupLaw = (a, b, p, q, r, s, t, u, v)->(
    R:= ZZ/p[x,y,z];
    E:= -y^2*z + x^3 + a*x*z^2 + b*z^3;
    if 4*a^2 + 27*b^3 == 0_R then
        error "cubic curve is not smooth";
    if substitute(E, {x=>q,y=>r,z=>s}) != 0 or substitute(E, {x=>t,y=>u,z=>v}) != 0 then
        error "point not on curve";
    if (q == 0 and s == 0) then return (t,u,v);
    if (t == 0 and v == 0) then return (q,r,s);
    --write your function here!
)
```