Cocycles

Because $\mathcal{L}$ is not a free module, a Cech cocycle representing $\mathcal{L}$ with respect to the open covering by trivial sets where a, b, c is inverted, is not a coboundary.

The smaller subscheme of the integer projective plane which we are looking at, where we've imposed $(abc)^p = 0$, is finite in the very strong sense that its coordinate ring has finitely many elements.

We constructed the roots of unity τ by permuting coordinates; this is different than the way we construct the cocycle for the line bundle; the cocycle for $\mathcal{L}^{\otimes 2}$ agrees when restricted to the subscheme up to possibly inverting τ;

The actual cocycle directly comes from the Fermat condition. Define, within the sheaf of units $\mathcal{O}^\times$ the subsheaf consisting of those units which restrict to a $2p$'th root of unity on the subscheme where $(abc)^p = 0$. The precise Fermat condition is firstly that $\mathcal{L}$ admits this sheaf of structural groups, and therefore that $\mathcal{L}^{\otimes 2p}$ restricts trivially to the subscheme. And secondly that the restriction of $\mathcal{L}^{\otimes p}$ is represented by the cocycle which evaluates to -1 on every pair of the three coordinate charts.

The condition still implies the weaker but simpler condition that $\mathcal{L}^{\otimes 2p}$ restricts to a trivial line bundle on the subscheme defined by $(abc)^p = 0$.

In terms of $\mathcal{L}$ viewed as a module, that the tensor product $\mathcal{L}^{\otimes 2p} \otimes_J J/((abc)^p)$ is a free module over $J/((abc)^p$.

The same is true if we restrct attention to our connected union of four components, where $\mathcal{L}^{\otimes 2p}$ has as its (global) sections explicitly the polynomials of degree congruent to $2p$ modulo $6p$ in

$$x = (a, a, a, a)$$
$$y = (b, b\omega, c, c\omega)$$
$$z = (c, c\omega, b\tau, b\omega\tau)$$

If the Fermat theorem were false, both for the whole fiber and for the

projection we've looked at carefully, our module $\mathcal{L}^{\otimes 2p} \otimes J_S/((abc)^p)$ being a free module would have a basic element, represented by a homogeneous polynomial of degree $2p$ in x, y, z.

Let us try to find a basic homogeneous polynomial of degree $2p$. Since we are working over $\mathbf{Z}$ where $6p$ is inverted, we can average over permutations of x, y, z and we should find a generator which is a symmetric polynomial in x, y, z of degree $2p$. This is a polynomial with integer coefficients (the only roots of unity we encounter are in the components of x, y, z in the normalization).

We can see that $x^{2p}+y^{2p}+z^{2p}$ works as such a basis element. Because $s_1 = 0$, this is just s_2.

In the case of the image of our four components, the image of this in the normalization is $(a^{2p} + b^{2p} + c^{2p})(1, 1, 1, 1)$ and in the case of the full fiber it is $a^{2p} + b^{2p} + c^{2p}$ times the identity element of J, the calculation uses the fact that the roots of unity are raised to a multiple of the p'th power, and on each component each entry specializes to one of a, b, c. As for the coefficient, when $a^p \equiv 0$, we have $b^p \equiv -c^p$ so the coefficient agrees with the unit $2c^{2p} \equiv 2b^{2p}$. Under the image of the map embedding the sections of $\mathcal{L}^{2p}$ into the normalization of J, this generating element is just the rational integer $a^{2p}+b^{2p}+c^{2p}$ times the identity. The coefficient restricts to a unit on the subscheme where $(abc)^p = 0$ and even on the subscheme where $(abc)^{3p} = 0$. Since we've specialized s_3^2 to a rational integer, this subscheme exactly the zero locus of s_3^2 as a global section of $\mathcal{L}^6$ viewed as the trivial line bundle.

Even if we had not passed to the fiber, but merely considered the variety defined by $x^p + y^p + z^p = 0$ in the projective plane, we would still have the line bundle, the restriction of a copy of a line bundle of the isomorphism type $\mathcal{O}(1)$, and $\mathcal{L}^{\otimes 6}$ would be generated by s_2^3 and s_1^2, furthermore, the restriction of $\mathcal{L}^{\otimes 6}$ to the locus where either section is zero, would be a line bundle generated by the other.

The section we are looking at is the restriction of s_2 to the subscheme of the Fermat curve defined by s_3^2. We know its third tensor power generates $\mathcal{L}^6$ and perhaps this abstractly implies s_2 generates $\mathcal{L}^{\otimes 2}$ however we verified this more explicitly after the specialization of

s_2^3 and s_3^2 to integers.

This is a good cross-check that things make sense. The actual Fermat condition concerns $\mathcal{L}^{\otimes p}$, and it is that in the restriction to the subscheme of the specialized fiber generated defined by $(abc)^p$ the actual cocycle of $\mathcal{L}^{\otimes p}$ using the sections x, y, z is the constant function -1.

This would not be true on the larger subscheme defined only by $(abc)^{3p}$; the connection there is our easy Hasse principle, that once the Fermat curve has a rational solution modulo $(abc)^p$ it also has one precisely.

Despite having a Hasse-type principle, it seems to make sense not to discard the part of the fiber in the complement of the scheme where this holds, because that subscheme, having a coordinate ring with finitely many elements, is a finite disjoint union along the prime divisors of abc. It is abstractly true that a Fermat counterexample could always be 'lifted' to the full scheme, however, the connectedness of the full scheme seems familiar.

Part of that connectedness was our proof of the existence of the four-fold intersection points. This was a deep proof which compared two "different" elements. This concerned connectedness prime-by-prime. Nevertheless it is a vivid experience to see that failure of the cocycle to be sufficiently near a root of unity, as required by the Fermat hypothesis, causes a tensor decomposition, a local ring that is not a discrete valuation ring.

One thing we have not done is to explore the properties of the ring we get if we go through the definition of J for a triple of integers a, b, c which do not satsify the Fermat condition. It involves relaxing the condition $s_1 = 0$

Actually, one way to relax the condition that $s_1 = 0$ is to consider the tranformation which converts the tuple of integers a^p, b^p, c^p into the tuple of differences $a^p - b^p, b^p - c^p, c^p - a^p$. as we will do in the next section.

The differences $a^p - b^p, b^p - c^p, c^p - a^p$.

We have, up to now, ignored the slight linear transformation relating the actual j invariant of the Frey curve with what we have called j. The issue is, the symmetric polynomials we are considering can be evaluted at differences, that is,

$$s_1(x-y, y-z, z-x) = 0$$
$$s_2^3(x-y, y-z, z-x) = -s_1^6 + 9s_1^4 s_2 - 27s_1^2 s_2^2 + 27s_2^3$$
$$s_3^2(x-y, y-z, z-x) = s_1^2 s_2^2 - 4s_1^3 s_3 - 4s_2^3 + 18 s_1 s_2 s_3 - 27 s_3^2.$$

Under the condition $s_1 = 0$ these become

$$s_2^3(x-y, y-z, z-x) = 27 s_2^3$$

$$s_3^2(x-y, y-z, z-x) = -4s_2^3 - 27 s3^2$$

and the matrix $\begin{pmatrix} 27 & 0 \\ -4 & -27 \end{pmatrix}$ interposes, which is invertible over our ring $\mathbf{Z}$ In fact, the matrix times $\frac{1}{27}$ is of order two, its own inverse, of course, as passing to successive differences twice is the same as multiplying by 3 or -3 depending on how the differences are ordered.

What this means is, now letting x, y, z be a^p, b^p, c^p, that the fiber we are calculating, where $[s_2^3 : s_1^2] = [\lambda_0 : \lambda_1]$, is such that we wish to set

$$\lambda_0 = 27\alpha$$

$$\lambda_1 = -4\alpha - 27\beta$$

if we wish $[\alpha : \beta]$ to be the j invariant of the Frey curve.

Under the assumption that $a^p + b^p + c^p = 0$, taking differences twice gets us back where we started, that is, for example,

$$(a^p - b^p) - (b^p - c^p) = a^p + c^p - 2b^p = -3b^p.$$

So, we are considering reducing modulo s_3 in one basis, whereas the Frey curve is the doubly branched cover over the zero locus of s_3^3 in the other basis, and the proof goes by considering the elliptic curve with cross-ratio $\lambda(a^p b^p)/c^p$ which is a branched cover of $\mathbb{P}^1$ at $[\frac{1}{3}(a^p - b^p) : 1], [\frac{1}{3}(b^p - c^p) : 1], [\frac{1}{3}(c^p - a^p) : 1], [1 : 0]$.

There is very little essential difference. It is essentially whether we allow ourselves to set the occurrences of s_1 to zero on the right sides of the equations for $s_2^2(x-y,y-z,z-x)$ and $s_3^2(x-y,y-z,z-x)$. If we do not assume s_1 to be zero, the fiber still exists.

The integers a,b,c which we put in the $6p+12$ entries times roots of unity to create x,y,z need to make the right sides of the three equations zero, and *one* way to do this is to make $s_1=0$ and then put $[9s_2^3(x^p,y^p,z^p) : -4s_2^3(x^p+y^p+z^p)-27s_3^2(x^p,y^p:z^p)$ into the desired ratio. The description this way is more general, it allows us to consider values of a,b,c which do not satisfy the Fermat equation, and when it comes to the situation of considering the cocycle of definition of $\mathcal{L}$ and its tensor powers, and specializing to subschemes, it attaches a particular special meaning to the specialization not only to where s_3^2 is zero but where $-4s_2^3-27s_3^2$ is zero.

That is the subscheme defined by the rational integer $(a^p-b^p)^2(b^p-c^p)^2(c^p-a^p)^2$. It is interesting that the rational integer related to the different element over j divided by the one for the disjoint union of the fibres over the six lambda values is a square root of this number times $s_2(a^p,b^p,c^p)^2$ times $s_3(a^p,b^p,c^p)$ times the (invertible) rational integer 6. In fact that ratio is $6s_2(a^p,b^p,c^p)^2s_3(a^p,b^p,c^p)s_3(a^p-b^pb^p-c^p,c^p-a^p)$ and if we substitute $\frac{1}{27}s_2(a^p-b^p,b^p-c^p,c^p-a^p)$ for $s_2(a^p,b^p,c^p)$ this becomes

$$2/9s_2(a^p,b^p,c^p)s_2(a^p-b^p,b^p-c^p,c^p-a^p)s_3(a^p,b^p,c^p)s_3(a^p-b^p,b^p-c^p,c^p-a^p).$$

The same is true of the actual different element as an element of $\mathcal{L}^{p-3}$ if we replace a,b,c by x,y,z. That is, up to a unit in $\mathbf{Z}$ where 6 is invertible, the different element ratio (the different element of J divided by the different element of Λ) is unaffected by replacing a^p,b^p,c^p by a^p-b^p,b^p-c^p,c^p-a^p.

We have talked about prime divisors of a,b,c and we have made roots of unity by dividing the Fermat equation by for example b^p to get $(c/b)^p+1 \equiv\ 0\ mod\ \frac{1}{b^p}a^p$, But we could have also interpreted the tautology $(a^p-b^p)+(b^p-c^p)+(c^p-a^p)$ in a similar way, for example divided by (b^p-c^p) and written

$$\frac{a^p-b^p}{b^p-c^p}+1 \equiv\ 0\ mod\ \frac{1}{b^p-c^p}(c^p-a^p).$$

The fibers over two different values of j are isomorphic, and in each there are two open covers, if we can check, are $a^p - b^p, b^p - c^p, c^p - a^p$ necessarily coprime?

A prime divisor of $a^p - b^p$ and $b^p - c^p$ (besides 3) will be a divisor of the difference, $-3b^p$. And then being a divisor of this and $a^p - b^p$ will be a divisor of a^p as well, which would be a contradiction.

There seems to be then a lot of symmetry, and we can make arguments about the differences just as we have for the sums.

What about whether the a^p, b^p, c^p are coprime to the differences? For example a^p is equal to $-b^p - c^p$, if it has a common divisor with $b^p - c^p$ then besides 2 it would with b^p, and whether a^p is coprime to $a^p - b^p$ it obviously is.

So this shows that we have six pairwise coprime entities, $a^p, b^p, c^p, a^p - b^p, b^p - c^p, c^p - a^p$. And we have an open cover of the fiber by six open sets. And a finer open cover where we invert all but one of the six quantities.

We can strengthen a result we just mentioned as follows:

Theorem. The restriction of $\mathcal{L}^{\otimes 2p}$ to the locus defined by $a^p b^p c^p (a^p - b^p)(b^p - c^p)(c^p - a^p)$ is a trivial line bundle spanned by $x^{2p} + y^{2p} + z^{2p}$

Proof The indicated locus is the union of the zero locus of s_3^2 and $-4s_2^3 - 27s_3^2$. Because either section together with s_2^3 spans $\mathcal{L}^6$ then it is true that s_2 spans the restriction of $\mathcal{L}^{\otimes 2p}$ to either locus separtely. It is always true that if a section t spans a line bundle $\mathcal{L}$ then $t^{\otimes m}$ spans $\mathcal{L}^{\otimes m}$ (the cokernel of the map from the structure sheaf is a tensor power of a zero module).

This proves that σ^2 or equialently $x^{2p} + y^{2p} + z^{2p}$ spans each part of the union of the two locii. However the locii are disjoint since, as we've just observed, $(abc)^p$ is coprime to $(a^p - b^p)(b^p - c^p)(c^p - a^p)$. Again recall well we are working over $\mathbf{Z} = \mathbb{Z}[1/(6p)]$ where 2 and 3

are invertible. QED

Corollary The locus defined by the different element of J has an open neighbourhood where $s_2(x^p, y^p, z^p)$ is nonzero.

Corollary Once we adjoin an inverse of $s_2(x^p, y^p, z^p)^2 = s_2(a^p, b^p, c^p)^2$ as a rationalnteger to $\mathbf{Z}$ the module $\mathcal{L}$ becomes free, and J becomes the coordinate ring of an affine neighbourhood of the support of the different element.

Note that $s_2(a^p, b^p, c^p) = -2(a^{2p} + b^{2p} + c^{2p})$.

Remark about an elliptic surface

We will not consider the elliptic surface in detail, let's just briefly outline things in a remark. It is possible to describe a scheme with more structure, if we adjoin variables w, v of degree $1, 2$ respectively and impose homogeneous equations $Aw^2+Bv = 0$, $s_1(e_1, e_2, e_3) = 0$, and $v^2 = w^4 + s_2(e_1, e_2, e_3)w^2 - s_3(e_1, e_2, e_3)w$, this describes the double cover of the projective plane branched over the lines $z = 0,\ z = e_1,\ z = e_2,\ z = e_3$ We can if we like think of this as an elliptic surface, the inverse image of the line in $\mathbb{P}^2$ where $[e_1 - e_3 : e_1 - e_2]$ is fixed, if we write this as $[\lambda : 1]$ is an elliptic curve with λ invariant $\frac{1-\lambda^2}{1-2\lambda}$ unless the line meets one of the six crossing points among the four lines. The different element aquires just one additional factor which is supported on the locus where e_1, e_2, e_3 satisfy the equations of the three cube roots of unity. We may delete that one j value and its fiber, and the resulting elliptic surface over $\mathbb{Z}$ maps to the Fermat fiber over j and has as its different element the same symmetric polynomial as we have already seen many times before, which has its vanishing locus defined by the same rational integer we have seen before. Note that when $s_1(x^p, y^p, z^p) = 0$ we have

$$s_2(x^p - y^p, y^p - z^p, z^p - x^p) = 3s_2(x^p, y^p, z^p)$$

We will not consider the elliptic surface here, but rather continue to look at the Fermat fiber, at the current moment we are still looking at it with the vanishing locus of $s_2(x^p, y^p, z^p)$ deleted, which is done merely by adjoining to our base ring $\mathbf{Z}$ the reciprocal of the rational

integer $a^{2p} + b^{2p} + c^{2p}$ or equivalently of $s_2(a^p, b^p, c^p)$.

The behaviour near the locus where $b^p = c^p$

Near the locus where $b^p = c^p$ the fiber over each λ value consists of just $p + 2$ isolated components. However, the rational component $Spec(\mathbf{Z})$ meets exactly one other component, and if we let J_S be the projection to the corresponding components of the normalization, it is spanned by monomials of degree a multiple of $6p$ in

$$\begin{array}{c} x = (a, a) \\ y = (b, c\omega) \\ z = (c, b\omega^{p-1}) \end{array} .$$

It contains the monomial

$$x^{6p-1}y = a^{6p-1}(b, c\omega)$$

and so it contains

$$(1, \frac{c}{b}\omega)$$

and also

$$(0, 1 - \frac{c}{b}\omega)$$

showing that modulo the corresponding maximal ideal Q of $\mathbb{Z}[\omega]$

$$\frac{b}{c} \equiv \omega \ mod \ Q.$$

If the prime q where Q meets $\mathbf{Z}$ is not a divisor of $b - c$ then necessarily $q \equiv \ 1 \ mod \ p$ and Q is totally split.

On the locus where $s_2 = 0$ we have that each rational component is connected to every component across a rotation, that is we look at $v = (0, i, j)$ an orbit rep, and

$$\begin{array}{c} x = (a, b) \\ y = (b, c\omega^i) \\ z = (c, a\omega^i) \end{array}$$

The element $(xyz)^{2p}$ is a homogeneous polynomial of degree $6p$ representing a unit times $(1, 1)$ and we may adjust the powers so we

have in J the differences such as $xy^{-1} = (ab^{-1}, bc^{-1}\omega^{-i})$ and multiplying by bc gives $(ac, b^2\omega^i)$. Now $(ac)^p - b^{2p}$ is congruent modulo s_2 to $-(ab)^p - (bc)^p - b^{2p}$ which is a unit times $-a^p - b^p - c^p$ thus this is congruent modulo s_2 to zero. It follows that if the ratio $\frac{ac}{b^2}$ is congruent to the root of unity ω^i modulo a prime of the cyclotomic integers the components will meet at that prime.

So that we have seen that a rational component meets a rational component correspnding to the identity permutation and meets components across a transposition fixing a at points lying over q a divisor of a which is a divisor of s_3, and across a transposition interchanging b, c at a prime divisor of $b^p - c^p$ which is a divisor of $-4s_2^3 - 27s_3^2$, and finally across a rotation at prime divisors of s_2. And we have seen how to index those components using p'th roots of unity.