Tamagawa numbers, Ed Schaefer, Santa Clara University

In an appendix to Silverman's first book on elliptic curves is a table of elliptic curves over p-adic fields with stick figures and below each stick figure is a group. For a project with V. Flynn, F. Leprévost, M. Stoll and J. Wetherell on finding empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves, we needed to find these stick figures and groups for genus 2 curves and their Jacobians. Here is how we did it.

Let K be a finite extension of $\mathbf{Q}_p$ and k be the residue class field. Let C be a curve (smooth, complete, absolutely irreducible) over K and $J = \mathrm{Jac}(C)$ be its Jacobian. There is a filtration $J^1(K) \subseteq J^0(K) \subseteq J(K)$. The group $J^1(K)$ is a pro-p group that is isomorphic to a formal group. The group $J^0(K)/J^1(K)$ is the identity component of the smooth reduction of J; there will be more on this in the Néron models talk. What about $J(K)/J^0(K)$? How do we compute it and what is it good for? Its size is called the Tamagawa number.

First we compute $J(K^{\mathrm{unr}})/J^0(K^{\mathrm{unr}})$ and then take $\mathrm{Gal}(K^{\mathrm{unr}}/K)$-invariants. Why is this OK? Note $J^0(K^{\mathrm{unr}})^{\mathrm{Gal}(K^{\mathrm{unr}}/K)} = J^0(K)$. In other words, J^0's are stable under unramified base extension. This is not as obvious as the notation suggests and is an indication that the notation is not good. In fact, for ramified extensions, such statements do not necessarily hold. Second, since $H^1(\mathrm{Gal}(K^{\mathrm{unr}}/K), J^0(K^{\mathrm{unr}})) = 0$, it turns out that $J(K^{\mathrm{unr}})/J^0(K^{\mathrm{unr}})^{\mathrm{Gal(K^{unr}/K)}} = J(K)/J^0(K)$.

Let $\mathcal{O}$ be the ring of integers in K^{unr} and $\mathfrak{p}$ be the prime of K and K^{unr}.

Outline.

1. Find a model for C over $\mathcal{O}$.

2. Blow up non-regular points of C until regular. Blowing up is a birational map, so what you get is isomorphic to C.

3. Blow down exceptional components of the special fiber.

4. Find degree-0 divisor classes of the components of the special fiber. This is isomorphic to $J(K^{\mathrm{unr}})/J^0(K^{\mathrm{unr}})$.

5. Find the Galois invariants.

First find a proper model for $C/\mathcal{O}$ "with minimal discriminant". I will not define proper here. If you use equations that describe a projective curve over K, then the model will be proper. Here is an example of what we mean by "minimal discriminant".

Example: Take the projective closure of $y^2 = x^3 + 5^6$. It is not minimal over $\mathbf{Z}_5^{\mathrm{unr}}$ since there is an ismorphism to $v^2 = u^3 + 1$ with $u = x/5^2$, $v = y/5^3$. The model $v^2 = u^3 + 1$ has minimal discriminant. It is known how to do this for elliptic curves in all cases and for genus 2 curves with odd residue characteristic. For other curves, this is a field of research.

When we consider $C/\mathcal{O}$, it is a surface. Note $0 \subset \langle u, v-1\rangle \subset \langle u, v-1, 5\rangle$ are all prime ideals, so the Krull dimension is 2. The ideal $\langle u, v-1\rangle$ corresponds to the point where u and $v-1$ are both 0, in other words the point $(0,1)$ over the p-adic field. The ideal $\langle u, v-1, 5\rangle$ corresponds to the point where u, $v-1$ and 5 are all 0, in other words the point $(0,1)$ over the residue class field. It is best to think of points of $C/\mathcal{O}$ as ideals. Working over $\mathcal{O}$ means no primes in denominators. We want to find a model of $C/\mathcal{O}$ that is non-singular. How could it be singular when C/K is non-singular? As we have seen above, $C/\mathcal{O}$ has a piece corresponding to the reduction, where we can find singularities.

Over rings, non-singularity is best measured by regularity. Let m_P be the maximal ideal at the point P. (We are now looking in the local ring at the point P, so the ideal is maximal. For computational purposes we can confuse the prime ideal with its associated maximal ideal in the localization.) $C/\mathcal{O}$ is regular at P if $\dim m_P/m_P^2 = \dim(C/\mathcal{O}) = 2$. If it is not regular, then the dimension of m_P/m_P^2 can only be higher.

Let us go through an example to familiarize ourselves with the concept of regularity. In particular, I would like to demonstrate that the idea of regularity agrees with the calculus definition of non-singularity over a field. Over a ring, we can not use the calculus definition, but we still have the concept of regularity, so it will serve us better.

Example. $y^2 = x^3 - x/\mathbf{C}$. (Since we are working over a field, this is, indeed, 1-dimensional.) We can use partial derivatives to show that this curve is smooth at the point $(0,0)$. We have $m_{(0,0)} = \langle x, y\rangle$ (that is the ideal of functions that are 0 at this point). What is $\dim\langle x,y\rangle/\langle x,y\rangle^2 =$? Well $x = y^2 - x^3 \in \langle x,y\rangle^2$ so $\langle x,y\rangle/\langle x,y\rangle^2$ is generated by y. Thus $\dim(\text{curve}/\mathbf{C}) = \dim\langle x,y\rangle/\langle x,y\rangle^2 = 1$, so the curve is regular at $(0,0)$.

We can use partial derivatives to show that $y^2 = x^3 - x^2/\mathbf{C}$ is singular at $(0,0)$. The quotient $\langle x,y\rangle/\langle x,y\rangle^2$ has two generators, since each term in the equation for the curve is in $\langle x,y\rangle^2$ so we can not use the same trick to eliminate anything. Thus the curve is not regular at $(0,0)$. We will work over a surface, so it is regular when this quotient has two generators, and not regular when it has more.

Whereever the surface is not regular, we will blow it up until it is all regular. Blowing up is a process of smoothing. When blowing up, we always get exceptional components that we do not want. We will break the surface into a union of two disjoint pieces.

Special fiber: prime ideals containing $\mathfrak{p}$. (For $v^2 = u^3 + 1/\mathbf{Z}_5^{\mathrm{unr}}$, $\langle u, v-1, 5\rangle$ is in the special fiber.)

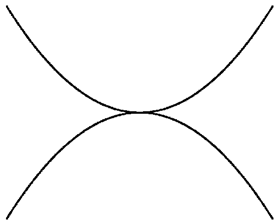
Generic fiber: prime ideals not containing $\mathfrak{p}$. (For $v^2 = u^3 + 1/\mathbf{Z}_5^{\mathrm{unr}}$, $\langle u, v-1\rangle$ is in the generic fiber.)

The generic fiber is the curve over the p-adic field. It is already non-singular, hence regular. The special fiber is the points of the reduction, which is not necessarily non-singular. Thus it suffices to check the special fiber for regularity.

If the reduction at $\mathfrak{p}$ is non-singular (working over k), then over $\mathcal{O}$, we have regularity at this point/ideal (though not necessarily vice versa).

Example. $C : y^2 = x^6 + 54x^3 - 27/\mathbf{Z}_3$. Technically, this should be glued together with another affine piece so that over $\mathbf{Q}_3$, we get the two points at infinity also. Over $\mathbf{Q}_3$, this is a genus 2 curve. We immediately start by taking C over $\mathbf{Z}_3^{\mathrm{unr}}$ and at the end, we will take Galois-invariants.

The reduction is $y^2 = x^6$. It has two components which we will denote A and B.



The reduction (over $\overline{\mathbf{F}_3}$) is non-singular except at $(0,0)$ so C is regular except, perhaps, at $\langle x,y,3\rangle$, where $x=y=3=0$. Note that neither x,y nor 3 can be written in terms of the other two modulo the square of the ideal, so C is not regular there.

We are OK at the points at infinity since we have $y^2 = 1\cdot x^6\dots$. However $y^2 = 3^2x^6+\dots$ would have been a problem and for that we would need to blow up the other affine cover.

We must blow up $y^2 = x^6+54x^3-27$ at $\langle x,y,3\rangle$. Algebraic geometers do not like the mixture of variables and numbers; they can only deal with variables. So we describe the affine part of C that we need to blow up as $f = x^6+2p^3x^3-p^3-y^2 = 0, p=3$. We blow up at the point $(0,0,0)$, i.e. the ideal $\langle x,y,p\rangle$. We always blow up the origin. If another point is not regular, then we move it to the origin.

Here is the process of blowing up, which is described in Hartshorne's book *Algebraic Geometry.*

First blow up. We embed (this affine part of) C into $\mathbf{A}^3\times\mathbf{P}^2$ with coordinates $(x,y,p,x_1 : p_1 : y_1)$ and relations $x_1p = xp_1$, $y_1p = yp_1$, $xy_1 = x_1y$. So now C is described by $f = x^6+2p^3x^3-p^3-y^2, p=3$, $x_1p=xp_1$, $y_1p=yp_1$, $xy_1=x_1y$. We will look in the three covers: $x_1=1$, $y_1=1$, $p_1=1$ and check for regularity.

First affine cover:

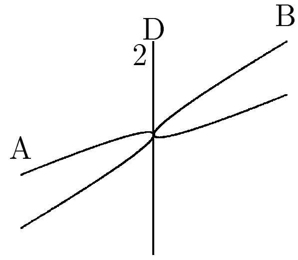
$x_1 = 1$. We have $y = xy_1$, $p = xp_1$. So we can consider this cover to be in $\mathbf{A}^3$. We get the pair of equations $((2p_1^3+1)x^4 - p_1^3x - y_1^2)x^2 = 0$, $xp_1 = 3$.

Note $x^2=0$ is exceptional. So we have $f_x = (2p_1^3+1)x^4 - p_1^3x - y_1^2 = 0, xp_1 = 3$.

We check the reduction: $3=0$. Either $x=0$ or $p_1=0$.

If $x=0$ we get $-y_1^2=0$. We denote this component D; it has multiplicity 2 (from the square).

If $p_1=0$ we get $x^4-y_1^2=0$. These are the old components A and B.



How can we tell that these are the same as the old A and B? Look at the gluing maps. We have $y_1 = y/x$ so $x^4 - y^2/x^2 = 0$ or $x^6 = y^2$. Note that what had been a terrible singularity (two cubics tangent at an inflection point) is now not quite as bad (two tangent conics).

Now let us check this first affine cover for regularity. The reduction is non-singular except along D: $x = -y_1^2 = 3 = 0$. So we check at the point $(x, y_1, p_1, 3) = (0, 0, t, 0)$, i.e. at the ideal $\langle x, y_1, p_1 - t, 3\rangle = \langle x, y_1, q, 3\rangle$ (where t ranges over $\mathbf{Z}_3^{\mathrm{unr}}$). We have

$$f_x(x, y_1, q + t) = h_1(q, t)x^4 + h_2(q, t)qx - y_1^2 - t^3 x = 0 \text{ and } x(q + t) = 3.$$

When $\langle x, y_1, q, 3\rangle/\langle x, y_1, q, 3\rangle^2$ has two generators, we have regularity at $\langle x, y_1, q, 3\rangle$. We note 3 is generated by x, q. Also, $x \in \langle x, y_1, q, 3\rangle^2$ if $t \not\equiv 0 (\mathrm{mod}\ 3)$. So we have regularity except at $\langle x, y_1, p_1, 3\rangle$. That completes the first affine cover.

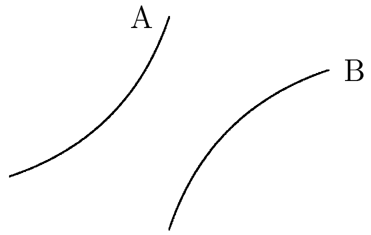
We have $f = x^6 + 2p^3x^3 - p^3 - y^2 = 0, p = 3$, $x_1 p = xp_1$, $y_1 p = yp_1$, $xy_1 = x_1 y$ and want to check the

second affine cover. $y_1 = 1$: We have $p = yp_1$, $x = yx_1$.

We get $((2x_1^3p_1^3 + x_1^6)y^4 - p_1^3 y - 1)y^2 = 0$, $yp_1 = 3$; $y^2 = 0$ is exceptional.

Reduction. $y = 0$: $1 = 0$ (empty)

$p_1 = 0$: $x_1^6 y^4 - 1 = 0$, A, B. Regular everywhere.

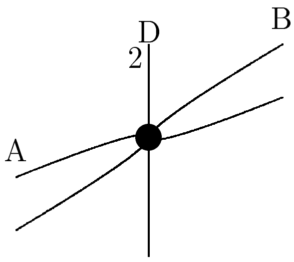


Third affine cover: $p_1 = 1$. We have $x = px_1$, $y = py_1$.

Get $((x_1^6 + 2x_1^3)p^4 - p - y_1^2)p^2 = 0$, $p = 3$. $p^2 = 0$ is exceptional.

Reduction $p = 0$: $-y_1^2 = 0$, D. Regular everywhere.

So after the first blow up, the current special fiber is below. The only non-regular point is on the first affine cover.

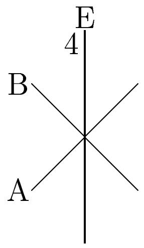


Second blow up. We blow up $f_x(x, y_1, p_1) = 0, xp_1 = 3$ at $\langle x, y_1, p_1, 3\rangle$. We get new coordinates $(x, y_1, p_1, x_2 : y_2 : p_2)$ with $xy_2 = x_2y_1$, $xp_2 = x_2p_1$, $y_1p_2 = y_2p_1$.

First affine cover: $x_2 = 1$. We get: (after getting rid of the exceptional component) $f_{xx} = (2p_2^3x^3 - p_2^3 + 1)x^2 - y_2^2 = 0$, $x^2p_2 = 3$.

Reduction. $x^2 = 0$: $-y_2^2 = 0$, E

$p_2 = 0$: $x^2 = y_2^2$, A, B.



We check regularity along E at $\langle x, y_2, p_2 - t, 3\rangle = \langle x, y_2, q, 3\rangle$. We have

$$f_{xx}(x, y_2, q + t, 3) = h_1(q, t)x^5 + h_2(q, t)x^2 - y_2^2, x^2(q + t) = 3.$$

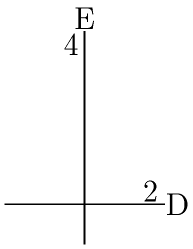
The quotient $\langle x, y_2, q, 3\rangle/\langle x, y_2, q, 3\rangle^2$ is generated by x, y_2, q. So we are nowhere regular along E.

There is nothing new in the second cover $y_2 = 1$.

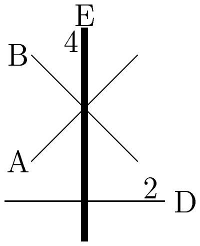
Third affine cover: $p_2 = 1$. We get $f_{xp} = (2x_2^3p_1^3 + x_2^3 - 1)x_2p_1^2 - y_2^2 = 0$, $x_2p_1^2 = 3$.

Reduction. $x_2 = 0$: $-y_2^2 = 0$, D.

$p_1^2 = 0$: $-y_2^2 = 0$, E. So were are nowhere regular along this part of E either.



What is worse, E does not lie entirely in any one cover. Thus we will have to blow up the first and third covers along E. The current special fiber is below.



Third blow up. We blow up the first cover: $f_{xx} = (2p_2^3x^3 - p_2^3 + 1)x^2 - y_2^2 = 0$, $x^2p_2 = 3$ along $x = y_2 = 3 = 0$.

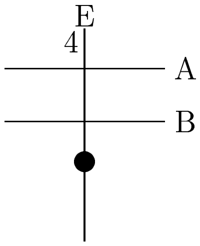
If $x, y_2 \in \mathcal{O}$, and they are not both 0, then $v_3(y_2) \geq v_3(x)$ so y_2/x is still integral (so were are not pushing bad stuff out to infinity). Thus it is safe to

let $y_2 = xy_3$. We get $f_{xx'} = 0$, $x^2p_2 = 3$.

Reduction. $x^2 = 0$: $y_3^2 = -p_2^3 + 1$, E.

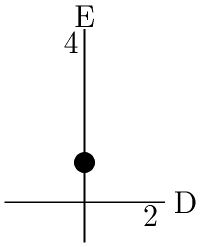
$p_2 = 0$: $1 = y_3^2$, A, B.

Note that E may appear to have genus 1, but since the reduction is $\overline{\mathbf{F}_3}$, we have a singular point at $(p_2, y_3) = (1, 0)$ and so the genus is 0.

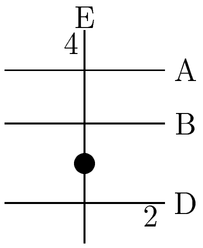


The non-regular point corresponds to the singular point mentioned above. Note that A and B have finally smoothed themselves out. They started as cubics tangential at their inflection points (terrible), then became tangential conics, then lines crossing transversally and now, separate lines.

The blow up of the third affine cover gives us the special fiber below.



The current special fiber is below.



It is not regular at $\langle x_1, y_3, p_2 - 1, 3\rangle$ only. So now we can blow up either the first or third cover. It does not matter, so we will blow up the first.

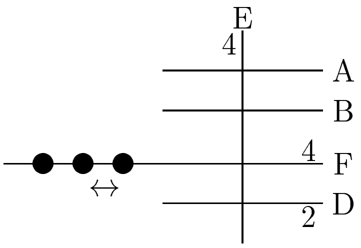
We have $f_{xx'}(x, p_2, y_3) = 0$, $x^2 p_2 = 3$, which is not regular at $\langle x_1, y_3, p_2 - 1, 3\rangle$. We always blow up the origin, so we must move the non-regular point there.

Let $p_3 = p_2 - 1$. We get

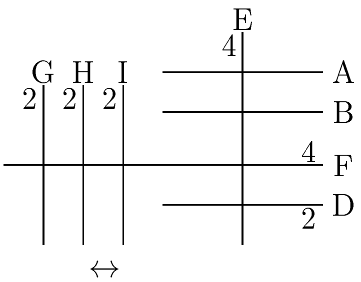
$$(2p_3^3 + 6p_3^2 + 6p_3 + 2)x^3 + (-y_3^2 + (-p_3^3 - 3p_3^2 - 3p_3)) = 0, x^2(p_3 + 1) = 3.$$

Note that there are 3's in the coefficients in the first equation and we do not want that. So we replace the 3's in first equation by $x^2(p_3+1)$. Then we get $g(x, p_3, y_3) = 0$, $x^2(p_3+1) = 3$. It is not regular at $\langle x, y_3, p_3, 3\rangle$.

Fourth blow up. We blow up $g = 0, x^2(p_3 + 1) = 3$ at $(x, p_3, y_3, 3) = 0$. We get the special fiber below with three points that are not regular; two are defined over $\mathbf{Q}_3(i)$ and conjugate.



Fifth through seventh blow ups. We blow up those three points and get the special fiber below.



Finally we have a regular model for $C/\mathbf{Z}_3^{\mathrm{unr}}$ (once we patch together all the affines). All components have genus 0. Elements of $\mathrm{Gal}(\overline{\mathbf{Q}_3}/\mathbf{Q}_3)$ not fixing $\mathbf{Q}_3(i)$ switch H and I.

We must remove remaining exceptional components. Let me finally define them. They are genus 0 curves with self-intersection number -1.

To understand this, we must define the intersection pairing. Let S' denote the current special fiber. The intersection pairing of the special fiber with any component is 0. So for example we have

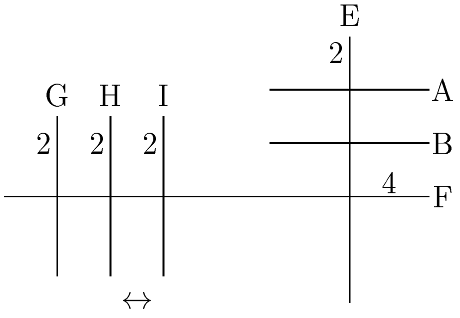
$$\begin{aligned} S' \cdot A = 0 \quad &= (A + B + 2D + 2E + 4F + 2G + 2H + 2I) \cdot A \\ &= A \cdot A + B \cdot A + 2D \cdot A + 2E \cdot A + 4F \cdot A + 2G \cdot A + 2H \cdot A + 2I \cdot A \\ &= A \cdot A + 0 + 0 + 2 \cdot 1 + 0 + 0 + 0 + 0. \end{aligned}$$

Thus $A \cdot A = -2$ so it is not exceptional. Since all of the intersections in our special fiber are transversal, the intersection pairings are all 1. If there are tangencies, you can get higher intersection multiplicities (and then you should look in Hartshorne to figure it out).

We can create an intersection pairing matrix, seen below. Above we created the first row of the matrix. Note that the dot product of a row, with the multiplicity row at the top, must be 0.

$$\begin{array}{cc} & \begin{array}{cccccccc} 1 & 1 & 2 & 2 & 4 & 2 & 2 & 2 \\ A & B & D & E & F & G & H & I \end{array} \\ \begin{array}{c} A \\ B \\ D \\ E \\ F \\ G \\ H \\ I \end{array} & \begin{bmatrix} -2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -2 \end{bmatrix} \end{array}$$

Note D is exceptional, so we blow down and start again. In this case, since D simply meets only E, the blow down means removing D. Were an exceptional component to meet a second and third component at different points, then in the blow down, the second and third components would meet transversally. If the second and third components meet the exceptional component at the same point, then see Hartshorne. Blowing does not change things birationally since we are blowing down a curve on a surface (so we are removing something of co-dimension 1). We get the following new special fiber and corresponding intersection pairing matrix.



$$\begin{array}{c|ccccccc} & 1 & 1 & 2 & 4 & 2 & 2 & 2 \\ & A & B & E & F & G & H & I \\ \hline A & -2 & 0 & 1 & 0 & 0 & 0 & 0 \\ B & 0 & -2 & 1 & 0 & 0 & 0 & 0 \\ E & 1 & 1 & -3 & 1 & 0 & 0 & 0 \\ F & 0 & 0 & 1 & -2 & 1 & 1 & 1 \\ G & 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ H & 0 & 0 & 0 & 1 & 0 & -2 & 0 \\ I & 0 & 0 & 0 & 1 & 0 & 0 & -2 \end{array}$$

None of the components are exceptional so we now have the correct special fiber. The model we have now of C is called the minimal proper regular model of C (more on that in the talk on Néron models). In order to find $J(\mathbf{Q}_3^{\mathrm{unr}})/J^0(\mathbf{Q}_3^{\mathrm{unr}})$, we need to apply a Picard functor. In other words we need to find degree 0 divisor classes. We will build up divisors from components of the special fiber.

The group $J(\mathbf{Q}_3^{\mathrm{unr}})/J^0(\mathbf{Q}_3^{\mathrm{unr}})$ is isomorphic to the quotient of

$$L = \{\alpha A + \beta B + \delta E + \epsilon F + \phi G + \gamma H + \eta I \mid \alpha + \beta + 2\delta + 4\epsilon + 2\phi + 2\gamma + 2\eta = 0\}$$

(degree 0 divisors) by the subgroup generated by the following divisors

$$-2A + E, -2B + E, A + B - 3E + F, E - 2F + G + H + I, F - 2G, F - 2H, F - 2I.$$

These are principal divisors corresponding to uniformizing parameters for the components $A, \dots, I$. Note how each arises from a row of the intersection pairing matrix.

Now we have an elementary group theory problem. We notice that α is determined by the rest of the coefficients, so when we project away from A we find that this group is isomorphic to

$$\begin{aligned} &\langle B, E, F, G, H, I \mid E = 0, E = 2B, 3E = B + F, \\ &\qquad 2F = E + G + H + I, F = 2G = 2H = 2I\rangle \\ &\qquad \cong J(\mathbf{Q}_3^{\mathrm{unr}})/J^0(\mathbf{Q}_3^{\mathrm{unr}}). \end{aligned}$$

We simplify by elimination, (removing Galois-invariant components first) and find that the group is isomorphic to $\langle H, I \mid 2H = 2I = 0\rangle$ and elements of $\mathrm{Gal}(\overline{\mathbf{Q}_3}/\mathbf{Q}_3)$, not fixing $\mathbf{Q}_3(i)$ switch H and I. Thus $J(\mathbf{Q}_3^{\mathrm{unr}})/J^0(\mathbf{Q}_3^{\mathrm{unr}}) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ and $\#J(\mathbf{Q}_3)/J^0(\mathbf{Q}_3) = 2 = c_3 =$ the Tamagawa number.

What is this good for? Now let K be a number field.

1. Let C/K. Say you're doing a $[q]$-descent on J, with q a prime. The Selmer group is contained in $H^1(K, J[q]; S)$ where $S = \{\mathfrak{q} \mid q$, primes of bad reduction of C, and if $q = 2$, real primes $\}$.

To compute the Selmer group you intersect the inverse images of $J(K_\mathfrak{p})/qJ(K_\mathfrak{p})$ for each prime $\mathfrak{p} \in S$, in $H^1(K, J[q]; S)$.

It turns out that if $\mathfrak{p}|p$ finite, $p \neq q$ and $q \not| c_\mathfrak{p}$, then since $H^1(\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{unr}}/K_\mathfrak{p}), J^0(K_\mathfrak{p}^{\mathrm{unr}})) = 0$, you can remove $\mathfrak{p}$ from S. That shrinks the size of the cohomology group and there are fewer local computations to do.

For example, if you are doing a 2-descent on an elliptic curve and there is an odd prime of bad reduction for which the Tamagawa number is odd, then that prime can be removed from consideration.

We can use the same argument for what Nils Bruin showed us. He had a set of covers (coming from the multiplication-by-2 map), parametrized by S. If there is an odd prime of bad reduction at which the Tamagawa number is odd, then you can remove that prime from the parametrizing set and there will be fewer covers to check.

2. The Birch and Swinnerton-Dyer conjecture tells you

$$\lim_{s\to 1}(s-1)^{-r}L(J,s) = \Omega \cdot \mathrm{Reg} \cdot \prod_{\mathfrak{p}} c_{\mathfrak{p}} \cdot \#\text{Ш}(J,K) \cdot (\#J(K)_{\mathrm{tors}})^{-2}$$

where $L(J,s)$ is the L-series, r is the rank, Ω is the determinant of a kind of real period matrix, Reg is the regulator of the Mordell-Weil group, $\text{Ш}(J,K)$ is the Tate-Shafarevich group and the $c_{\mathfrak{p}}$'s are Tamagawa numbers.

This was a lot of work. Are there any computer programs that will do the computation for us? For elliptic curves, PARI's elllocalred command will tell you c_p. Qing Liu's program gives $\#J(\mathbf{Q}_p^{\mathrm{unr}})/J^0(\mathbf{Q}_p^{\mathrm{unr}})$ for genus 2 curves, $p \neq 2$. He is working on $p = 2$ and doing this over $\mathbf{Q}_p$.