Examples and simplifications related to the Fermat equation.

Contents.

I. Introduction

Let a, b, c be pairwise coprime integers and p an odd prime, and $a^p + b^p + c^p = 0$. What we will call the 'different element' is a particular element of a locally free module over the coordinate ring of the fiber in the Fermat curve over the rational j value corresponding to the numbers $a, b, c.$. That module embeds into the normalization of the coordinate ring of the fiber; the image of the different element in the normalization corresponds to a rational integer times a root of unity, and the rational integer, along with another rational integer for the fiber over a rational lambda value, provide a guide for how to assemble the components of the fiber, first putting together the components in the fiber over each of the six lambda value separately, and then attaching the partly-assembled pieces together to make the fiber over one j value. In each case, the rational integer indicates, on each irreducible component of the relevant fiber, the locus where that component meets the union of all the other components.

In general, once the discriminants of the irreducible components are inverted, a necessary and sufficient condition for a fiber to consist of smooth rational points of a curve is that the different element can be reduced to zero in an ambient resolution of singularities of the fiber. We obtain the different element by restricting a section of a line bundle of isomorphism type $\mathcal{O}(13p - 3)$ on the integer projective plane to an element of a locally free module over the coordinate ring of a fiber. The same one section of $\mathcal{O}(13p - 3)$ works for all fibers.

When the different element required fibers over separate rational λ values to intersect I first thought there was a contradiction; I'd expected only fiber and cusp components to meet. We now understand something else. The requirement of two generators in a finite residue algebra yields a tensor decomposition when their valuations are comparable, which is a residue of the pullback structure one would see analytically if such intersections were not empty, inconsistent with the differentials being locally principal.

The tensor indecomposability holds even if we do not assume that the Fermat equation is true, only that the fiber occurs in *some* smooth curve, and as we vary a, b, c over integers, we see that the non-reduced coordinate ring at the four-fold intersection point merges, the tensor decomposition disappears, when the valuation of a and of $b + c$ become incompatible, for the simple reason that in the finite residue algebra the order of nilpotency is finite, one or the other must be zero. This same finite order is present in the ordinary completion or in the local ring, because of Nakayama's lemma (an ordinary fact about radicals and ordered sets). When one of the generators shifts out of range, the tensor decomposition which would contradict the known smoothness for the Fermat curve and other curves degenerates, the tensor factors merge, and this then makes a place where a smooth rational point can come into existence.

1. Theorem. (under revision)

Preliminary results

We still assume $a^p + b^p + c^p = 0$ with a, b, c pairwise coprime and p an odd prime. Let q be a prime divisor of a, so the order $m = v_q(a) \geq 1$. from the formula $-a^p = b^p + c^p$ we have $1 + (c^{-1}b)^p$ is congruent to zero modulo q^{pm} where c^{-1} refers to the inverse of c modulo q^{pm}. Thus

$$(-c^{-1}b)^p \equiv 1 \ mod \ q^{p \cdot v_p(a)}.$$

and we arrive at $-c^{-1}b$ one of the (possibly trivial) p'th roots of unity modulo q^{mp}. The units modulo q^{mp} is cyclic when q is odd, and the p-primary component is the trivial group when $q = 2$ since p is odd. There are at most p p'th roots of unity in the group of units of the integers modulo q^{mp}, that is, there are p if $q \equiv 1 \ mod \ p$ and just 1 otherwise. If $p \neq q$ they can be described by first choosing any integer which represents a p'th root of unity modulo q and raising to a sufficiently high p'th power. There are two cases, still with $p \neq q$. If $-c^{-1}b \equiv 1 \ mod q^{p \cdot v_q(a)}$ then $q^{p \cdot v_q(a)}$, the highest power of q to divide a^p, is a divisor of $b + c$ and therefore q is not a divisor of the difference quotient $\frac{-a^p}{b+c} = \frac{b^p + c^p}{b+c} = b^{p-1} - cb^{p-2} ... + c^{p-1}$. This is consistent with what we see if we just use the congruence $b + c \equiv 0 \ mod \ q$ to replace c with $-b$ in the formula for the difference quotient, all terms are equal and we obtain $b^{p-1} + b^{p-1} + ... + b^{p-1} = pb^{p-1}$, the derivative of b^p with respect to p, which is indeed coprime to q since $q \neq p$ and $p|a$ which is coprime to b.

On the other hand, if $-c^{-1}b \not\equiv 1 \ mod q^{p \cdot v_q(a)}$ then q is not a divisor of $b+c$, and all of $q^{p \cdot v_q(a)}$ must be a divisor of the difference quotient $p^{p-1} - cb^{p-2} ... + c^{p-1}$.

Moreover then it must be a nontrivial p'th root of unity, this requires there to be nontrivial p'th roots of unity modulo $q^{pv_q(a)}$, equivalently modulo q, so $q \equiv 1 \ mod \ p$

When $q = p$ the p'th roots of unity in the units of the integers modulo $p^{p \cdot v_p(a)}$ are the cyclic group under multiplication generated by $(1+p)^{p \cdot v_p(a) - 1} \ mod \ p^{p \cdot v_p(a)}$. When $-c^{-1}b \equiv 1 \ mod \ p^{p \cdot v_p(a)}$ then again the full power of q divising into $-a^p = b^p + c^p$ also divides into $b + c$ so p is not a divisor of the difference quotient $b^{p-1} - cb^{p-2} ... + c^{p-1}$.

Now we see a little inconsistency, because now using $b + c \equiv 0 \ mod \ q^2$ and replacing c by $-b$ in the formula for the difference quotient again gives us pb^{p-1} the derivative, but the formula says the difference quotient *is* divisible by p, precisely the first power and not the second. The contradiction implies that we can remove this case: that when $q = p$ is a divisor of a it never happens that the root of unity $-c^{-1}b \ mod \ p^{p \cdot v_p(a)}$ is the trivial root of unity, but always nontrivial. When p is a divisor of a, the factorization of a^p into its greatest common divisor with $b + c$ and its greatest common divisor with $b^{p-1} - cb^{p-2} ... + c^{p-1}$ would never quite be be a division into a pair of coprime p'th powers. It would be when

p is not a divisor of a, with the prime divisors in the second factor required to be congruent to 1 modulo p, and for which the $p'th$ root of unity $-c^{-1}b \; mod \; q^{p \cdot v_q(a)}$ is a nontrivial p'th root of unity, and those primes q in the first factor allowed to have any congruence class $1, 2, 3, .., p-1$ modulo p being the ones for which the root of unity $-c^{-1}b \; mod \; q^{p \cdot v_q(a)}$ is the trivial root of unity.

But when the divisor q of a is congruent to 0 modulo p since $p \cdot v_p(a)$ is never equal to 1, the prime $q = p$ occurs on both sides of the factorization, exactly once in the second factor, and $p \cdot v_p(a) - 1$ times in the first factor, and the root of unity $-c^{-1}b \; mod \; p^{p \cdot v_p(a)}$ is never the trivial root of unity.

These facts merely restate the truth of the equation $a^p + b^p + c^p = 0$ when a, b, c are pairwise coprime and p odd reduced modulo a^p. The equation is equivalent, of course, to the more precise equation where we consider $= c^{=1}b^p = 1 - a^p$ modulo arbitrarily high powers of a, or in the completion of the integers at a, and also of course the same conditions apply after permuting a, b, c. In any case we will restate the weak version

2. Lemma. Let a, b, c be pairwise coprime and p an odd prime. The equation $a^p + b^p + c^p = 0$ implies that a^p factorizes into two parts, its greatest common divisor with $b + c$ and, if a is coprime to p, its greatest common divisor with the difference quotient $b^{p-1} - cb^{p-2} ... + c^p$, otherwise the second part is this divided by p. That is, each prime divisor q of a besides p occurs with multiplicity $p \cdot v_q(a)$ in one factor or the other. The factor p if it occurs, occurs with multiplicity 1 in the second factor and multiplicity $p \cdot v_p(a) - 1$ in the first. For $q \neq p$ the prime q belongs to the first factor if and only if the p'th root of unity $-c^{-1}b \; mod \; q^{p \cdot v_q(a)}$ is the trivial root of unity, and in the second factor if it is a primitive p'th root of unity. The primes q besides p which belong to the second factor are all congruent to 1 modulo p while the primes q besides p in the first factor can have any congruence class modulo p. If p is a divisor of a the root p'th root of unity $-c^{-1}b \; mod \; p^{p \cdot v_p(a)}$ is always a primitive p'th root of unity. The same conditions remain true under permuting a, b, c of course, and more precise conditions are true if one completes at a instead of just reducing modulo a^p.

Remark. For fixed p we can interpret the equation $x^p + y^p + z^p = 0$ as saying that on the locus where yz is invertible $1 + (y/z)^p = -z^{-p}x^p$ where $-z^{-p}$ is a unit, and we can lift $(-y/z)$ to a Teichmuller root of unity in the completion at x, or we can write

$$1 + (z/y)^p = -y^{-p}x^p$$

and lift $(-z/y)$ to the reciprocal Teichmuller unit. A more general equation in four variables $x^p + y^p + z^p + w(xyz)^p = 0$ and note whenever this has an integer solution so does the original equation, as $w = (x^p + y^p + z^p)/(xyz)^p$ has small absolute value. The more general equation just asserts $x^p + y^p + z^p \equiv 0 \; mod (xyz)^p$, and it is this which is equivalent to compatibility of the Teichmuller roots of unity.

Thus consistency of the Teichmuller roots of unity (the conclusion of Lemma 2) would imply the existence of an actual solution of $x^p + y^p + z^p = 0$.

Another way of saying this is, any proof of of the Fermat theorem implies that the assignment of Teichmuller roots of unity, which underlie the structure of the fiber over a lambda value and controls the tensor decompositions at meeting points of fiber components over different lambda values, actually is internally inconsistent in the fiber, and so the phenomenon of tensor decompositions which are residual of the analytic structure can be in a meta-mathematical sense 'proven' to be the reason why the theorem is true.

That word 'proven' can be made rigorous in the one easy step; a solution in the three separate completions, meaning, a solution of $x^p + y^p + z^p \equiv 0 \; mod(xyz)^p$ really does lift to a solution of the precise equation, therefore a strategy to 'homotop' the existing proof into one aims to establish that an inconsistency in the Teichmuller roots of unity implies the existence of a tensor decomposition at the intersection of components of two fibers over separate lambda values, cannot be defeated by someone saying, "yes, but an assignment of Teichmuller roots being inconsistent with there being no such tensor decomposition only produces *fake* solutions of the Fermat equation! Is there a Hasse principle completing this picture by converting fake solutions into actual Fermat olutions? The answer to this question is provably "yes" because of the archimedian magnitude of the integer w.

In the remainder of the paper we will continue to look at difference quotients. We will initially work in the integers with $2, 3, p$ inverted so that the only ramification we will encounter is due to intersections.

We will see that we will be able to re-deduce Lemma 2 only from indirect properties such as symmetry of the different element and smoothness of the Fermat curve.

Definitions

When we write $\mathbf{Z}$ this will mean the ring $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{p}]$. The ring $\mathbf{Z}[\omega]$ will denote $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{p}]$ also adjoined a primitive p'th root of unity ω.

We will be interested in finite index subrings of cartesian products $R \subset A_1 \times ... \times A_m$ where each A_i is a copy of either $\mathbf{Z}$ or $\mathbf{Z}[\omega]$. The trace dual of such a ring R (within the corresonding cartesian product of copies of $\mathbb{Q}$ and $\mathbb{Q}[\omega]$) will be called R' and the normalization, which is merely $A_1 \times ... \times A_m$, may be also called $\overline{R}$.

We will say that the *different ideal* of R is the set of $r \in R$ such that $rR' \in R$.

When we speak of a direct sum of two rings, these are considered to be rings with identity element, and the direct sum ring has as its identity element the

sum of the two separate identity elements for the subrings. Thus the inclusions and projections are not "homomorphisms of rings with identity element."

At times, we may be concerned with the cases when R has a locally principal differentials module, thus we sate

Definition. the differentials module of a ring R is the R-module generated by a symbol dr for each $r \in R$ with relations that $d(ab) = adb + bda$ for all pairs $a, b \in R$.

If $R \subset A_1 \times ... \times A_m$ is such a subring, for any subset $S \subset \{1, 2, .., .m\}$ we will abbreviate by A_S the same cartesian product in which the factors A_i for $i \notin S$ are just ignored. The image of R in A_S will be called *the projection of R into A_S* , it is a homomorphic image of R and we will denote it by the symbol R_S.

Orbit representatives

Here is a set of orbit representatives for the action of $\mathrm{Aff}(F_p)$ on F_p^3 which we will need later. These will be the elements

$$(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), ..., (0, 1, p-1).$$

These comprise all tuples for which the first entry is 0, the second entry is 0 or 1 and if the second entry is 0 the last entry is 0 or 1.

Using these, and choosing or remembering our primitive p'th root of unity $\omega \in \mathbf{Z}[\omega]$, we may make three particular elements of $\mathbf{Z} \times \mathbf{Z}[\omega]^{p+1}$ depending on numbers a, b, c, which we call

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

I hope that the pattern is clear, if we think of x, y, z as three rows of a matrix, each column consists of a, b, c with each term multiplied by the power of ω indicated by the entries of the corresponding three-tuple of elements of F_p, one for each of our choseen $\mathrm{Aff}(F_p)$ orbit representatives. In other words, if our orbit representatives are $v_1, ..., v_{p+2}$, our elements are

$$\begin{aligned} &(a\omega^{v_i(1)})_i \\ &(b\omega^{v_i(2)})_i \\ &(c\omega^{v_i(3)})_i \end{aligned}$$

.

Define Λ (the reason for the notation will become clear later), to be the subring of $\mathbf{Z} \times \mathbf{Z}[\omega]^{p+1}$ which is spanned as a $\mathbf{Z}$-module by all monomials in x, y, z whose total degree in x, y, z is a multiple of p.

The next algebra will describe is Λ^6, the cartesian product of six copies of Λ within $(\mathbf{Z} \times \mathbf{Z}[\omega])^{p+1})^6$. We will index the cartesian factors by the six elements of the symmetric group S_3 writing $\Lambda^6 = \prod_{\sigma \in S_3} \Lambda_\sigma$. Likewise we will index the factors in the normalization, where each factor is a copy of $A_1 \times ... \times A_{p+2}$, by the elements of S_3 in the same way, so when we write A_σ we are referring to a cartesian product of $p+2$ factors, the first a copy of $\mathbf{Z}$ and the others copies of $\mathbf{Z}[\omega]$, so we may write

$$\Lambda^6 = \prod_{\sigma \in S_3} \Lambda_\sigma \subset \prod_{\sigma \in S_3} A_\sigma.$$

Define J to be the subalgebra of Λ^6 spanned by all monomials of degree a multiple of $6p$ in the three six-tuples which we will call

$$X = (x, y, x, z, y, z)$$
$$Y = (y, x, z, y, z, y)$$
$$Z = (z, z, y, x, x, x)$$

The columns result by applying each of the six possible permutations of $\{x, y, z\}$ to the first column, therefore the rows are also described

$$X = (\sigma(x))_{\sigma \in S_3}$$
$$Y = (\sigma(y))_{\sigma \in S_3}$$
$$Z = (\sigma(z))_{\sigma \in S_3}$$

Note that Λ is just the sum of the six projections of J on six summands of its normalization.

Examples of components in a fiber

Let a, b, c now be any three pairwise coprime numbers, and p an odd prime number. We construct the corresponding coordinate ring Λ. of the fiber of the Fermat curve over the corresponding lambda value. $Spec(\Lambda)$ has 1 irreducible component which is a copy of $Spec(\mathbb{Z})$ and $p+1$ irreducible components which are copies of $Spec(\mathbb{Z}[\omega]$. The components are indexed by the following triples of elements of $\mathbf{F}_p^3$ which are orbit representatives for the $\mathrm{Aff}(F_p)$ action

$$(0,0,0), (0,0,1), (0,1,0), (0,1,1), (0,1,2), ..., (0,1,p-1).$$

Let q be a divisor of a. The tensor product of Λ over $\mathbb{Z}$ with the local ring $\mathbb{Z}_q$ of $\mathbb{Z}$ at q is a semilocalization. The corresponding semilocalization of the normalization is such that the first component is local and the others each have as many maximal ideals as the index in the units of $\mathbb{F}_p$ of the subgroup generated by $q \ mod \ p$. These maximal ideals in the localization of each component, direct sum the unit ideal of other components, comprise maximal ideals in the normalization $\overline{\Lambda}$, but they are allowed to coalesce when they are intersected with the subring Λ.

We will show that this semilocalization of Λ decomposes as a cartesian product of two rings, one is the projection on the first and fourth component, the other is the projection on the other components.

The first component corresponds to a copy of $Spec(\mathbb{Z}_q$ which has the prime residue field F_q. The corresponding maximal ideal in the fourth component must also be one with the prime residue field F_q therefore, however the fourth component is a semilocal ring allowed to have more than one maximal ideal.

We have been looking at $\Lambda = \Lambda_1$. When we look at the semilocalization at q of Λ_s for s the transposition fixing a, we will find that the components indexed by $(0,0,0),(0,1,1)$ there are disjoint from the corresponding components in $Spec(\Lambda_1)$ and do each meet all of the remaining $p-1$ components.

The different element

Let me preface this section by saying that there are many languages it could be written in, the language of bimodules, of dualizing sheaves, or of differential forms. The fact they are equivalent is explained in the Stacks project [3]. We will use the language of differential forms.

Here is what we will establish. Let $\mathcal{L}$ be the locally free J-module of rank one which consists of the values at the specific elements $X, Y, Z \in \overline{J}$ of all homogeneous polynomials of degree congruent to 1 modulo $6p$. The tensor power $\mathcal{L}^{\otimes i}$ depends only on the residue class of i modulo $6p$, and we may write $\mathcal{L}^{6p} = \mathcal{L}$ with an equality sign once we interpret the tensor power as representing polynomial multiplication.

In this section we'll consider a particular element of $d_J(X,Y,Z) \in \mathcal{L}^{\otimes(p-3)}$ which we've called the 'different element,' it is expressed as a particular homogeneous polynmial of degree $13p-3$ in X, Y, Z, and which is a restriction of a section of $\mathcal{O}(13p-3)$ on the integer projective plane which can be described by the same polynomial multiplied by, for example, $\frac{s}{X^{13p-3}}$ where s is a section of a line bundle with divisor of zeroes of degree $13p-3$ where $x=0$, so that the product is s times a rational function and the product is a section without poles.

We will also describe a rational integer. It will be the value at a, b, c of the polynomial $d_J(X,Y,Z)$ which we will call $d_J(a,b,c)$. The way they will be related is, there will be a root of unity $\alpha_J \in \overline{J}$ and the rational integer times a root of unity in the normalization, that is, the product $d_J(a,b,c)\alpha_J$ is equal to the image in the normalization of an embedded copy of the locally free module, such that the image of $d_J(X,Y,Z)$ under the embedding is $d_J(a,b,c)\alpha$.

We begin with the global picture.

Let $s_1 = X^p+Y^p+Z^p$, $s_2 = X^pY^p+Y^pZ^p+Z^pX^p$, $s_3 = X^pY^pZ^p$. To specialize the Frey j-invariant to a rational point we choose a matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sl_2(\mathbb{Z})$

and consider the residue of $d\ log\ \frac{A+Bj}{C+dj}$ on the Fermat curve $s_1 = 0$ restricted to the fiber where $A + Bj = 0$. We will arrive at the element $d_J(X, Y, Z) =$

$6(XYZ)^{p-1} \cdot p^2(X^pY^p - Y^pZ^p)(Y^pZ^p - Z^pX^p)(Z^pX^p - X^pY^p)(X^pY^p + Y^pZ^p + Z^pX^p)(X^pZ^p + Z^pY^p + Y^pX^p)$

of $\mathcal{L}^{\otimes(13p-3)} = \mathcal{L}^{\otimes(p-3)}$.

To relate this to the different ideal of J, we will apply E. Noether's notion of the different [1], in the context of multilinear algebra and projective geometry [2],[3]. The overall picture is this: if we had defined the Noether different ideal of the affine cone of the fiber, it would have been generated by a size three Jacobian determinant. The value of this is our homogeneous polynomial of degree $13p-3$. Associated to the homogeneous polynomial is a section of $\mathcal{O}(13p-3)$ on the integer projective plane. The scheme where the section meets the zero section is defined locally by a size two Jacobian determinant. Thus when the line bundle is trivialized on affine charts the zero scheme agrees with the Noether different of the fiber.

Here are our conventions about projective geometry and first principal parts. In projective geometry, considering differentials like dx and dy when you care about the ratio $[x : y]$ if you allow yourself to write $[x : y] = [1 : y/x]$ then there should be some way to make sense of $d1$ and $d(y/x)$.

The trick is to understand that you are on a line bundle, the disjoint union of the lines through the origin, and you can think of x and y as linear functionals on each *line*. You imagine, the coordinate ratio is telling you which line to look at, one of x or y is a nontrivial linear functional on that line. If f is a section of the dual bundle, it induces a functional on any one of the lines. Working locally, we consider df and also f times the differential of a coordinate specifyng which line we are on, such as y/x. So we consider df and $fd(y/x)$; For example, when we take $f = x$ we have dx and $x(xdy - ydx)/x^2$ which is dx and $dy - (y/x)dx$, and by a change of basis this is the same as dx and dy again.

It is said that the rational function y/x, which makes sense at every point of the integer projective line, is a 'nome.' If we interpret it as the ratio $[y : x]$ it is defining an isomorphism, but a question is, if we instead interpret y/x as an element of the quotient field of a function ring, or as a function with a simple pole, how can we identify that it is a nome? We can consider the differential $d(y/x)$ and this is nonzero wherever it is defined, but fails to make sense at one point. Crucially, if y, x are sections of a line bundle on some other manifold, giving a map to the projective line, how do we find the 'critical locus' which if there were no denominator would be the locus of zeroes of the pullback of $d(y/x)$?

The clearest way of answering this will be to say that the deRham differential d in exactly this setting extends to a connection ∇ with values in first principal parts, and we may rigorously write $d\ log\ (y/x) = \nabla\ log(y/x)$ and then follow this with

$$\nabla\ log(y/x) = \nabla\ log(y) - \nabla\ log(x)$$

Each of $\nabla(x)$ and $\nabla(y)$ is the rigorous manifestation of what earlier I called dx and dy, they are global sections of a rank two vector bundle over $\mathbb{P}^1$ which is the prinicpal parts bundle of $\mathcal{O}(1)$, and becauses principal parts is suitably functorial if $\mathcal{L}$ is the line bundle pullback of $\mathcal{O}(1)$ under the morphism underlying our rational function, whose domain is the complement of the indeterminacy locus, the same symbols describe the corresponding global sections of the rank two pullback vector bundle. This principal part is a rigorous and meaningful interpretation for what should be the residue of the logarithmic derivative, that is

$$y \cdot \nabla \ log(y) = \nabla(y)$$
$$x \cdot \nabla \ log(x) = \nabla(x)$$

The wedge product $\nabla(x) \wedge \nabla(y)$ is, up to sign, the unique generator for the second exterior power of the first principal parts of $\mathcal{O}(1)$ on the projective line, the global sections sheaf is a free module of rank one over the rational integers.

Next let's talk about a very general principle under which we can generalize the expression $xdy - ydx$ to higher dimensions and explain how it is related to logarithmic differential forms. First we work in affine space in three dimenisions. Here, consider

$$xdy \wedge dz - ydx \wedge dz + zdx \wedge dy$$

It is very interesting that the value of such an expression, as a differential form, is unaffected by multiplying each of x, y, z by the same differentiable function of x, y, z. For example in this case of three variables

$$(fx)d(fy) \wedge d(fz) - (fy)d(fx) \wedge d(fz) + fzd(fx) \wedge d(fy)$$

$$= f^3(xdy \wedge dz - ydx \wedge dz + zdx \wedge dy) + f^2(xzdy \wedge df + xydf \wedge dz - yzdx \wedge df - xydf \wedge dz + xzdf \wedge dy + yzdx \wedge df)$$

in which the second term is zero. We can use this differential n form – the contraction of $dx_0 \wedge ... \wedge dx_n$ along the vector-field $\sum x_i \frac{\partial}{\partial x_i}$ – to describe a global section of differential n-forms on projective space $\mathbb{P}^n$ tensored with a line bundle $\mathcal{O}(n+1)$. On $\mathbb{P}^2$, we may choose our function f to be $\frac{1}{x_0}$ so that the left side of the equation in the calculation above is

$$(fx)d(fy) \wedge d(fz) - (fy)d(fx) \wedge d(fz) + fzd(fx) \wedge d(fy) = d\frac{y}{x} \wedge d\frac{z}{x} - 0 + 0$$

and we have arrived at the standard volume two-form on the affine plane with coordinates $\frac{y}{x}, \frac{z}{x}$. The fact that the patching when we change from one of the standard coordiante charts to the other involves homogeneity of degree three explains why this is not describing a differential two-form, but a global section of the two-forms tensored by $\mathcal{O}(3)$.

We are going to give a better explanation of that standard form on affine space by pulling it back to the line bundle. First we need a tutorial about line bundles and vector bundles.

We can interpret line bundles two separate ways. To construct a line bundle we might call $\mathcal{O}(3)$ we first imagine that we have a line bundle $\mathcal{L}$ with a global section s whose divisor of zeroes is some curve or divisor, for example the divisor described by x^3. Then we may obtain other global sections by multiplying by rational functions which have poles no worse than the zeroes of x^3 so that the product will have no poles. These are the $\frac{1}{x^3}x^iy^jz^ks$ such that $i+j+k=3$ with $i,j,k \geq 0$. It is sometimes a convention to erase the symbol $\frac{1}{x^3}$ and the symbol s and to state that global sections of $\mathcal{O}(3)$ have as a basis the actual monomials $x^iy^jz^k$ for $i+j+k=3$, but this would be misleading and confusing.

Now that we are done with the tutorial about vector bundles, let's talk about logarithmic forms. We usually consider those differential one-forms on the total space V of a line bundle which are allowed logarithmic poles on the zero section E, and twisted by $-E$. These are the one-forms which restrict to zero on E in the forms sense, and when we restrict to E in the coherent sheaf sense we arrive at the first principal parts bundle of the dual line bundle $\mathcal{L}$. This is just copying what we have said already, if f is a nonzero section of the dual bundle $\mathcal{L}$, we have a local basis $df, fdx_1, ..., fdx_n$ We may consider one local section to be fixed, and imagine that $\nabla(f) = df + 0fdx_1 + ... + 0fdx_n$ is the deRham differential on the line bundle of f, which is our section of the dual bundle Then any other nonzero local section is a multiple gf and working on the total space of the line bundle $\nabla(fg) = d(fg) = gdf + \frac{\partial g}{\partial x_1}fdx_1 + ... + \frac{\partial g}{\partial x_n}fdx_n$. in the original basis. So the sequence of coordinates of the coherent sheaf restriction of dg is $(g, \frac{\partial g}{\partial x_1}, ..., \frac{\partial g}{\partial x_n})$. We are describing the firt principal parts sheaf – or vector bundle – of the dual line bundle, and except for questions of naturality it would be OK to say that it is spanned by formal direct sums $g \oplus dg$. Note also that we can formalize the rule above as the rule of a connection, $\nabla(gf) = g\nabla(f) + f \otimes dg$, section of $\mathcal{L} \otimes \Omega_{\mathbb{P}^2}$. where $\mathcal{L}$ is our dual line bundle.

Questions of naturality explain why we are not describing a direct sum bundle, but rather we are describing a vector bundle $\mathcal{P}(\mathcal{L})$ and an exact sequence $0 \to \Omega \otimes \mathcal{L} \to \mathcal{P}(\mathcal{L}) \to \mathcal{L} \to 0$. This sequence makes sense even on singular varieties, and remains exact if one reduces Ω and $\mathcal{P}(\mathcal{L})$ modulo torsion. It is the same as $(\mathcal{O} \otimes \mathcal{O})/I^2 \otimes \mathcal{L}$ with its coherent sheaf structure on the left, where $\mathcal{O}$ is the structure sheaf, and it can be geometrically understood as sections of $\mathcal{L}$ keeping track of an infinitesimal neighbourhood.

Just on general principles, the exact sequence shown above induces a long exact sequence involving exterior powers of $\mathcal{P}(\mathcal{L})$, but it makes more sense to go to the conceptual origin. If V is a line bundle and $\mathcal{L}$ its dual, the sheaf $\mathcal{O}(-E)$ on V pulls back to $\mathcal{L}$ itself, and as $\mathcal{O}(-E)\Omega_V(log(E))$ pulls back to $\mathcal{P}(\mathcal{L})$ the sheaf $\Omega_V(log(E))$ just pulls back to $\mathcal{L}^{\otimes(-1)} \otimes \mathcal{P}(\mathcal{L})$.

For the logarithmic differential forms of all degrees, contracting against the Euler derivation gives a long exact sequence of vector bundles on V

$$0 \to \Lambda^{r+1}\Omega_V(log\ E) \to \Lambda^r\Omega_V(log\ E) \to ,,, \to \mathcal{O}_V \to 0$$

This pulls back on the zero section E to a long exact sequence

$$0 \to \mathcal{L}^{\otimes(-r-1)} \otimes \Lambda^{r+1}\mathcal{P}(\mathcal{L}) \to \mathcal{L}^{\otimes(-r)} \otimes \Lambda^{r}\mathcal{P}(\mathcal{L}) \to ...$$

In the case when E is the projective plane and V is the disjoint union of the lines through the origin in three space, this becomes

$$\mathcal{O}(-3) \otimes \Lambda^3\mathcal{P}(\mathcal{O}(1)) \to \mathcal{O}(-2) \otimes \Lambda^2\mathcal{P}(\mathcal{O}(1)) \to ...$$

The sheaf $\mathcal{P}(\mathcal{O}(1))$ is just a trivial vector bundle of rank 3 with basis $\nabla(x), \nabla(y), \nabla(z)$. Tensoring with $\mathcal{O}(3)$ gives

$$0 \to \Lambda^3\mathcal{P}(\mathcal{O}(1)) \to \mathcal{O}(1) \otimes \Lambda^2\mathcal{P}(\mathcal{O}(1)) \to ...$$

I apologize if this was a lengthy development, it is something trivial. The sheaf on the left, $\Lambda^3\mathcal{P}(\mathcal{O}(1))$ is a trivial sheaf of rank one, it has a unique generating section up to sign which is $\nabla(x) \wedge \nabla(y) \wedge \nabla(z)$. So the first sheaf is

$$\Lambda^3\mathcal{P}(\mathcal{O}(1)) = \mathcal{O} \cdot \nabla(x) \wedge \nabla(y) \wedge \nabla(z).$$

When we wrote that form on affine space which is 'homogeneous' of degree three with respect to function multiplication, can now describe the phenomenon rigorously. The image of $\nabla(x) \wedge \nabla(y) \wedge \nabla(z)$ under the embedding shown is

$$x \otimes (\nabla(y) \wedge \nabla(z)) - y \otimes (\nabla(x) \wedge \nabla(z)) + z \otimes (\nabla(x) \wedge \nabla(y))$$

It spans the image of the first map from $\mathcal{O}$ in the exact sequence

$$\begin{aligned} 0 \to \mathcal{O} = \Lambda^3\mathcal{P}(\mathcal{O}(1)) &\to \mathcal{O}(1) \otimes \Lambda^2\mathcal{P}(\mathcal{O}(1)) \\ &\to \mathcal{O}(2) \otimes \Lambda^1\mathcal{P}(\mathcal{O}(1)) \to \mathcal{O}(3) \to 0 \end{aligned}$$

which comes from the action of contracting the exterior algebra on the differentials of the total space of $\mathcal{O}(-1)$ with log poles on the zero section along its Euler vector field, and tensoring with $\mathcal{O}(3)$. This global section is a natural image of the triple wedge product $\nabla(x) \wedge \nabla(y) \wedge \nabla(x)$ which bases $\Lambda^3\mathcal{P}(\mathcal{O}(1))$.

If we allow ourselves to write down *rational* sections of the prinicpal parts sheaf we can simplify this natural image section as

$$= xyz(\nabla\ log(y) \wedge \nabla\ log(z) - \nabla\ log(x) \wedge \nabla\ log(z) + \nabla\ log(y) \wedge \nabla\ log(z)).$$

Using the valid rules like

$$\nabla(x) = \nabla(y\frac{x}{y}) = \frac{x}{y}\nabla(y) + y \otimes d\frac{x}{y}$$

and so

$$\nabla\ log(x) = \frac{1}{x}\nabla(x) = \frac{1}{y}\nabla(y) + \frac{1}{(x/y)}d(x/y)$$

giving

$$d\ log\ (x/y) = \nabla\ log(x) - \nabla\ log(y).$$

Using this, our invariant expression can be rewritten without needing to use ∇, it is

$$(xyz)d\ log(y/x) \wedge d\ log(z/x)$$

and this expression is invariant under even permutations of the variables.

First let's include formal details of this, and then make it more rigorous. For the formal details, we have

$$xyz\nabla\ log(y/x) \wedge \nabla\ log(z/x) = xyz(\nabla\ log\ y - \nabla\ log\ x) \wedge (\nabla\ log\ z - \nabla\ log\ x)$$

$$= xyz(\frac{\nabla(y)}{y} - \frac{\nabla(x)}{x}) \wedge \frac{\nabla(z)}{z} - \frac{\nabla(x)}{x})$$

$$= (xz\nabla(y) - yz\nabla(x)) \wedge (\frac{\nabla(z)}{z} - \frac{\nabla(x)}{x}$$

$$= x\nabla(y) \wedge \nabla(z) - y\nabla(x) \wedge \nabla(z) - z\nabla(y) \wedge \nabla(x)$$

To be more rigorous we should rewrite xyz as a rational function like $\frac{yz}{x^2}$ times a section s of $\mathcal{O}(3)$ which takes a zero of order three on the hyperplane defined by x. So a more correct expression is

$$\frac{y}{x}\frac{z}{x}s \otimes d\ log\ \frac{y}{x} \wedge d\ log\ \frac{z}{x}.$$

As a sanity check, since we are talking about rational sections we are allowed to move the first two factors past the tensor sign and this just becomes

$$s \otimes d\frac{y}{x} \wedge d\frac{z}{x}$$

the tensor product with the most obvious two-form in coordinates y/x and z/x, with our section of the line bundle $\mathcal{O}(3)$.

This too can be totally explained. From the exact sequence $0 \to \mathcal{L} \otimes \Omega_E \to \mathcal{P}(\mathcal{L}) \to \mathcal{L} \to 0$ we obtain when E is dimension two

$$\Lambda^3\mathcal{P}(\mathcal{L}) \cong \mathcal{L} \otimes \Lambda^2(\mathcal{L} \otimes \Omega_E)$$
$$0 \to \Lambda^2(\mathcal{L} \otimes \Omega_E) \to \Lambda^2\mathcal{P}(\mathcal{L}) \to \mathcal{L} \otimes \Lambda^1(\mathcal{L} \otimes \Omega_E) \to 0$$
$$0 \to \Lambda^1(\mathcal{L} \otimes \Omega_E) \to \Lambda^1\mathcal{P}(\mathcal{L}) \to \mathcal{L} \otimes \Lambda^0(\mathcal{L} \otimes \Omega_E) \to 0$$

and tensoring each with the next higher power of $\mathcal{L}$ gives the short exact sequences which splice together to give the long exact sequence. Just splicing the first with the twist of the second gives

$$0 \to \Lambda^3\mathcal{P}(\mathcal{L}) \to \mathcal{L} \otimes \Lambda^2\mathcal{P}(\mathcal{L}) \to \mathcal{L}^{\otimes 3} \otimes \Omega_E \to 0.$$

On each local chart where we trivialize $\mathcal{L}$ this yields an actual presentation of Ω_E with generators pairwise wedge products of $\nabla(x), \nabla(y), \nabla(z)$ and with one relation which is the image of the triple wedge product $\nabla(x) \wedge \nabla(y) \wedge \nabla(z)$ under our map, which had been induced on logarithmic differentials by the Euler flow.

In our setting, we have a rational function given by the j invariant we wish to calculate the residue of $d\ log\ \frac{A+Bj}{C+dj}$ or, to remove some prejudice, let us say, $d\ log\ \frac{As_2^3+Bs_3^2}{Cs_2^3+Ds_3^2}$ at the locus of the Fermat curve where the numerator is zero and the denominator is 1, and where s_1, s_2, s_3 are the degree two and three elementary symmetric polynomials in X^p, Y^p, Z^p (the Fermat equation asserts $s_1 = 0$).

We had shown on the projective plane that when s is a section of $\mathcal{O}(3) = \mathcal{L}^{\otimes 3}$ which vanishes to degree three on the hyperplane defined by x, the expression

$$\frac{y}{x}\frac{z}{x}s \otimes d\ log\ \frac{y}{x} \wedge d\ log\ \frac{z}{x}.$$

describes a section of $\mathcal{L} \otimes \Lambda^2\mathcal{P}(\mathcal{L})$ which spans the kernel of the map to $\mathcal{L}^3 \otimes \Omega_E$ and here E is the integer projective plane.

Although it is not quite the right thing to do, if we just choose a homogeneous polynomial P of degree $5p$ in X, Y, Z then we can consider a rational map to $\mathbb{P}^2$ with the role of x being played by $Cs_2^3 + Ds_3^2$, the role of y being played by $As_2^3 + Bs_3^2$, the role of z being played by s_1P as all three have degree $6p$, and we arrive at

$$\frac{As_2^3 + Bs_3^2}{Cs_2^3 + Ds_3^2}\ \frac{s_1P}{Cs_2^3 + Ds_3^2}s \otimes d\ log(\frac{s_1P}{Cs_2^3 + Ds_3^2}) \wedge d\ log(\frac{As_2^3 + Bs_3^2}{Cs_2^3 + Ds_3^2})$$

Let us take some time to explain what this formula represents. To the left of the tensor sign, the symbol s is a global section of $\mathcal{O}(18p)$ and the rational functions multiplying it just mean the symbol to the left of the tensor sign is a rational section of $\mathcal{O}(18p)$ on the integer projective plane.

The symbols to the right of the tensor sign are a wedge product the differentials of two ordinary rational functions, thus a rational section of the two-forms, which we could if we wish interpret as a rational section of $\mathcal{O}(-3)$.

Because of the rule in affine space $d(s_1P) = s_1dP + Pds_1$ where we have $s_1 = 0$ the sheaf spanned by these sections for all choices of P is just $\mathcal{O}(5p)$ times the single section of $\mathcal{O}(13p-3)$ coming from the Jacobian matrix with P replaced by 1.

This means, the actual calculation which we want is the same as we have done, setting $P = 1$ and taking the determinant of the affine size three Jacobian determinant to obtain a homogeneous polynomial of degree $13p - 3$.

An easy way of remembering what that homogeneous polynomial is, if we had merely calculated the Noether different of the affine cone of a fiber over a j value, we would have obtained a homogeneous polynomial of degree $13p - 3$ as a generator, and it is this same homogeneous polynomial which, when viewed as a section of the line bundle $\mathcal{O}(13p-3)$, defines the different subscheme of the fiber by its intersection with the zero-section of that line bundle.

To be very clear, there are three ways of rewriting our vector bundle section. If we write it

$$\frac{As_2^3+Bs_3^2}{Cs_2^3+Ds_3^2}s\otimes d\frac{s_1P}{Cs_2^3+Ds_3^2}\wedge d\ log(\frac{As_2^3+Bs_3^2}{Cs_2^3+Ds_3^2})$$

we could view it as the residue of $d\ log\ j$ for a particular j value, restricted to the curve by wedging with the differential of its defining relation, and then tensored with our rational section.

If we write it

$$s\otimes d\frac{s_1P}{Cs_2^3+Ds_3^2}\wedge d\frac{As_2^3+Bs_3^2}{Cs_2^3+Ds_3^2}$$

and similarly on other coordinate charts, we see the Noether different tensored with the section s and with the ambient two-forms. This is what proves that the different section as we have defined it locally agrees with the Noether different.

For the analogous different element of the fiber over a λ value one can repeat the calculation but instead of the polynomials s_2 and s_3 just using X^p and Y^p.

We also need a tutorial about Noether's different. If a $\mathbf{Z}$-algebra R were built from generators ω_1,ω_2 and relators

$$\begin{cases} f(\omega_1,\omega_2)=0 \\ g(\omega_1,\omega_2)=0 \end{cases}$$

then we might repeat the construction, adjoining variables x_1,x_2 subject to the same relations, building $R\otimes_{\mathbf{Z}}R$. Then

$$0=f(x_1,x_2)-f(\omega_1,\omega_2)$$

$$=f(x_1,x_2)-f(\omega_1,x_2)+f(\omega_1,x_2)-f(\omega_1,\omega_2)$$

$$=\frac{f(x_1,x_2)-f(\omega_1,x_2)}{x_1-\omega_1}(x_1-\omega_1)+\frac{f(\omega_1,x_2)-f(\omega_1,\omega_2)}{x_2-\omega_2}(x_2-\omega_2)$$

and likewise

$$0=g(x_1,x_2)-g(\omega_1,\omega_2)$$

$$=\frac{g(x_1,x_2)-g(\omega_1,x_2)}{x_1-\omega_1}(x_1-\omega_1)+\frac{g(\omega_1,x_2)-g(\omega_1,\omega_2)}{x_2-\omega_2}(x_2-\omega_2)$$

Here, what are written as difference-quotient fractions should really be thought of as polynomials (and the same thing is familiar in analysis using Weierstrass preparation theorems) with a degree-one divisor removed. We obtain that the two-by-two matrix of difference quotients annihilates the column $(x_1-\omega_1,x_2-\omega_2)$, from the calculation of adjoint matrices its determinant annihilates the diagonal ideal I in $R\otimes R$, the kernel of multiplication $R\otimes R\to R$ which introduces the relations $x_i=\omega_i$. In general, Noether defines the different ideal to be the image in R of the annihilator of I, a special case being the determinant of a square Jacobian matrix of partial derivatives. We do not yet have this situation four our size three determinant, but the definition applies locally (this precise identity involving a size two determinant).

The relation between Noether's notion of different and the trace element is that the annihilator of $I \subset R \otimes R$ can be interpreted as bimodule homomorphisms $Hom(R, R \otimes R)$ and there is a general principle that bimodule maps from R to $Hom_{\mathbf{Z}}(A, B)$ for R modules A, B gives $Hom_R(A, B)$. Applying this to $A = Hom_{\mathbf{Z}}(R, \mathbf{Z})$ and $B = R$ gives that the annihilator of I is a copy of the R-module maps $Hom_{\mathbf{Z}}(R, \mathbf{Z}) \to R$, and the image in R is then the possible images of the trace element.

Note well that even though the principal parts module of the restriction of $\mathcal{O}(6p)$ to an affine coordinate chart already is of the form $R \otimes R$ tensored with the restricted module, Noether's reasoning about different quotients does not directly apply there, it needs to be generalized, but, in fact, one way to generalize it is to observe that the three-by-three determinant, when written in local coordinates, due to the magic we saw above, of how the Leibniz quotient rule interacts with the invariant differential form, becomes a two-by-two Jacobian determinant made of rational functions that happen to be defined near a point of interest when the line bundle is trivialized. The size three determinant really is the one which could have arisen, if we had wished to consider it, from the defining relations of the affine cone. Therefore, it is the messy local calculation immediately above which proves that Noether's different extends to principal parts.

Thus, let $\mathcal{L}$ be the subset of $\overline{J}$ consisting of all polynomials in the elements $X, Y, Z \in J$ whose degree is congruent to 1 modulo $6p$. It is locally free of rank one over J and each tensor power $\mathcal{L}^{\otimes i}$ can be identified with the polynomials in X, Y, Z of degree congruent to i modulo $6p$. Likewise let $\mathcal{N}$ be polynomials in $x, y, z \in \overline{\Lambda}$ of degree congruent to 1 modulo p. Let $d_\Lambda(x, y, z) = p^2(xyz)^{p-1} \in \mathcal{N}^{\otimes p-3}$ and $d_J(X, Y, Z) = p^2(XYZ)^{(p-1)} \cdot 6(X^pY^p - Y^pZ^p)(Y^pZ^p - Z^pX^p)(Z^pX^p - X^pY^p)(X^pY^p + Y^pZ^p + Z^pX^p)(Y^pX^p + Z^pY^p + X^pZ^p) \in \mathcal{L}^{\otimes(p-3)}$.

4. Theorem.

i) There is a root of unity $\alpha_J \in \overline{J}$ such that $d_J(X, Y, Z) = d_J(a, b, c)\alpha_J$ and where we define $d_J(a, b, c)$ to be the rational integer $d_J(a, b, c) = p^2(abc)^{p-1} \cdot 6(a^pb^p - a^pc^p)(b^pc^p - b^pa^p)(c^pb^p - c^pa^p)(a^pb^p + b^pc^p + c^pa^p)(b^pa^p + c^pb^p + a^pc^p)$.

ii) Assuming $a^p + b^p + c^p = 0$, the different ideal of the algebra J is $\mathcal{L}^{\otimes(4p+3)} d_J(X, Y, Z)$. Explicitly it is polynomials in $X, Y, Z \in \overline{J}$ which are simultaneously multiples of $d_J(X, Y, Z)$ and degree a multiple of $6p$.

iii) There is a root of unity $\alpha_\Lambda \in \overline{J}$ such that $d_\Lambda(x, y, z) = d_\Lambda(a, b, c)\alpha_\Lambda$ and where we define $d_\Lambda(a, b, c)$ to be the rational integer $d_\Lambda(a, b, c) = p^2(abc)^{p-1}$

iv) The different ideal of the algebra Λ is $\mathcal{M}^{\otimes 3} d_\Lambda(x, y, z)$. Explicitly it is polynomials in $x, y, z \in \overline{\Lambda}$ which are simultaneously multiples of $d_\Lambda(x, y, z)$ and degree a multiple of p.

v) Also, the index of each relevant algebra R in its trace dual R' is the square of its index in its normalization $\overline{R}$, so the rational integer d_R in each case is given

$$d_R = [R' : R]^{\frac{1}{rank_{\mathbf{Z}^{(R)}}}} = [\overline{R} : R]^{\frac{2}{rank_{\mathbf{Z}^{(R)}}}}.$$

Proof. We have already seen that the different element is an element of the module $\mathcal{L}^{\otimes(p-3)}$ Before specializing it was possible to identify the different element after locally trivializing a line bundle with the Noether different. Therefore the differentials module is $\mathcal{L}^{p-3}$ modulo the span of the different element, tensored with $\mathcal{L}^{3-p}$.

By wedging the logarithmic form $d\ log\ \ j$ with the differential of the defining equation of the fermat curve we were restricting it correctly, and the "different element" in $\mathcal{O}(13p-3)$ was describing the residue. Now in the end we are just calculating the Kahler differentials of each coordinate chart of the fiber in a standard way. Although we needed to insert and then remove the polynomial P and keep track of twisting (as we did not do very well in the end anyway).

The same considerations apply to the module $\mathcal{M}$ and the algebra Λ.

Using part v) to calculate $d_J(a,b,c)$ would requires a significant note of caution. The legitimacy of the calculation relies on the assumption that $a^p+b^p+c^p=0$. Hence we can never actually apply the index formula above $d_J(a,b,c) = [\overline{J} : J]^{\frac{1}{rank(R)}}$ to evaluate $d_J(a,b,c)$ explicitly unless we could find such numbers a,b,c. Here is an example using the formula with $p=1$ (which is not a prime). Take $a=5, b=7, c=-12$, adding to zero. The index is the $6/2$ (=half the rank) power of $2^3\cdot 3\cdot 5\cdot 7\cdot 17\cdot 19\cdot 109^2$, which is identical to $(abc)^{p-1}\cdot(a^pc^p - b^pc^p)(b^pa^p - c^pa^p)(c^pb^p - a^pb^p)(a^pb^p+b^pc^p+a^pc^p)^2$ (for some reason the leading coefficient of 6 is missing, but it is invertible since we work in $\mathbf{Z}$ now, not $\mathbb{Z}$). Once we repeat for $a=3, b=-9, c=5$ adding to -1 the index is the $6/2$ power of $2^4\cdot 3\cdot 7$, not even divisible by 5. The reappearance of of factors when the sum becomes zero forbids a direct sum decomposition of the residue algebra we will look at later when the symmetrical different applies, as part of the expression factorizes $...(abc)^{p-1}\cdot(a^pc^p - b^pc^p)... = ...(abc)^{p-1}\cdot c^p(a^p-b^p)...$ with a factor of c on both sides of the dot. When it is direct-sum indecomposable we will pass to considering tensor decompositions.

Returning to generalities, in scheme language, when the different ideal of such an algebra R as we are discussing generates the same ideal in the normalization as an element of $\mathbf{Z}$, the implies that the same element of $\mathbf{Z}$ defines on each irreducible component of $Spec(R)$ the locus where that component meets the union of all the other components. We have allowed $2,3,p$ to have inverses in $\mathbf{Z}$ to ensure that no ramification occurs in normalizing any component, that is why the different element can correctly describe intersections. But we must be careful. The relation on components of meeting in the semilocalization at a rational prime is not an equivalence relation.

Let us state just one direction of this bi-implication carefully and precisely, including making a choice of a prime ideal in $\mathbb{Z}[\omega]$.

5. Theorem. Let $q \in \mathbf{Z}$ be a prime divisor of $d_\Lambda(a,b,c)$. Then for every $i \in \{1,...,p+2\}$ there is a two element subset subset $S = \{i,j\} \subset \{1,2,...,p+2\}$ including i and a prime ideal Q of Λ_S containing q times the identity element, such that, denoting by $\Lambda_{S,Q}$ the corresponding local ring, and $\Lambda_{\{i\},Q}$ and $\Lambda_{\{j\},Q}$ the corresponding projections to components of the corresponding semilocalization of the normalization (or components of the total fraction ring of the normalization as one may wish), $\frac{[\overline{\Lambda}_{S,Q}:\Lambda_{S,Q}]}{[\overline{\Lambda}_{\{i\},Q}:\Lambda_{\{i\},Q}]\cdot[\overline{\Lambda}_{\{j\},Q}:\Lambda_{\{j\},Q}]}$ is divisible by q. Likewise let q instead be a prime divisor of $d_J(a,b,c)$. Then for every $j \in S_3 \times \{1,...,p+2\}$ there is a two-element subset $S = \{j,k\} \subset S_3 \times \{1,2,...,p+2\}$ including j and a prime ideal Q of J containing the identity time q, such that the index quotient $\frac{[\overline{\Lambda}_{S,Q}:J_{S,Q}]}{[\overline{\Lambda}_{\{j\},Q}:J_{\{j\},Q}]\cdot[\overline{\Lambda}_{\{k\},Q}:J_{\{k\},Q}]}$ is divisible by q

Recall where we are, the numbers $1,2,...,p+2$ index orbit representatives for the action of $\mathrm{Aff}(F_p)$ on F_p^3 with the number 1 indexing $(0,0,0)$.

Applying this principle, and the invariance of the rational integer associated to the different element in $\mathbf{Z}$ under direct sum and summand, one has this corollary.

6. Corollary. Let $q \in \mathbf{Z}$ be a prime element which is a divisor of abc. Suppose the different element of Λ and J are as we described. Then there is a four-element subset $S \subset S_3 \times \{1,2,..,.p+2)\}$ and a prime ideal Q of J_S with $S = \{(1,1),(1,j),(\sigma,k),(\sigma,l)\}$ with the permutation σ satisfying $\sigma \neq 1$, and with i,j,k,l satisfying $j \neq 1, k \neq l$, such that for every two-element subset $T = \{\alpha,\beta\} \subset S$ the index quotient $\frac{[\overline{J}_{T,Q}:J_{T,Q}]}{[\overline{J}_{\{\alpha\},Q}:J_{\{\alpha\},Q}]\cdot[\overline{J}_{\{\beta\},Q}:J_{\{\beta\},Q}]}$ is divisible by q.

Proof. First let's give a scheme-theoretic proof. $Spec(J)$ is a union of six schemes each with $(p+2)$ irreducible components, one copy of $Spec(\mathbb{Z})$ and $p+1$ homomorphic images of copies of $Spec(\mathbb{Z}[\omega]$. $Spec(\Lambda^6)$ is the abstract disjoint union of those six schemes. Choose any prime ideal of $A_{1,1}$ containing q and let Q denote its inverse image in $\Lambda = \Lambda_1$. We may assume by permuting a,b,c that $q|a$. The rational integer $d_\Lambda(a,b,c)$ describes the locus on each component of $Spec(\Lambda)$ where that component meets the union of the remaining components. Since q times the identity element of Λ belongs to Q there must be at least one other component among the images of $Spec(A_{1,2}),...,Spec(A_{1,p+2})$ whose image meets $Spec(\Lambda_1)$ at the point corresponding to Q. So there is a j such that the image of A_j contains the point Q. Consider the image in $Spec(\Lambda)$ of the disjoint union of $Spec(A_{1,1}$ and $Spec(A_{1,j})$ The coordinate ring of the union is the image of the projection of all of Λ_1 on two factors, which is the same as the projection of J on the same two factors, it is $((\Lambda_1)_{\{(1,1),(1,j)\}} = J_{\{(1,1),(1,j)\}}$ The local ring of this ring corresponding to our prime ideal Q is just the image of of the local ring $\Lambda_Q = \Lambda_{1,Q}$ in either the semilocalization or total fraction

ring of the normalization projected to the same two components. We may call this $\Lambda_{\{1,1,1,j\},Q}$. The index of the localized ring in its normalization, which is incidentally just $A_{(1,1),Q} \times A_{(1,j),Q}$ is divisible by q just because it is not an isomorphism, the local ring is not normal since it is not irreducible. (We could use the symbol J or Λ_1 or Λ interchangeably since we the projection of J onto two factors of the normalization of $\Lambda = \Lambda_1$ factors through the projection of J in Λ_1 itself.) Next, if all the irreducible components of J which are incident to $Spec(A_{1,1})$ at Q belong to the image of $Spec(\Lambda_1)$ then they are in the image of a part of the disjoint union which would map isomorphically in a neighbourhood of the intersection point, and the rational integers $d_J(a,b,c)$ and $d_\Lambda(a,b,c)$ associated to the different elements, being an invariant of the isomorphism types of the coordinate rings, would be agree as elements of $\mathbb{Z}$ localized at q. But this is not the case, a higher power of q is a divisor of $d_J(a,b,c)$. Therefore some projection $J_{\{(1,1),(\sigma,k)\}}$ has index in its normalization divisible by q, and this produces our permutation σ. Now we work within Λ_σ and repeat the earlier steps which we did when we were talking about Λ_1, to produce a (σ, l) such that $J_{\{(\sigma,k),(\sigma_l)\}}$ has index in its normalization divisible by q. We have produced our four element set S and verified a relation between pairs whose transitive closure is all of S. Since one of the components is rational ($\mathbf{Z}$) the inverse image of the maximal ideal defined by q is a maximal ideal of J with residue field the prime field F_q, and the relation in question is merely the equality of the intersection of the maximal ideal with J. This is a transitive relation, so all other pairwise projections coming from other two-element subsets of S must have index in their normalization divisible by q. Note that for components whose normalization is isomorphic to $\mathbf{Z}[\omega]$, even while the normalization can have more than one maximal ideal containing q, this is not so for J itself.

9. Remark. If J occurs as the coordinate ring of an affine subscheme of a curve whose localization at $6p$ is smooth (such as a Fermat curve), the ring J and also hence its homomorphic image which we are considering here must have locally principal differentials module. This is an extremely restrictive condition; it imples that the indecomposable local ring of order q^{2p} with residue field F_q produced by the theorem must be tensor indecomposable, so isomorphic to $F_q[T]/(T^{2p})$. We will give examples at the end where a choice of a, b, c not satisfying the Fermat equation has the expected tensor decomposition – thus detectably inconsistent with the Fermat equation – but where the tensor factors merge into one once the q-adic valuation of $b + c$ is allowed to be much larger than that of a.

Direct-sum decomposition

The previous results use the different element to establish a hypothesis, and that is exactly the hypothesis of the next theorem.

10. Theorem. Let p be a prime number, let ω be a primitive p'th roof of unity. Let a, b, c be pairwise coprime, let $q|a$ be prime divisor of a with $q \neq 2, 3, p$.

Choose the set H of orbit representatives of $\mathrm{Aff}(F_p)$ acting on F_p^3 such that the first coordinate is zero, the second coordinate is 0 or 1 and if the second coordinate is 0 the third coordinate is 0 or 1. Let s be a permutation of a,b,c. Let v_0, v_1, v_2, v_3 be elements of our orbit representative set $H \subset F_p^3$ such that $v_0 = (0,0,0)$, $v_1 \neq v_0$, and $v_3 \neq v_2$. Consider the subring of $Z[w]^4$ spanned by all homogeneous polynomials of degree a multiple of $6p$ in the three elements

$$x = (aw^{v_0[0]}, aw^{v_1[0]}, s(a)w^{v_2[0]}, s(a)w^{v_3[0]})$$
$$y = (bw^{v_0[1]}, bw^{v_1[1]}, s(b)w^{v_2[1]}, s(b)w^{v_3[1]})$$
$$z = (cw^{v_0[2]}, cw^{v_1[2]}, s(c)w^{v_2[2]}, s(c)w^{v_3[2]})$$

It has rank k where k is the number of i such that $v_i = (0,0,0)$ plus $p-1$ times the number of i such that $v_i \neq (0,0,0)$. Choose a prime divisor q of a in $\mathbf{Z}$ and localize our algebra at a prime ideal Q containing q times the identity element. Suppose that the corresponding projection on the corresponding semilocalization of the first two components in the normalization is direct-sum indecomposable (corresponding to the corresponding components meeting at Q in the fiber over one λ element), and suppose also that the projection on corresponding semilocalization of the normalization of the last two comments is direct-sum indecomposable (corresponding to two components meeting at Q in the fiber over another λ value). Suppose now that the local ring is direct-sum indecomposable (by transitivity which holds since we are talking about a local ring, (this could be established by showing one commponent of the first two meets one commponent of the second two at Q)

Then necessarily s is the transposition

$$s(a) = a$$
$$s(b) = c$$
$$s(c) = b$$

. Also, after interchanging v_2 and v_3 if necessary, there is a $j \in \{1, 2, .., p-1\}$ such that

$$v_0 = (0,0,0)$$
$$v_1 = (0,1,1)$$
$$v_2 = (0,0,1)$$
$$v_3 = (0,1,j)$$
$$b^2 \equiv c^2\omega \ mod\ Q$$

Proof. In the case when $s(a) \neq a$, we may assume by interchanging labels that $s(a) = b$. Then $x^{6p} = (a^{6p}, a^{6p}, b^{6p}, b^{6p}) \in J$ This has two components which are units and two which are divisible by q times the identity so belong to Q. The reduction modulo Q of this together with the identity span an F_q algebra which is at least two dimensional, but the residue field of Q is just F_q so the algebra could not be direct sum indecomposable.

We turn to the more difficult case when $s(a) = a$. Our choice $v_0 = (0, 0, 0)$ ensured that the residue field we are considering is the prime field F_q. This means that when we consider our algebra, a localization at one prime ideal Q of the set of polynomials in x, y, z homogeneous of degree a multiple of $6p$ where x, y, z are the particular elements of the normalization shown above, the residue field is the prime field, and the reduction of the first coordinate modulo q gives a consistent way to evaluate the residue class of any such polynomial modulo Q. Those which evaluate to 0 are the ones which belong to Q. By contrast, the actual multiples of q in our subring are represented by those polynomials $P(x, y, z)$ of degree a multiple of $6p$ which have only the weaker condition that all coefficients are divisible by q.

Any polynomial divisible by x (as a polynomial, recall x is not an element of our subring) does belong to Q since the first coordinate of x is a which is divisible by q. Next consider polynomials not involving x, the $P(y, z)$ which are homogeneous of degree a multiple of $6p$ as expressions in the variables y and z. We know y and z as elements of $\overline{J}$ are of the form

$$y = (b, b\omega^q, c\omega^r, c\omega^s)$$

$$z = (c, c\omega^t, b\omega^u, b\omega^v).$$

Consider the particular monomial of degree $6p$ which is $y^{3p-1}z^{3p+1} = b^{3p-1}c^{3p-1}(c^2, c^2\omega^{t-q}, b^2\omega^{r-u}, b^2\omega^{s-v})$. Now, b and c are invertible in our local ring which then includes

$$(1, \omega^{t-q}, b^2c^{-2}\omega^{r-u}, b^2c^{-2}\omega^{s-v})$$

Unless $t \equiv q \ mod \ p$ the projection on the first two factors has a direct sum decomposition. We can see that by exhibiting the first two entries of x, y, z

$$(a, a)$$
$$(b, b\omega^q)$$
$$(c, c\omega^t)$$

We may take q, t to be the last two entries in any one of our orbit representatives besides of $(0, 0, 0)$ which occurs already in the first column. If we choose any but $(0, 1, 1)$ we have $q \not\equiv t \ mod \ p$ and the monomials of degree 1 and $6p$ include

$$(b^ic^j, b^ic^j\omega^{qi+tj}) = b^ic^j(1, \omega^{qi+tj})$$

for $i + j = 6p$ and $(1, 1)$. Since b, c are coprime to q the span of these if we invert b, c in our base ring $\mathbf{Z}$ is the same as the span of

$$(1, \omega^{qi+tj})$$

Thus we have $(1, \omega^j)$ for all j, the sum of these for $j = 0, 1, ..., p-1$ is $(p, 0) = p(1, 0)$ and recall p is invertible so we obtain $(1, 0)$. Then we obtain all $(0, \omega^j)$.

Thus the only possibility for the second column is the orbit representative $(0, 1, 1)$.

Our ring is now spanned by monomials multiples of $6p$ in

$$\begin{array}{c} x = (a, a, a, a) \\ y = (b, b\omega, c\omega^u, c\omega^v) \\ z = (c, c\omega, b\omega^r, b\omega^s) \end{array}.$$

From the monomial $y^{3p+1}z^{3p-1}$ after dividing by $(bc)^{3p+1}$ as we may, assuming b, c invertible, we are obtain as an element of our subring

$$(1, 1, c^2b^{-2}\omega^{r-u}, c^2b^{-2}\omega^{s-v}).$$

Subtracting $(1, 1, 1, 1)$ gives

$$(0, 0, c^2b^{-2}\omega^{r-u} - 1, c^2b^{-2}\omega^{s-v} - 1).$$

Now localize our algebra at a maximal ideal Q containing q times the identity element $(1, 1, 1, 1)$ to obtain a local ring. Unless all four entries belong to the maximal ideal Q some entries will be invertible and others zero, splitting the algebra. This requires then that $r - u = s - v$ and $\omega^{r-u} \equiv c^{-2}b^2 \; mod \; Q$. where the expression c^{-2} refers to the inverse of c mod q.

After replacing the third component by its AffF_p representative we obtain up to interchanging v_2 and v_3 is the claimed pattern. QED

11. Example. If we take a, b, c, p, q to be $13, 7, 3, 5, 11$ we obtain an algebra of rank 13 and index $3^4 \cdot 5^2 \cdot 7^6 \cdot 11^{16} \cdot 41^2 \cdot 101^2$ in its normalization. The reduction modulo 11 is direct sum decomposable of dimension 13 over $\mathbb{F}_{11}$. If we instead build the subring of $\mathbb{Z}^4$ where we have substituted ω with 37107 in the three rows, the reduction of the subalgebra modulo q times its identity element is an indecomposable algebra of rank four but with radical whose third power is zero, which is therefore tensor-decomposable by our definitions. The way we chose the number 37107 is to take $c^2b^{-2} \equiv 4 \; mod 11$ and raise it to a high power of 11, and reduce modulo a high power of 11 to obtain the corresponding Teichmuller representative.

In some sense, it seems the tensor decomposability of the algebra is merely encoding that in attempting to solve the Fermat equation, 11^5 is not really a divisor of $3^5 + 7^5$.

Tensor decomposition

I should clarify, when I speak of a tensor decomposition of an algebra A over a field F, I mean a surjecive homomorphism $B \otimes_F C \to A$ in which neither the composition with $A \otimes F \to A \otimes B$ nor with $F \otimes B \to A \otimes B$ is surjective.

Let's make a deformation construction. Consider the algebra which we were already looking at, the subring of $\mathbb{Z} \times \mathbb{Z}[\omega]^3$ spanned by monomials of degree multiples of $6p$ in

$$x = (a, a, a, a)$$
$$y = (b, b\omega, c, c\omega)$$
$$z = (c, c\omega, c\omega, c\omega^2)$$

We might as well revert to calling this J_S for S the appropriate four-element subset of $S_3 \times \{1, 2, ..., p+2\}$. A generalization of this is the sub-algebra of the polynomial algebra $\mathbf{Z}[T]^4$ generated by polynomials of degree multiples of $6p$ in the elements

$$x = (a, a, a, a)$$
$$y = (b, bT, c, cT) \quad .$$
$$z = (c, cT, cT, cT^j)$$

Another specialization of the general algebra occurs if we apply the homomorphism of $\mathbb{Z}[T]^4 \to \mathbb{Z}^4$ which on each component is the map $\mathbf{Z}[T] \to \mathbf{Z}$ sending T to an integer representative of $c^2 b^{-2}$ *mod* q, under our assumptions of direct sum indecomposability this will reduce to a primitive p'th root of unity in $\mathbf{F}_q$, and we may choose the integer representative to reduce to a p'th root of unity modulo a successively higher power of q by raising it to the p'th power repeatedly.

If we apply instead the homomorphism $\mathbb{Z}[T] \to \mathbf{Z}[\omega]$ on each component sending T to ω we'll recover our algebra.

Next, we reduce our subalgebra of $\mathbf{Z}^4$ modulo the ideal *in the subring* generated by q times the identity element. The result will always be an $\mathbf{F}_q$-algebra of dimension four.

I claim that this algebra of dimension four is a homomorphic image of the localization of J_S at Q.

A conventional way of arguing, instead of using $\mathbf{Z}[T]$, would be to embed $\mathbf{Z}[\omega]$ into the completion of $\mathbf{Z}$ at q. Under our assumptions of direct sum indecomposability we do have that $q \equiv 1$ *mod* p so this is possible.

In any case, we may find a sufficiently high power of (q, q, q, q) in $\mathbf{Z}^4$ such that the ideal generated in $\mathbf{Z}^4$ by that power (q^N, q^N, q^N, q^N) is contained in the ideal in the subring generated by the first power (q, q, q, q), and therefore we may obtain the same $\mathbf{F}_q$ algebra at the end if we first tensor $\mathbf{Z}^4$ over $\mathbf{Z}$ with $\mathbf{Z}/(q^N\mathbf{Z})$. For example, by the Artin-Rees theorem. When we do that, we see that ω has been correctly specialized to a primitive p'th root of unity in each factor anyway.

12. Theorem. Let a, b, c be coprime integers and p an odd prime. If any divisor q of a besides $2, 3, p$ is not a divisor of $b + c$ and the subalgebra of $\mathbb{Z}^4$ described above, reduced modulo its own element q, is tensor decomposable (as it indeed is in many examples) then $a^p + b^p + c^p \neq 0$.

Proof. This may be an elementary property of the structure of the algebra, but it is easiest to prove by combining things we know. The algebra is not even direct sum indecomposable unless ω is congruent to $b^{-2}c^2$ modulo Q in $\mathbf{Z}[\omega]$, this implies that q is a divisor of the difference quotient $b^{p-1} - cb^{p-2} ... + c^{p-1}$. The comparison of the rational integer $d_\Lambda(a,b,c)$ coming from the different element of the disjoint union of the fibers over the λ lying over j and the rational integer $d_J(a,b,c)$ coming from the full fiber showed that there must be such an indecomposable configuration of four components such as this, even while localized at a particular prime ideal Q containing q, and we showed in the previous theorem that this is the essentially unique way it could happen. But any such local algebra must have locally principal differentials module (recall we inverted $1/6p$), and this forces the maximal ideal in our local algebra to become principal when the algebra is reduced modulo q. QED

Remark. Tensor indecomposability of the reduction modulo q of such examplesis equivalent to the condition that for all α, β in our F_q algebra which do not reduce to zero, α is a divisor of β in the F_q algebra if and only if $v_m(\alpha) < v_m(\beta)$.

We already know from the preliminary section that if the Fermat equation were true, once $v_q(b^{p-1} - cb^{p-2} ... + c^{p-1})$ is nonzero, as long as $q \neq p$, the valuation must take the value $p \cdot v_q(a)$. It is interesting to consider the remark above taking α to be a monomial of degree $6p$ in x, y, z which is divisible only by the first power of x, and to take β to be $(y - z)$ times a monomial of degree $6p$. It seems likely that the comparison critereon above about anti-symmetry of valuation comparisons would allow a person to re-deduce the fact that the order at q of the difference quotient cannot take any intermediate value between 0 and $pv_q(a)$ just from the previous remark, depending therefore only on smoothness of the Fermat curve (with p inverted) and the symmetry of the different element.

Examples

14. Example. We already know that this type of example will be inconsistent with the Fermat equation anyway, but it is interesting to see what happens with actual numbers a, b, c which – by necessity of our choices – do not satisfy the Fermat equation. To find an example where the F_q algebra is tensor indecomposable, we avoid the condition in Theorem 13, thus let's take $b + c$ divisible by a high power of q, so we take $a = 3, b = 19, c = 59030, p = 5, q = 3$ obtaining a rank 10 subring of index 52851989777827347726236832454215866380455969825 in its normalization whose reduction modulo q is neither direct-sum decomposable nor tensor indecomposable. Perhaps this example can exist because $b + c = a^{2p}$, and so $(y + z)y^{6p-1}$ exceeds the nilpotency degree of the algebra and cannot be a generator. To see this example calculated click here.

The clear situation is this: in analysis the fiber over a j value is a pullback, and smooth local analytic rings are topologically monogenic, while fibers over

distinct lambda values do not meet. In algebra, the different element says the fibers meet at closed points, and differential calculus still holds that the residue rings over $Spec(Z)$ must be literally monogenic. In cases when the order of a and $b+c$ at a prime q are comparable, a sort of analytic pullback structure peeks in, a pair of generators is needed. But algebraic local rings at pullback points have a tensor decomposition, here we expected a tensor decomposition and found there is, two generators are needed. Yet, the order of nilpotency of a finite algebra is also finite, and we can shift one or the other generator out of existence by making the order at q of a and $b+c$ incomparable. Although the order of nilpotency is $2p$, for some reason we cannot prove decomposability when the valuation of one element is even p times that of the other.

15. Comment. Our analysis in Corollary 3 involving the factorization of b^p+c^p breaks down in the case $p=2$. Theorem 13 refers to q-adic order in $\mathbf{Z}$ where 2 is invertible. I do not know if it is possible to prove that $x^2+y^2+z^2$ cannot be zero for x,y,z not all zero, without attaching signs to real values. Hilbert attached signs algebraically for example, to the odd number -135, by considering the indecomposable sumamnds of $\mathbf{Z}/((-135)\mathbf{Z}) \cong \mathbf{Z}/(5\mathbf{Z}) \oplus \mathbf{Z}/(27\mathbf{Z})$. He reduced the orders of the summands modulo 4 to arrive at the sequence $(1,-1)$ and compared this to the reduction $-135 \; mod \; 4 = 1$. The triple product $1\cdot(-1)\cdot 1 \equiv -1 \; mod \; 4$ is the sign. As odd squares are added the reduction modulo 4 cycles through the number of terms in the sum.

We are approaching the same limitation, even without any precise calculation, this must be true because reducing modulo q means that when the valuation at q of a and $b+c$ differs by more than the dimension $2p$ one or the other becomes negligible. Using the completion instead of the reduction will not help since in this setting a module is principal if and only if it is principal modulo its radical.

The absence of nontrivial sums of squares adding to zero, and explanation of the Fermat equation, would be explained by by the concept of tensor indecomposability in all cases when the valuation at q of $b+c$ and a are not too far apart multiplicatively.

16. Remark. In the example, if 59030 is replaced by 3^5-19 the algebra remains tensor indecomposable, and tensor decomposes when it is replaced by 3^4-19. The case of 3^5-19 is when the bound is achievable, but recall q is not supposed to equal $2, 3$ or p. We should not be using $a=3$ since it is not coprime to the permutation group order, but the analogous transition occurs when $q=a=5, p=3, c=q^n-b$, for various values of b. They are are indecomposable and tensor indecomposable for $n=p$. Click here for the case $b=3$ and you can observe that if you reduce c to $5^2-b=22$ a tensor decomposition occurs.

17. Remark. Robert May once used Lotka-Volterra's equations to contradict a report asserting that subdividing a natonal park by a road would increase species diversity. I failed to understand that May was not actually saying,

"Let's rely on Lotka-Volterra from now on."

While it could have acted as a salve to run a model like Lotka-Volterra showing virtual animals springing into existence when a road is removed (I actually tried to do this), absent being able to apply Popper's philosophy of science where people need to irreversibly decide future actions, we need to understand, as likely Robert May would have understood – in fact I know that he was dismissive of my attempt when I had hoped to tutor a student about it – that every model is actually only a disaster model. Climate models can meaningfully show something going wrong; but they can not establish any way back to safety, besides contradicting isolated misconceptions (engines in these tractors will make the soil suitable for food, this dam will generate power, etc). Evolutionary psychology does give a reliable intuitive vision of the shifting baseline paradigm, the so-called 'appeal to nature fallacy' is not a fallacy even while it cannot be scientifically supported.

For a specific example, Chemists label lines in a spectrum by a pair of 'term symbols.' Although they speak colloquially about an 'electron transition' they know full well that it is almost never correct to speak of an 'electron' unless The notion of probability can be rigorous when observing experiments, but it is not rigorous to say, here is a way a photon can appear, leaving this type S term symbol, an electron.

Wave equations were historically justified by thinking of a fluid as a collection of particles, or trying to describe probability waves or quantum fields. One intuitively knows, (this may be universal among practitioners in chemistry) that a harsh logical proposition about the type of a term symbol sits as a sort-of damaging piece of hardware in a stream of consciousness in some sense almost intended to more faithfully represent what is naturally there, but which is not scientifically supported. Here, for the Fermat equation, the same familiar paradigm shows us a tensor decomposition merging, as for isolating a rational point, or for a chemist to isolate an electron, or in elementary teaching, for an inequality about a discriminant or some sort of base extension to separate roots of a polynomial. There could be no ab initio notion that it should be insightful to look at real points and guess conditions for them to be rational, as the case of $x^2 + y^2 + z^2$ illustrates. (We can interpret non-negativity of area various ways, instead of subdividing a mosaic, Pythagoras might have noticed that the self-similar subdivision which fails for the pentagram actually does work for similarities of a right triangle, or anyway our consistent mainstream formulations of the real line and exterior algebra support that there was no such reason to restrict area be only a positive quantity).

For us to say, once the tensor decomposition has merged, a rational point can appear, is still only yet another statement passing from being intuitive, tentative, and ambiguous, to being mechanical, eventually seen failing to encompass duality, perspective. Removing such a notion by a type of political correctness isn't good to do either. It is hard then to see any option besides an accumulating

warehouse of conceptual junk that does not work anymore, or give up and wait for the boss at Microsoft to update something, or try to find it on the first page of Google.

The situation reminds me of Wittgenstein's well-discussed notion of the dangerous cave, about the danger of wasting time reconsidering things that needn't be considered. A notion of considering that beliefs could be illusory was then a playful abstraction, the danger was wasting time examining meaning and intentions which needn't be considered anymore. But there is in that sense in modern discourse what would be termed another cave where people go all the time without worrying. Animals appear healthy and well if they are well-kept, while, by contrast, in wild animals a relatively un-eroded context for meaningful thought allows something relatively transient and powerful. I liked listening to an online comment of N Chomsky, we are familiar with ways that animals don't appreciate human thought; it might be likely that if we could have encountered an intact residue of pre-historic thought, that is, some thinking of wild or un-domesticated people, we would be in the position of an animal trying to understand human speech.

References

1. E.Noether, Idealdifferentiation und Differente, notes from 1929 lecture in Prague, J.reine ang.Math, 188, 1-21 (1950)
2. E. Kunz, Kahler Differentials, Advanced Lectures in Mathematics (1986)
3. Discriminants and Differents (38 pages), the Stacks project.

II. Elementary observations

This is of course a post-retirement article, and what I will say here is very easy to establish, even though there is an accompanying article with more details and computer code to make sure things make sense technically.

Teichmuller roots and a Hasse principle

Let p be an odd prime number, and consider the equation $a^p + b^p + c^p = 0$ for a, b, c pairwise coprime. We can fix a and see what the condition requires of the residue classes

$$\begin{array}{l} \beta = b \ mod \ a^p \\ \gamma = c \ mod \ a^p \end{array}.$$

In the completion at a the equation requires

$$(-bc^{-1})^p = 1 + ua^p$$

where u is the invertible element $\frac{1}{c^p}$, and in the reduction modulo a^p is just the congruence

$$(-\beta\gamma^{-1})^p \equiv \ 1 \ mod \ a^p.$$

In this situation, $-\beta/\gamma$ is also the reduction modulo a^p of a "Teichmuller p'th rooot of unity" in the completion. One can be found by first choosing a root p'th root of unity modulo a (which is allowed to be trivial) and taking the limit of its p'th powers. It is allowed to be unequal to $-b/c$ as long as the congruence holds.

1. Theorem. Suppose a, b, c are such that $-b/c, -c/a, -a/b$ are p'th roots of unity modulo a^p, b^p, c^p respectively. Then necessarily $a^p + b^p + c^p = 0$.

Proof. The hypothesis implies that there is a number d such that a, b, c, d solve the equation $a^p + b^p + c^p + d(abc)^p = 0$. This require the Euclidean magnitude of d to be less than 1 so it is zero and a, b, c solve the original equation; the theorem is of the same philosophy as the Hasse principle.

Here is a consistency condititon about the p'th roots of unity.

2. Theorem. Suppose a, b, c are pairwise coprime and $a^p+b^p+c^p = 0$. Then the highest common divisor of $(b+c)$ and the difference quotient $(b^{p-1}-cb^{p-2}+...+c)$ is p if p is a divior of a and otherwise 1.

The theorem implies that the prime q divisors of a are of three types, as we can see by reducing the equation modulo the highest power of q dividing a^p. We either have $b + c \equiv 0$ in which case the first power of $-b/c$ is congruent to 1 and the difference quotient is congruent to $b^{p-1} + b \cdot b^{p-2} + ... + b^{p-2} \cdot 1 = pb^{p-1}$ (the *derivative*), which is prime to q or, if $q = p$ is just the first power, or the equality between $-b/c$ and a p'th root of unity implies the difference quotient is congruent to zero modulo the highest power of q dividing a^p.

Cubic polynomials

The coeffients of the cubic polynomial $(T+a^p)(T+b^p)(T+c^p)$ are the elementary symmetric polynomials s_1, s_2, s_3. If we make the ring $\mathbf{Z}[a,b,c]/(s_1, As_2^3 + BS_3^2)$ where $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ has determinant one, we see that we could have set $Bs_2^3 + Cs^2 = 1$ and we obtain a $\mathbb{Z}/(6p\mathbb{Z}$-graded ring. We call the component of degree 0 *mod* $6p$ with the name J, and the component of degree 1 *mod* $6p$ which is locally free as J module with the name $\mathcal{L}$, it can be interpreted as a sub-J module of the normalization of J. For technical reasons we take $\mathbf{Z} = \mathbb{Z}[1/(6p)]$, rather than just the rational integers.

3. Theorem. We find a particular element of $\mathcal{L}^{\otimes(13p-3)}$ which maps to be a root of unity in the normalization of J times a rational integer. And the rational integer is the $2/rk$ power of the index of J in its normalization, where rk is the rank of J over $\mathbf{Z}$.

The element of $\mathcal{L}^{\otimes(13p-3)} \cong \mathcal{L}^{\otimes(p-3)}$ is a different element for the fiber of the Fermat curve over a j value, and the corresponding different element for the fiber over a lambda value is of degree $p-3$ *mod* p is obtained by using $Aa+Bb$ in place of $As_2^3 + Bs_3^2$. Each rational integer so obtained specializes on each component to describe the ideal where that component meets the union of all other components. Considering both together gives a template for how to construct the irreducible components. The irreducible components of J when the fiber contains a rational point are six copies of $Spec(\mathbf{Z})$ and $6p+6$ copies of homomorphic images of $Spec(\mathbf{Z}[\omega])$ for ω a primitive p'th root of unity.

4. Crucial remark. The polynomial of degree $13p-3$ in a, b, c can be evaluated even if $a^p + b^p + c^p \neq 0$, however it is not true that raised to the $rk/2 = 3p+6$ power it gives the index of J in its normalization. It is a polynomial which can be evaluated for any (a, b, c) and *would have* given the index if $a^p + b^p + c^p = 0$ had been true. This assertion is not vacuous because the implication is a clear geometric argument.

Symmetry

In the analytic situation, the modular group Γ modulo the p-commutator subgroup of $\Gamma(2)$, that is $\Gamma(2)^{(p)}$ acts on the Fermat curve, but

5. Theorem. The the irreducible components over each λ value are indexed by orbits of AffF_p acting on F_p^3 if one of them is rational.

One way of characterising the non-existence of a rational point would be to show that the action which exists in the analytic case must also exist in the arithmetic case. The fact that the different element both of the fiber over a j value and of the fiber over a λ value are rational integers unaffected by permuting a, b, c is

consistent with the existence of some symmetry in the arithmetic case.

Tensor decomposition

In the analytic case, fibers over distinct λ values cannot intersect, but if they could one would have had an analytic pull-back structure. In the arithmetic case, the different element over lambda implies that a rational component over one lambda value is incident at each point indicated by the different element to exactly one non-rational component over that same lambda value, and the different element over J tells us that the point of intersection is also incident to an intersection of two components over another lambda value.

The p'th roots of unity, now manifested as literal roots of unity in the normalization of J, dictate exactly how the components meet. If the prime divisor q of a is also a divisor of $b+c$ then one has a root of unity order 1, and the point at q in the rational component over one lambda value, where it already meets one non-rational component over lambda, now meets at q the rational point over the lambda value where a is fixed and b, c interchanged by a transposition, and the non-rational component which it meets, and none other.

But if q is not a divisor of $b+c$ then the meeting point between the rational component at q and one non rational component over lambda now meets an intersecting pair (of possibly more) of non-rational components, at a point whose inverse image in each of the two normalizations generates a totally split prime Q containing q. The difference between $(-b/c)$ or its reciprocal with a particular p'th root of unity in the normalization of a component together with the rational integer q, necessarily congruent to 1 modulo p in this case, are a pair of generators of Q. In both cases, four primes in the normalization of J share the prime residue field F_q in J.

6. Theorem. The order of divisibility of q into a and into either $b+c$ or $b^{p-1} - cb^{p-2} .. + c^{p-1}$ is what determines whether the *local* ring of J at the four-fold intersection point, once reduced modulo the rational integer q, has a tensor decomposition (meaning it is nontrivially a homomorphic image of a tensor product over $\mathbf{F_q}$). If the valuations are compatible (sufficiently nearby, meaning, inconsistent with the conclusion of Theorem 2), it has such a decomposition.

The inconsistency with the equation $a^p + b^p + c^p = 0$, which does come down to calculus in either explanation, can be interpreted geometrically like this. Rather than invoking Theorem 2 to find a contradiction, one can say, since the Fermat curve is smooth over $\mathbf{Z}$ (recall $\mathbf{Z}$ contains $1/(6p)$), the differentials module of the ring J and any homomorphic image of the ring J must be locally principal, and the only F_q algebras with residue field F_q and locally principal diffferentials modules have to be isomorphic to $F_q[T]/(T^r)$ where r is the dimension of the algebra, it is not a nontrivial homomorphic image of a tensor product.

7. Remark. What controls the structure of local ring at such a point of the fiber is, rather than $(-b/c)^p \equiv 1$ rather the slightly weaker equation $(-b/c)^{2p} \equiv 1$. We can apply an automorphism to the third component of the normalization and replace our pattern of roots of unity such that the four components we describe are indexed by $[a : b : c], [a : b\omega : c\omega], [a : c : b\tau], [a : c\omega : b\tau\omega]$ for ω primitive. We are looking at a coordinate ring whose normalization has four components, and although it is not totally rigorous to think this way, we can imagine why the components meet. The identity between $[a : b : c]$ and $[a : b\omega : c\omega]$ is telling us we may act on b, c by ω when a is zero. The identity between $[a : b : c]$ and $[a : c : b\tau]$ is telling us that the ratio $[b : c]$ is the same as the ratio $[c : c^2/b]$ and to the extent $(-c/b)^2$ is congruent to a root of unity τ we may make the replacement. All of these notions make sense without localizing at any particular prime ideal. The fact that both coincidences can be made to happen 'simultaneously' is a deep fact that depends on comparing the different elements. The transpositions generate the full symmetric group; the root of unity τ, and its approximation $(-c/b)^2$ could act as a type of cocycle that would need to be a coboundary if we are to build the whole fiber. One can formulate the existence of a rational point as a problem of Serre's theory of Galois descent in this way, quite literally, after a base extension, where the cocycle values are automorphisms of the extended fiber and the group $\Gamma/\Gamma(2)^{(p)}$. What we are seeing, when the descent fails, is reminiscent of an abelian quotient surface singularity related to the cyclic subgroup generated by ω and the cyclic subgroup generated by a transposition, at least in the sense of having two independent differentials. A curve over the integers is two-dimensional as a scheme. In a neighbourhood of the scheme defined by a, b and c – they are sections of a line bundle really – only matter up to congruence modulo a^p, while a only matters modulo units, for the question whether $(-b/c)^p$ is really congruent to 1. Then as one considers a neighourhood of the scheme defined by b, the roles change, and now a matters more than just up to units, it matters up to congruence modulo b^p, and so-on. If we can ignore the discrepancy between the conditions that $(-b/c)^p = 1$ and $(-b/c)^{2p} = 1$ then what one always finds, when trying to construct a solution first on one of the three parts, and proceeding by applying transpositions, is that a failure always means a differentials module which is non-locally-principal (even while it is never locally free).

The weaker condition $(-b/c)^{2p} \equiv \ 1 \ mod \ a^p$ is preserved upon negating b or c. Thus if one wanted to go all the way in making logical equivalence between tensor indecomposability at the four-fold intersection and existence of solutions, one might have to re-invoke the Fermat equation only as a congruence modulo each prime divisor q of a to the first power to rule out the case $(-b/c)^p \equiv -1$.

Conclusion.

We have seen that $-b/c \ mod \ a^p$ and being an abstract p'th root of unity (and the same with a, b, c permuted) are equivalent to having solution of the Fermat

equation, and except for a slight issue of signs, which would requre us to re-invoke the Fermat equation modulo each prime under consideration, to the first power only, the Fermat question in principle can be settled in either direction after passing to the fiber to test whether an inconsistency among the p'th roots of unity implies a tensor decomposition at a four-fold intersection point, of the type which would have had to exist in the analytic world when pullbacks with neither factor discrete cannot have locally principal differentials modules.

This leaves open the problem of finding the inconsistency from first principles, or relating it to the proven Taniyama conjecture, rather than literally applying the equivalence with the global equation and invoking an existing proof. So far we have only used the different element by considering that its support is the inverse image of a subscheme of $Spec(\mathbf{Z})$, and not looked at its actual structure except intuitively, where one sees factors corresponding to transpositions, rotations etc.

The theory of Noether differents, or duality, were useful because we could never write down the index of J in its normalization by calculating it...without writing down – which means finding – a solution a, b, c of the Fermat equation. But we can calculate it indirectly as a polynomial function of a, b, c which allows us to invoke the assumption that J has a particular known index in its normalization.

Because the calculation assumes we are on a Fermat fiber, if we just put arbitrary numbers in for a, b, c the index in the normalization will not be what is predicted, of course.

What is an involution once 3 is inverted is the transformation sending (a^p, b^p, c^p) to $(a^p - b^p, b^p - c^p, c^p - a^p)$. In the second set of coordinates, the fact that the sum is zero does not need to be externally imposed, and this will give us a valid way of specializing.

:

III. 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 func-

tion -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,

$$\begin{gathered} s_1(x-y, y-z, z-x) = 0 \\ s_2^3(x-y, y-z, z-x) = -s_1^6 + 9s_1^4 s_2 - 27s_1^2 s_2^2 + 27s_2^3 \\ s_3^2(x-y, y-z, z-x) = s_1^2 s_2^2 - 4s_1^3 s_3 - 4s_2^3 + 18s_1 s_2 s_3 - 27s_3^2. \end{gathered}$$

Under the condition $s_1 = 0$ these become

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

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

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 $6s_2(a^p, b^p, c^p)^2 s_3(a^p, b^p, c^p) s_3(a^p - b^p b^p - c^p, c^p - a^p)$ 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

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

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

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

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.

IV. Overview and new conjectures.

Combinatorial group theory and Taniyama's conjecture.

The curve $\Gamma_0(N) \setminus \mathbb{H}$ is not quite the curve which 'parametrizes' an elliptic curve. Because a cusp form extends to a one-form on the smooth compactification there is a normal subgroup $M \subset \Gamma_0(N)$ such that $M \setminus \mathbb{H}$ is a contractible manifold (a copy of $\mathbb{H}$ in fact), with infinitely many points deleted. And $M \setminus \Gamma_0(N)$ is a surface group.

The homomorphism $\Gamma_0(N) \to \mathbb{Z}^2$ in Taniyama's conjecture factorizes through this quotient (M is contained in the kernel). A map $\Gamma_0(N)/M \to \mathbb{Z}^2$ describing the map of compact real surfaces is biuniquely determined by an element of $H^1(S, \mathbb{Z}^2)$ where S is the smooth compact surface; a choice of holomorphic one-form on S amounts to a holomorphic function from the universal cover of S such that each deck transformation amounts to adding a complex constant. If those constants span a copy of $\mathbb{Z}^2 \subset \mathbb{C}$ we obtain an map from the universal cover of S to the universal cover of an elliptic curve which is equivariant for a map $\Gamma_0(S)/M \to \mathbb{Z}^2$, and it descends to a map from S to an elliptic curve.

This map is not a covering space, only a branched cover. So it is induced by an equivariant map $\mathbb{H} \to \mathbb{C}$ but one which has branching.

Explicitly, if one takes the differential form ('cusp form') and pulls it back to $\mathbb{H}$ it will be of the form $f(\tau)d\tau$, it must have zeroes at the limiting 'cusps' in order to descend to a holomorpic form on S, but also $f(\tau)$ is allowed to have zeroes.

If we put things together in the simplest way, we obtain a map from $\mathbb{H}$ to the elliptic curve, but it is branched over finitely many points of the elliptic curve. The limiting 'cusps' that mapped to cusps of S do close up, but there are still points deleted from $\mathbb{H}$ There is not simply, quite, a diagram of groups.

The strategy of applying Taniyama's conjecture, first mentioned in Frey's paper, to the Fermat equation, while it is not directly enumerating subgroups of Γ, does amount to generating a combinatorial list of elliptic curves defined over $\mathbb{Q}$ and going through the enumeration

(by 'conductor').

The elliptic surface

It is possible to extend the analysis above about the Fermat fiber to the elliptic surface lying over it; it seems better, rather than using a Weierstrass/Neron model, to use the compact model corresponding to the homogeneous equation $z^4 + s_2 z^2 - s3z$ which is the product $z - e_i$, i=1,2,3,4, when $e_4 = 0$ and $e_1 + e_2 + e_3 = 0$. We set $e_i = x_i^p$. However, the different element of the whole elliptic surface is just the pullback from the Fermat fiber anyway, and it is my belief that the interesting aspect of the Fermat equation lies in the fiber.

The Fermat fiber

The different element of the fiber is the section of $\mathcal{L}^{\otimes(13p-3)}$ described by $p^2(xyz)^{p-1} \cdot 6s_2^2(x^p, y^p, z^p)s_3(x^p - y^p, y^p - z^p, z^p - x^p)s_3(x^p, y^p, z^p)$.

Although for Hellegoauarch the 'Roland's horse' was an elliptic curve, for me the 'Roland's horse' is the fact that corresponding ratios among nine elements of the local ring of $J/(Jq)$ at a maximal ideal have divisibility modulo associates satisfying the axiom of a total ordering.

When we looked at other intersections we found that it is possible to satisfy the smoothness condition 'locally,' what goes wrong at one prime can be corrected by changing a, b, c but then something else goes wrong at another prime.

Because for a, b, c coprime and p odd the equation $a^p + b^p + c^p \equiv 0 \; mod(abc)^p$ implies a Fermat counterexample, and this is an equation in a ring that splits according to the prime factorization of abc, it is possible to formulate the Fermat equation, or, just the question of existence of rational solutions, as a condition about a disjoint union over primes.

The same type of unenlightening observation occurs for the intersection of components having to do with transpositions or multiplying entries by roots of unity.

But here, in the case of the rotations, there is what may be a substantial condition on a single prime.

In the case of a prime power divisor of a, one found only that the local ring at a four-fold intersection having to do with a transposition and roots of unity, modulo q times that ring, becomes a discrete valuation ring when the valuation of a^p and of $b^p + c^p$ at the prime become incomparable. In fact, the incomparability is just a reformulation of saying that the full power of that prime which divides a^p must either divide one of the coprime parts $a + b$ or $\frac{a^p+b^p}{a+b}$

But for the rotation case, there is no such disappointingly transparent or direct reformulation of the Fermat equation which relates to the divisibility ordering of ratios of nine determnantal minors.

The fact that the issue is local makes it hard to experiment. As far as I can see, we really would need a Fermat counterexample to construct the local ring at the three-fold intersection corresponding to a rotation. The issue is, each time we consider a number like $a^p b^p - c^{2p}$ which is the product of all $ab - \omega^j c^2$ we rewrite it as $s_2(a^p, b^p, c^p) - c^p(a^p + b^p + c^p)$ and the first factor is symmetric, constant on all components, the second factor zero by the Fermat hypothesis. We can find a common prime divisor of all such expressions by merely choosing a prime divisor of $s_2(a^p, c^p, c^p)$. But it is not so easy to find a common prime divisor of $a^p b^p - c^p, b^p c^p - a^p, c^p a^p - b^p$, it is impossible, and the issue is, is it the case that it is impossible because otherwise the divisibility relation among the determinantal minors modulo associates would need to be a total ordering, and this violates some type of symmetry?

Examples.

For the first example, let's illustrate a typical tensor decomposition of a subring of $\mathbf{Z}^3$ when we reduce the subring modulo a prime(what I have been on about). Consider the subring of $\mathbb{Z}^3$ generated by $\alpha = (5, 0, 0)$ and $\beta = (0, 5, 0)$. The relations

$$\alpha^2 = 5\alpha, \beta^2 = 5\beta, \alpha\beta = 0$$

hold. If we reduce *the subring* modulo five we have the relations of a tensor decomposition,

$$0 = \alpha^2 = \alpha\beta = \beta^2.$$

We will exhibit this type of phenomenon at three components of the Fermat fiber where they meet at a closed point fixed by a cyclic permutation of (a, b, c).

We cannot actually choose a, b, c such that $a^p + b^p + c^p = 0$, so we make a simulated example which will reduce correctly modulo $q = 31$, having chosen this prime so it is congruent to 1 modulo 5 and 3. a primitive fifth root of unity modulo 31 is 2 and a primitive cube root is 5.

We start with ascending powers of 5 so we use

$$1, 5, 25$$

and we take a to be our primitive fifth root

$$a = 2.$$

Now we take b, c to be other fifth roots times our powers of 5 so

$$b = a \cdot 2^3 \cdot 5 = 80$$

$$c = a \cdot 2^2 \cdot 5^2 = 200$$

We modify these without affecting the residue class modulo 31 to make them coprime

$$b = 49$$

$$c = 45$$

Thus $a, b, c, p = 2, 49, 45, 31$. Then our sections x, y, z restricted to our three components are

$$(a, b\omega^2, c\omega^3)$$
$$(b\omega^2, c\omega^3, a)$$
$$(c\omega^3, a, b\omega^2)$$

These can be viewed as sections of L or as elements in the normalization.

Since it is computationally expensive to do the actual calculation we just specialize ω to 10945 which is 2 raised to a high power of 31 and reduced modulo a high power of 31. This is because we have to be careful not to reduce modulo q times the normalization. The reduction of the *subring* modulo $q = 31$ is such that all three components meet pairwise as we expect

specialize omega to:

a 2 b 49 c 45 p 5 N 3 q 31 10945

```
[
[[0,0],[1,2],[2,3]],
[[1,2],[2,3],[0,0]],
[[2,3],[0,0],[1,2]]
]
```

calculate
graph

0 1 31^1
0 2 31^1
1 2 31^1

and the algebra of dimension 3 over F_{31} is indecomposable but not tensor indecomposable

specialize omega to:

a 2 b 49 c 45 p 5 N 3 q 31 10945

```
[
[[0,0],[1,2],[2,3]],
[[1,2],[2,3],[0,0]],
[[2,3],[0,0],[1,2]]
]
```

calculate
graph

Subring rank should be 3
Index of subring in its normalization is 961.
Factorization of this is 31^2
Is its reduction modulo 31 *direct sum* indecomposable (trace 0 => nilpotent)? true
Is its reduction modulo 31 *tensor* indecomposable (nilpotency order 3 achieved)?false
(see developer console for a matrix representation of the subring)

And here is the matrix representation of that algebra

```
Reduction modulo q of the matrix rep
```

```
[["1","0","0"],
["0","1","0"],
["0","0","1"]]
```

```
[["0","1","0"],
["0","0","0"],
["0","0","0"]]
```

```
[["0","0","1"],
["0","0","0"],
["0","0","0"]]
```

In these calculations $\mathbf{Z}[\omega]$ has been replaced by $\mathbb{Z}$, replacing ω by 10945 to reduce computation time.

Note that this example has a special property by construction, that the ratios among a, b, c could simultaneously be specialized to p'th

roots of unity. The Fermat hypothesis and assumption that q is a divisor of $s_2(a^p, b^p, c^p)$ do not imply that this is the most general situation.

Construction of a ring J

Assume $a^p + b^p + c^p = 0$ for a, b, c pairwise coprime, p any prime number.

Make the matrix

$$\begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}$$

Multiply each entry by a formal symbol, representing a p'th root of unity so we obtain

$$\begin{pmatrix} a\omega^r & b\omega^s & c\omega^t \\ b\omega^i & c\omega^j & a\omega^k \\ c\omega^l & a\omega^m & b\omega^n \end{pmatrix}$$

for $r, s, t, i, j, k, l, m, n \in \mathbb{Z}/(\mathbb{Z}p)$.

Call the rows x, y, z.

There is an affine scheme $Spec(J)$, it is $Spec$ of the $\mathbb{Z}$ span of monomials in x, y, z of degree congruent to 0 mod $6p$. It is a subscheme of the Fermat curve.

There is a scheme L mapping to $Spec(J)$

$$\pi : L \to Spec(J).$$

It can be constructed as Spec of the symmetric algebra of $\mathcal{L}^{\otimes -1}$ over J, it is a line bundle.

The global sections of L are faithfully represented as the $\mathbb{Z}$ span of monomials of degree $\equiv 1 \ mod \ 6p$ in x, y, z.

A section of L means a map $s : Spec(J) \to L$ such that $\pi \circ s = identity$.

We fix one section s whose intersection with $Spec(J)$ we decree is defined by the Cartier divisor of x. It is two subschemes of L meeting.

For any homogeneous polynomial of degree congruent to 1 *mod* $6p$ we get another section, for instance x, y, z of degree 1 give us rational functions $1 = x/x,\ y/x,\ z/x$ and when we multiply by s we get $s,\ (y/x)s,\ (z/x)s$ which have no pole since s has a zero at x.

While the polynomials x, y, z are sections of L, we have to multiply by $\frac{s}{x}$, treating it as a formal symbol.

Remark about naturality

We can consider the global sections sheaf $\mathcal{L}$ as an ordinary module, it is the $\mathbb{Z}$-span of monomials of degree congruent to 1 modulo $6p$ in the three elements x, y, z of $\mathbb{Z}[\omega]^3$ (or we may use $3p$ now since we've passed to a subgroup). It is a rank-one projective module, and the way an element of this module determines a Cartier divisor can be described just using a principle of naturality: that for an element $s \in \mathcal{L}$ the quotient module $\mathcal{L}/(s\mathcal{L})$ is *locally cyclic*, and hence its endomorphism ring is locally isomorphic with the module itself. The coordinate ring of the subscheme of $Spec(J) \subset L$ where s meets the zero section is *Spec* of that endomorphism ring.

Contextual Remark. Choosing a meaning of the formal symbol is done in a different way in each column of the matrix; the issue of naturality turns into one of symmetry, which is familiar from many places. IBM is mixing two microwave beams to get a point of $\mathbb{C}^2$, then reducing modulo scalars to crate a Bloch sphere labelled by the hardware with $0, 1, \infty$. The purpose of a qubit might be to remove a favoured choice of basepoints; the hardware framework does specify one basis. The complement of digital computing does contain some magic. In Schroedinger's equation it relates to the ambiguity when we reformulate something real in complex language. The same notion in the past led some people to incorrectly believe complex conjugation might have been natural or intrinsic, that it could be used to define zeroes of zeta functions. This is because of wanting a formalism to be there, not caring where it comes from. Rather, forgetting, as we necessarily must, their original appeal to nature. Genetic codes, a type of phrenology, have the same well-recognized analogy with computer code; now with an instruction set among proteins expressed by the developed organism with more complexity than genetics has, which extends beyond quantum theory and beyond chemistry, the relation balanced during evolution

among massive amounts of data, even symbioses and the long term effects of social data and thinking, as Darwin contemplated so wonderfully. So it is not like we could know the instruction set, and this is obvious if you think of any way intentionality could have evolved. To the extent technology provides unprecedented choices, the choices can can only be approached based on the inescapable and false biological assumption that the consequences would have taken place pre-technology. Physics was involved with least-squares perturbation theory, consecrated into Hilbert space theory and unitary matrices, which are considered to act on the sphere as if it were a rigid planetary object, not even reaching the historical development of map projections. Each line in an emissions spectrum is labelled by a pair of term symbols, and there is almost never any 'electron' which has undergone a 'transition.' Seeing that there is no Fermat solution is reminiscent of how there is no single electron, it is reminiscent of the failure of Galois symmetry when a cube root of 2 is adjoined to $\mathbb{Q}$, except 'not Galois' is specific to multiple solutions; for a single solution one includes nilpotency.

The sections of L comprise a coherent sheaf $\mathcal{L}$ on $Spec(J)$. The global sections of L are a copy of homogeneous polynomials of degree cngruent to 1 mod $6p$. Most people would call them 'global sections of $\mathcal{L}$' and omit writing L.

Since we are on an affine scheme, we need not worry about the sheaf structure of $\mathcal{L}$, we can think of it as a rank one projective module over J, and J itself is spanned over Z by monomials in x, y, z of degree congruet to 0 mod $6p$.

We can think algebraically if we like, the normalization of J is just a cartesian product of 3 rings, each $\mathbb{Z}$ or $\mathbb{Z}[\omega]$ depending on how we assign the roots of unity.

There is a type of relativity when we assign roots of unity, we can think of the roots of unity as a torsor over Aff (μ_p) and so we view the action of Aff(μ_p) as inconsequential. In articular if we assign all entries of a column to ω^i with the same i, we can translate them to $i = 0$ and the component of the normailzation will be just $\mathbb{Z}$.

If we included a column with every possibility of permuting a, b, c and assigning roots of unity, one for each of $p + 2$ orbits of Aff(μ_p) on μ_p^3 we would have a matrix of $6p + 12$ columns and 3 rows which

would be 3 elements of $Z^6xZ[\omega]^{6p+6}$, the normalization would be rank $6p^2$ over Z as the ring itself is and that ring would be the coordiinate ring of the fiber in the Fermat curve over one lambda value.

By including just 3 columns, we are selecting 3 components and looking at the coordinate ring of the image of the map from the disjoint union of their normalizations to J.

We are interested in the scheme defined by $s_2(x^p, y^p, z^p) \in \mathcal{L}^{\otimes 2p}$ a section of $L^{\otimes 2p}$. Because the polynomial is symmetric it is the same as the subscheme defined by the rational integer $s_2(a^p, b^p, c^p)$.

We will work in a neighbourhood of this subscheme, this means we can work where a, b, c are nonzero because abc is coprime to $s_2(a^p, b^p, c^p)$.

Because we assume $a^p + b^p + c^p = 0$ so is its square so $0 = (a^{2p} + b^{2p} + c^{2p}) + 2s_2(a^p, b^p, c^p)$

This means $|s_2(a^p, b^p, c^p)| \geq \frac{1}{2}(a^p)^2 + (b^p)^2 + (c^p)^2)$.

It is a negative number of quite large magnitude.

When we look at the size two determinantal minors of our matrix we get expressions which are a root of unity times

$$ac - \omega^j b^2$$

for various j, and their transforms under permuting a, b, c, these are divisors of $a^p c^p - b^{2p}$.

Consider the number

$$a^p c^p - b^{2p}$$

Add the other two terms of s_2 to the first summand and subtract from the second

$$= a^p c^p + c^p b^p + b^p a^p - (b^{2p} + c^p b^p + b^p a^p)$$

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

The Fermat assumption thus tells us that the polynomial expression we are interested in is symmetric, it is just a symmetric polynomial

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

This means, if we choose a prime divisor q of $s_2(a^p, b^p, c^p)$ and choose a prime Q in $Z[\omega]$ lying over q, there must be a j such that $a^p c^p - \omega^j b^{2p} \in Q$

And, the same is true upon permuting a, b, c although the value of j might change.

There is a relation among the nine size two minor determinantal minors, once we reduce them modulo Q and interpret the entries as in a field. All nine determinantal minors are zero if and only if the four which correspond to deleting first or last row or column are zero. This is because for nonzero vectors pairwise linear dependence is an equivalence relation.

These four determinantal minors can be controlled, the roots of unity attached to the four corner entries of the matrix belong each to exactly one of the submatrices.

The fact that q is a common divisor of $a^p b^p - c^{2p}$ and its transforms under permuting a, b, c (which happen to all be equal) impies that once we know from the divisibility of Q that there is some choice of root of unity to put in each corner to make each of the four minor determinants zero in a residue field, we also know by independence of the four corners (each contained in just one size two submatrix) that there is a choice which makes all four, and hence all nine, simultaneously zero; and what this implies is that we can choose 3 of the $6p + 12$ components of the Fermat fiber which intersect at a closed point lying over $q \in Spec(Z)$.

We have allowed ourselves to take Q to be the 'same' prime ideal in each non-rational component of the normalization, and think of ourselves adjusting the multiplier roots of unity by choosing three components to make all four determinantal minors belong to that same prime ideal. So we can think of our matrix as a matrix with entries in just one copy of $\mathbb{Z}[\omega]$, and we can think that we have fixed one prime Q lying over q, and we just choose the components to make the matrix modulo Q have rank 1.

Now let's see if we can build the tensor decomposition. For this, we will look at the rational functions $x/y, y/z$ which are well-defined in a neighbourhood of the subscheme defined by q. These generate the

coordinate ring of a neighbourhood of the locus of interest, because from these we can obtain $(x/y)\cdot(y/z) = x/z$, and y/z.

These are

$$\begin{matrix}(\frac{a}{b}\omega^{r-i}, \frac{b}{c}\omega^{s-j}, \frac{c}{a}\omega^{t-k}) \\ (\frac{b}{c}\omega^{i-l}, \frac{c}{a}\omega^{j-m}, \frac{a}{b}\omega^{k-n})\end{matrix}.$$

The conditions for tensor decomposition modulo q.

The choice of r, s, t, i, j, k allows us to choose a prime ideal Q of $\mathbb{Z}[\omega]$ containing q such that the inverse image of Q under each of the three projections is one and the same maximal ideal $\mathcal{Q}$ in the ring J generated over $\mathbb{Z}$ by the two rows shown above. We will localize J at $\mathcal{Q}$ to obtain a local ring $J_{\mathcal{Q}}$ and consider what conditions control whether $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$ has its maximal ideal principal.

Since some determinantal minors are repeated, we will show that we can simultaneously arrange this when l, m, n are just $i+j-s, j+k-t, k+i-r$. We retain the properties we have discussed so far, so that a single ideal $\mathcal{Q}$ of J is the inverse image of Q under the projection to each component; but in addition gain the property that each of the three entries of $x/y - y/z$ belongs to Q^m times $\mathbb{Z}[1/(abc)]$. Thus in $Spec(J)$ we have three components meeting at one closed point, which is is the image of either Q or its intersection with $\mathbb{Z}$ under a map $Spec(\mathbb{Z}) \to Spec(J)$ or a map $Spec(\mathbb{Z}[\omega]) \to Spec(J)$ for each of the three components.

In the case of two components meeting at a point there would be no contradiction, for instance if I take $\mathbb{Z}[x, y]$ modulo relations $x^2 = 5x, y^2 = 5y, xy = 0, x + y = 5$ we find it is just isomorphic to $\mathbb{Z}[x]$ with relation $x^2 = 5x$ and the reduction modulo 5 is $F_5[x]/x^2$ which has no tensor decomposition.

It is possible to have three components meeting at a point without having a nontrivial tensor decomposition of $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$.

Here are some basic remarks

Remark. The algebra $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$ contains a subring reducing isomorphically to the residue field $J_{\mathcal{Q}}/(QJ_{\mathcal{Q}})$.

Proof. Because of Artin-Rees there is some N such that $Q^N \mathcal{J}_{\mathcal{Q}} \subset qJ_{\mathcal{Q}}$. It is standard that the algebra $J_{\mathcal{Q}}/(\mathcal{Q}J_{\mathcal{Q}})^N$ contains a copy of its residue field and the desired algebra is a homomorphic image.

Remarks.

i) A necessary and sufficient condition, in our situation, for $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$ to have a nontrivial tensor decomposition is that $\mathcal{Q}^2 \subset qJ_{\mathcal{Q}}$.

ii) A necessary and sufficient condition for the algebra *not* to have any nontrivial tensor decomposition over the subring isomorphic to the residue field is that every generating set of as an algebra over that field contains a single element which generates that algebra over its residue field.

Proof. Let k denote the completion of $\mathbb{Z}[\omega]$ at Q so that J is a subring of k^3. The reduction of the image modulo $q^N(k^3)$ contains the reduction of the diagonal k, and since by Artin-Rees we only care about the image for some large N we can replace J with the algebra generated by J and the diagonal k. Another way of seeing this is, the completion of J at $\mathcal{Q}$ attains an unramified extension which increases its residue field to match that of k.

Rather than try to apply these conditions directly, It simplifies things a bit if we pass to completions. Let k be the completion of $\mathbb{Z}[\omega]$ at Q. By Artin-Rees there is an N so that $\mathcal{Q}^N J_{\mathcal{Q}} \subset qJ_{\mathcal{Q}}$, so it does not make any difference whether we complete $J_{\mathcal{Q}}$ at $\mathcal{Q}J_{\mathcal{Q}}$ or at $qJ_{\mathcal{Q}}$. The completion of J embeds in k^3.

If $q \equiv 1 \ mod \ p$, which is the main case we consider, then the diagonal $k(1,1,1)$ is already contained in the completion of J, and the completion of J is a submodule for the underlying k-module structure of k^3.

In general, we can consider the sub-k-module of k^3 generated by J, it is a subalgebra of k^3 containing the diagonal k.

In passing from the completion of J to the sub-k-module it generates, the residue field of J increases from the prime field to the residue field of k.

We are interested in the F_q-algebra $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$, and whether it has a nontrivial tensor decomposition. Because by Artin-Rees it is a homomorhic image of $J_{\mathcal{Q}}/(QJ_{\mathcal{Q}})^N$ for some N, and that algebra contains a ring reducing isomorphically to its residue field, the same is true of $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$.

The map from the completion of J to the sub-k-module of k^3 spanned by that completion becomes an isomorphism once we reduce both algebras modulo q, therefore.

The sub-k-module of k^3 generated by the completion of J is also, incidentally, just generated by J itself. It is a free module of rank three. It contains the k-span of $(1,1,1)$ and so it has a k-basis consisting of $(1,1,1)$ together with two additional elements, which can be taken to be either of the form $q^i(1,\alpha,0),\ q^j(1,\beta,0)$ or of the form $q^i(1,\alpha,0), q^j(\beta,1,0)$. To see this, first subtract a multiple of $(1,1,1)$ from each of the two other basis elements make the third entry zero, then divide out the highest possible power of q so one entry is a unit, and finally divide by that unit.

There is an amusing process of performing a cyclic rotation. Writing $\alpha = uq^s$ for u invertible, From $(1,uq^s,0)$ we can subtract $(1,1,1)$ to obtain $(0,uq^s-1,-uq^s) = (0,1,\frac{u}{1-uq^s}q^s)$ which is of the form $(0,1,vq^s)$ for a unit v. There is also an amusing process of interchanging the two entries of highest order (taking 0 to be order infnity). That is, from $(1,uq^s,0)$ we subtract $uq^s(1,1,1)$ to obtain $(1-uq^s,0,-uq^s)$ and multiply by a unit to obtain $(1,0,\frac{-u}{1-uq^s}q^s)$ which is of the type $(1,0,vq^s)$.

Combining these processes, we can obtain a basis consisting of $(1,1,1), q^i(1,\alpha,0), q^j(1,\beta,0)$. we may assume $i \leq j$ by interchanging the labels α,β and then we can subtract a multiple of one from the other to arrive at $(1,1,1), q^i(1,\alpha,0), q^j(0,\beta,0)$. Finally we can increase j and multiply β by a unit to arrive at $(1,1,1), q^i(1,\alpha,0), q^j(0,1,0)$ with $j \geq i$. Closure under multipication is equivalent to the notion that the square of the second basis vector is in the span of the three, which is the same as saying it is in the span of the last two. From $(q^{2i}, q^{2i}\alpha^2, 0)$ we subtract $q^i(q^i, q^i\alpha, 0)$ to get $((0, q^{2i}\alpha(\alpha-1), 0)$ and for this to be a multiple of $(0,q^j,0)$ we need j to be no larger than the order of the middle term, which is $2i$ plus the order of α. Since we are assuming that the algebra is closed under multipication, we know then that $j \leq 2i + v_q(\alpha)$.

Now we know the structure constants of the algebra, the action of multiplying by the two nontrivial basis elements is a multiple of q if and only if the inequality is strict.

Theorem. The algebra $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$ admits a nontrivial tensor decomposition over a field if and only if the subalgebra of the complete algebra k^3 which it spans over k, when given a basis $(1,1,1), q^i(1,\alpha,0), q^j(0,1,0)$ for $i \leq j$ satisfy $j < 2i + v_q(\alpha)$. Otherwise $j = 2i + v_q(\alpha)$.

Example. The subring of $\mathbb{Z}^5$ with basis $(1,1,1), (25,125,0), (0,625,0)$ when the *subring* is reduced modulo 5 is tensor decomposable, that with basis $(1,1,1), (25,125,0), (0,3125,0)$ when the subring is reduced modulo 5 is tensor indecomposable, and the commutative group with basis $(1,1,1), (25,125,0), (0,15625,0)$ is not a subring. Tensor indecomposability occurs when the third basis element is $(0,1,0)$ multiplied by the highest power of 5 which still allows closure under multiplication, which is the order of the product of the entries of the basis element $(25,125,0)$.

We can sharpen the argument a bit.

Theorem. Let k be a complete discrete valuation ring, and consider any two elements of k^3 which form a linearly independent set together with $(1,1,1)$. The linear span of the three elements has a basis of the form

$$(1,1,1), (\alpha,\beta,0), (0,\gamma,0)$$

such that α, β, γ have strictly positive valuation (lie in the maximal ideal), while β/α and γ/α are integral (have valuation greater than or equal to zero)

i) If $\gamma/(\alpha\beta)$ is in the maximal ideal (has valuation greater than or equal to 1 then the span of the three original elements is not a subring, nevertheless the ring which they *generate* is also generated by just the single element $(\alpha,\beta,0)$. If we call the subring J, then the tensor product of J with the residue field k is isomorphic to $k[T]/(T^3)$ generated by the image of $(\alpha,\beta,0)$.

ii) If $\gamma/(\alpha\beta)$ is invertible (has valuation zero) then the three original elements do span a subring, and it is still true that it is generated by the single element $(\alpha,\beta,0)$. The tensor product of the subring with the residue field k is also in this case isomorphic with $k[T]/(T^3)$.

iii) If $\gamma/(\alpha\beta)$ is not integral (has strictly negative valuation) then the span of the original three elements is a ring, and that ring is also generated by $(\alpha, \beta, 0)$ and $(0, \gamma, 0)$. Moreover both elements are nilpotent of order two. The tensor product of the subring with the residue field is isomorphic with $k[X, Y]/(X^2, XY, Y^2)$.

Application to the complete subring

Let's apply these considerations to the subring of k^3 generated by J. It is the subring of the complete ring k^3 generated by x/y and y/z and each component of the difference has the same order m at q as the elementary symmetric polynomial $s_2(a^p, b^p, c^p)$ at q.

Since we now are working over k in k^3 we can interpret the roots of unity in the 3-tuples which represent x/y and y/z as elements of the base ring k. Recall these are

$$\begin{matrix}(\frac{a}{b}\omega^{r-i}, \frac{b}{c}\omega^{s-j}, \frac{c}{a}\omega^{t-k}) \\ (\frac{b}{c}\omega^{i-l}, \frac{c}{a}\omega^{j-m}, \frac{a}{b}\omega^{k-n})\end{matrix}.$$

Because the entries of x, y, z were in close proportion, we know that any of the six entries shown above is congruent to 1 modulo Q.

Note that there is no requirement that $m = r$, for example, so it is not required that we can absorb the roots of unity into the letters a, b, c.

Let us follow our prescription in the previous theorem so we divide each element by its last entry and subtract $(1, 1, 1)$ to obtain

$$\begin{matrix}(\frac{a^2}{bc}\omega^{r-i-t+k} - 1, \frac{ba}{c^2}\omega^{s-j-t+k} - 1, 0) \\ \frac{b^2}{ac}\omega^{i-l-k+n} - 1, \frac{bc}{a^2}\omega^{j-m-k+n} - 1, 0)\end{matrix}$$

Incidentally, the superscripts in the second row are uniquely determined modulo p to make particular minor determinants of the original matrix belong to Q and because the entries a, b, c occur in more than one location, we already know

$$i - l - k + n = i - r - j + s$$

$$j - m - k + n = t - r + i - k$$

modulo p so we can write this as

$$\begin{matrix}(\frac{a^2}{bc}\omega^{r-i-t+k} - 1, \frac{ba}{c^2}\omega^{s-j-t+k} - 1, 0) \\ \frac{b^2}{ac}\omega^{s-j-r+i} - 1, \frac{bc}{a^2}\omega^{-r+i+t-k} - 1, 0)\end{matrix}$$

We now know that each nonzero entry has valuation *exactly* m where m is the order of $s_2(a^p, b^p, c^p)$ at q. To create γ we make a linear combination of these rows which has zero in the first entry to obtain $(0, \gamma, 0)$

One way to do this is to cross-multiply such that γ is the determinant of the matrix made from the four entries, which is

$$\begin{pmatrix} \frac{a^2}{bc}\omega^{r-i-t+k} - 1 & \frac{ba}{c^2}\omega^{s-j-t+k} - 1 \\ \frac{b^2}{ac}\omega^{s-j-r+i} - 1 & \frac{bc}{a^2}\omega^{-r+i+t-k} - 1 \end{pmatrix}$$

The first entry of each three-tuple is a multiple of q^m and we can do better by dividing each entry by q^m, this gives the determinant of the matrix above but with the entries in the first column divided by q^m, and that is our value of γ such that $(0, \gamma, 0)$ is a linear combination of the two three-tuples shown with unit coefficients. The pair of units can be complemented to make an invertible matrix and hence we have as generators either of the two three-tuples shown above together with q^{-m} times the determinant of the matrix shown.

If the determinant has order $2m$ (the same as each of the two binomials which make it up) then γ will have order m and α, β, γ will satisfy the condition guaranteeing a tensor decomposition of $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$. On the other hand, if there is sufficient cancellation in the determinant formula that the order of the determinant reaches $3m$ so the order of γ reaches $2m$ the tensor decomposition will merge and fail, and we will have no contradiction.

We can multiply each row by an invertible element to arrive at

$$\begin{pmatrix} \frac{a}{b}\omega^{r-i} - \frac{c}{a}\omega^{t-k} & \frac{b}{c}\omega^{s-j} - \frac{c}{a}\omega^{t-k} \\ \frac{b}{c}\omega^{s-j} - \frac{a}{b}\omega^{r-i} & \frac{c}{a}\omega^{t-k} - \frac{a}{b}\omega^{r-i} \end{pmatrix}$$

. Setting

$$A = \frac{a}{b}\omega^{r-i}$$

$$B = \frac{b}{c}\omega^{s-j}$$

$$C = \frac{c}{a}\omega^{t-k}$$

this becomes

$$\begin{pmatrix} A - C & B - C \\ B - A & C - A \end{pmatrix}$$

which has determinant

$$-A^2 + 2AC - C^2 - B^2 + BA + BC - AC$$

$$= AB + BC + CA - A^2 - B^2 - C^2$$

The choice of r, s, t, i, j, k has arranged that A, B, C occupy the same residue class modulo Q^m but any pair is distinct modulo Q^{m+1}. If we trace back the reason it is because each difference times a unit is a divisor of an expression that is invariant under permuting a, b, c with the other factor invertible and which has order precisely m at q.

The very strict condition which we're considering is just a necessary consequence of the Fermat equation, and smoothness of the Fermat curve away from the locus defined by p.

Smoothness of the Fermat curve requires that expression above to belong to Q^{3m}, while it is expressed as a difference of two terms in Q^{2m}.

If we write each of A, B, C as a $3p$ root of unity τ plus an error term, then the differences like $A - B$ amount to the differences of the error terms. Write

$$A = \tau + q^m \alpha$$
$$B = \tau + q^m \beta$$
$$C = \tau + q^m \gamma$$

and then our determinant $(A - C)(C - A) - (B - A)(B - C)$ is

$$q^{2m}((\alpha - \gamma)(\gamma - \alpha) - (\beta - \alpha)(\beta - \gamma))$$
$$= q^{2m}(\alpha\beta + \beta\gamma + \gamma\alpha - \alpha^2 - \beta^2 - \gamma^2).$$

From $ABC = \tau^3$ we have

$$\tau^3 = (\tau + q^m \alpha)(\tau + q^m \beta)(\tau + q^m \gamma)$$

$$= \tau^3 + q^m(\alpha + \beta + \gamma)\tau^2 + q^{2m}(\alpha\beta + \beta\gamma + \alpha\gamma)\tau + q^{3m}\alpha\beta\gamma.$$

This shows

$$\alpha + \beta + \gamma \in Q^m,$$

from this

$$2(\alpha\beta + \beta\gamma + \alpha\gamma) + \alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 \in Q^{2m}.$$

The Fermat smoothness condition (failure of tensor decomposition modulo q) was

$$\alpha\beta + \beta\gamma + \gamma\alpha - \alpha^2\beta^2 - \gamma^2 \in Q^m.$$

This is equivalent to

$$3(\alpha\beta + \beta\gamma + \gamma\delta) \in Q^m,$$

then. This shows when $q = 3$ there is never a tensor decomposition mod q. As long as $q \neq 3$ this is equivalent to

$$\alpha\beta + \beta\gamma + \gamma\delta \in Q^m.$$

This is useful now as in our earlier equation involving τ^3 the lack of tensor decomposition modulo q is (for $q \neq 3$) equivalent to $\alpha+\beta+\gamma \in Q^{2m}$. And this is equivalent to

$$\frac{1}{3}(A + B + C) \equiv \tau \ mod Q^{2m}.$$

This implies that there is a j such that

$$(\frac{1}{27}(A + B + C))^3 \equiv \omega^j \ mod \ Q^{2m}.$$

We can explicitly remind ourselves what A, B, C are, they are multiples of the forward ratios $a/b, b/c, c/a$ by p'th roots of unity to make all three mutually congruent modulo Q^m, and then the failure of tensor decomposition modulo q enforces that the average

Thus,

Theorem. Suppose $a^p+b^p+c^p = 0$ with p prime and a, b, c pairwise coprime. Let ω be a primitive p'th root of unity. Let q be a prime divisor of $s_2(a^p, b^p, c^p)$ and let m be the order of $s_2(a^p, b^p, c^p)$ at q. It is possible to multiply each forward ratio $a/b,\ b/c,\ c/a$ by a p'th root of unity in $\mathbb{Z}[\omega]$ to make all three mutually congruent modulo Q^m for Q a prime ideal of $\mathbb{Z}[\omega]$ lying over q, and none congruent to a $3p$ root of unity modulo Q^{m+1}. Call these elements A, B, C (so that each of A, B, C is one of the forward ratios $a/b, b/c, c/a$ times a p'th root of unity). There is a corresponding local ring $J_{\mathcal{Q}}$ of the subscheme of the Fermat fiber over its j value consisting of

three irreducible components meeting at a point. (Note $\mathcal{Q}$ is not quite the same as Q). Smoothness of the Fermat curve implies that for $q \neq p$ the algebra $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$ must be tensor indecomposable (not nontrivially a homomorphic image of a tensor product over a field). Tensor indecomposability of that ring automatically holds for $q = 3$; and for $q \neq 3$ it is equivalent to the condition that $\frac{1}{27}(A+B+C)^3$ is congruent modulo the higher power of Q^{2m} to a power ω^j in $\mathbb{Z}[\omega]$, in other words that in the completion k of $\mathbb{Z}[\omega]$ at Q there exists a $j \in \{0, 1, 2, ...p-1\}$ and an $x \in k$ such that $\frac{1}{27}(A+B+C)^3 = \omega^j + q^{2m}x$.

Strategy to calculate the determinant

Let's name the particular p'th roots of unity $\omega_1, \omega_2, \omega_3$ such that

$$A = \frac{a}{b}\omega_1$$

$$B = \frac{b}{c}\omega_2$$

$$C = \frac{c}{a}\omega_3.$$

There is no requirement that $\omega_1\omega_2\omega_3$ should equal 1, rather they are chosen so that A, B, C are mutually congruent modulo Q^m.

However, we can write

$$B = A + q^m\phi$$

$$C = B + q^m\psi$$

for $\phi, \psi \in k$ where k is the localization (or we may take the completion here) of $\mathbb{Z}[\omega]$ at Q. Or we may even use $\mathbb{Z}[\omega]$ with $\frac{1}{abc}$ adjoined.

Then

$$\begin{aligned} B^p &= A^p + (B^p - A^p) \\ &= A^p - \frac{1}{b^p c^p}s_2 \end{aligned}$$

where by s_2 we mean $s_2(a^p, b^p, c^p) = a^p c^p - b^{2p}$; and

$$\begin{aligned} C^p &= A^p + (C^p - A^p) \\ &= A^p + \frac{1}{a^p b^p}s_2 \end{aligned}$$

where now $s_2 = c^p b^p - a^{2p}$. But we may also raise the earlier equations to the p'th power

$$B^p = \sum_{i=0}^{p} \binom{p}{i} A^{p-i} q^{mi} \phi^i$$

$$C^p = \sum_{i=0}^{p} \binom{p}{i} A^{p-i} q^{mi} \psi^i.$$

Combining

$$-\frac{1}{b^p c^p} s_2 = \sum_{i=1}^{p} \binom{p}{i} A^{p-i} q^{mi} \phi^i$$

$$\frac{1}{a^p b^p} s_2 = \sum_{i=1}^{p} \binom{p}{i} A^{p-i} q^{mi} \psi^i.$$

As congruences modulo Q^{2m} we have

$$-\frac{1}{b^p c^p} s_2 \equiv p A^{p-1} q^m \phi$$

$$\frac{1}{a^p b^p} s_2 \equiv p A^{p-1} q^m \psi$$

Then since

$$A^{p-1} = \omega_1^{-1} \frac{a^{p-1}}{b^{p-1}}$$

we have as congruences modulo Q^m

$$\phi \equiv -\frac{1}{b^p c^p} \frac{s_2}{q^m} \omega_1 \frac{b^{p-1}}{a^{p-1}} p^{-1}$$

$$\psi \equiv \frac{1}{a^p b^p} \frac{s_2}{q^m} \omega_1 \frac{b^{p-1}}{a^{p-1}} p^{-1}$$

Also

$$\phi - \psi \equiv \frac{-a^p - c^p}{a^p b^p c^p} \frac{s_2}{q^m} \omega_1 \frac{b^{p-1}}{a^{p-1}} p^{-1}$$

Since $-a^p - c^p = b^p$

$$\phi - \psi \equiv \frac{1}{a^p c^p} \frac{s_2}{q^m} \omega_1 \frac{b^{p-1}}{a^{p-1}} p^{-1}$$

The determinant is $q^{2m}(-\psi^2 - \phi(\phi - \psi))$ with the second factor a unit times

$$\begin{aligned}
&\frac{-1}{a^{2p}b^{2p}} + \frac{1}{b^p c^p a^p c^p} \\
&= \frac{-a^p b^p c^{2p} + a^{2p} b^{2p}}{a^{3p} b^{3p} c^{2p}} \\
&= \frac{a^p b^p - c^{2p}}{(abc)^{2p}} \\
&= \frac{s_2(a^p, b^p, c^p)}{s_3^2(a^p, b^p, c^p)}
\end{aligned}$$

This has order precisely m at Q confirming that the determinant has order $3m$, so our third generator $(0, \gamma, 0)$ has that the order of γ at Q is indeed equal to $2m$ precisely, confirming as we knew that the span of our elements is closed under multiplication and however showing that tensor indecomposability can be derived directly from polynomial algebra and is not an independent conddition.

What we have shown is that each of

$$\begin{array}{l}
(\frac{a^2}{bc}\omega^{r-i-t+k} - 1, \frac{ba}{c^2}\omega^{s-j-t+k} - 1, 0) \\
\frac{b^2}{ac}\omega^{s-j-r+i} - 1, \frac{bc}{a^2}\omega^{-r+i+t-k} - 1, 0)
\end{array}$$

is contained in the algebra over k generated by the other.

A case of more than four components

Let's return to the case when a is a multiple of q. When we consider more than four components, here is what we find. Call a component 'rational' if our $\mathrm{Aff}(F_p)$ representative is $(0, 0, 0)$ and 'quasi-rational with respect to q for q a divisor of a if its representative is $(0, 1, 1)$. Then I will state without proof, but what I have checked,

Theorem. Let q be a prime divisor of a and assume q is a divisor of the difference quotient $b^{p-1} - cb^{p-2} ... + c$ (and therefore not a divisor of $b + c$) . There are $2(p - 1)$ maximal ideals of J containing q. The $p-1$ prime ideals lying over q in the quasi-rational components which we may label by $(a, b\omega, c\omega)$ all contract to a single prime ideal of J – the same one as comes from the rational component (a, b, c), that is, the inverse image of $q\mathbb{Z}$ under the projection $J \to \mathbb{Z}$ on the corresponding rational component. The $p - 1$ prime ideals

in each non-quasi-rational and non-rational component across the transposition interchanging b and c we may label $(a, c\omega^i, b\omega^j)$ for $(0, i, j)$ one of our Aff(F_p) orbit representatives in F_p^3 contract one each to one of $p-1$ maximal ideals of J lying over q. One of these $p-1$ maximal ideals is the same one coming from the rational component (a, b, c). Symmetrically opposite, the non-rational and non-quasi-rational $(a, b\omega^i, c\omega^i)$, p in number, each have $p-1$ maximal ideals mapping to $p-1$ new maximal ideals of J and one of these is equal to the contration of both the rational (a, b, c) and quasi-rational $(a, b\omega, c\omega)$ component across the transposition.

If we want to be precise about specifying maximal ideals in J and also using our Aff(F_p) orbit representatives, we can be explicit about the automorphism bringing each prime in each component of the normalization into a standard position, that is, we will specify a nonzero $i \in F_p$ for each component, and explicitly replace ω by ω^i. Thus when q is a divisor of a and we have our $p+2$ components meeting at a point with

$$\begin{gathered} x = (a, a, a, a, a, a, ...a) \\ y = (b, b\omega, c, c\omega, c\omega, c\omega, ..., c\omega) \\ z = (c, c\omega, b\omega, b, b\omega^2, b\omega^3, ...b\omega^{p-1}) \end{gathered}$$

(and note crucially the term $b\omega$ is correctly removed from the sequence), we assume ω as it is in the third component of z is chosen to make $b^2\omega - c^2$ belong to a particular maximal ideal Q in the third component containing q, and then we raise ω in every subsequent component of y and z to a suitable power that the maximal ideal which we would label with the name Q in the other components, using whatever was our initial labelling of ω, is the one containing the minor determinants as if we could have identified all components using our original arbitrary labelling.

This means we should now write

$$\begin{gathered} x = (a, a, a, a, a, a, ...a) \\ y = (b, b\omega, c, c\omega^{(0-1)^{-1}}, c\omega^{(2-1)^{-1}}, c\omega^{(3-1)^{-1}}, ..., c\omega^{(p-2)^{-1}}) \\ z = (c, c\omega, b\omega, b(\omega^{(0-1)^{-1}})^0, b(\omega^{(2-1)^{-1}})^2, b(\omega^{(3-1)^{-1}})^3, ...b(\omega^{(p-2)^{-1}})^{p-1}) \end{gathered}$$

Here the sequence $(0-1)^{-1}, (2-1)^{-1}, (3-1)^{-1}, ...$ which is correctly missing the case of $1-1$ refers to the inverses in F_p, and runs through the nonzero elements of F_p. To see how this works, if we

look at the last entry of $\frac{z}{y}$ we get $\omega^{\frac{p-1}{p-2}}$ divided by $\omega^{\frac{1}{p-2}}$ with the exponent ratios calculated in F_p, and the ratio is $\omega^{\frac{p-1}{p-2}-\frac{1}{p-2}} = \omega$ a constant ratio throughout all but the first two entries, which is what ensures all components meet at the maximal ideal which is the pullback now of what we would call the same maximal ideal on each component (based on our original and unchanged labelling of one of the primitive p'th roots of unity on each component with the name ω).

Of course $\omega^{(0-1)^{-1}}$ is just ω^{-1} and its zero'th power is 1.

Generators over the local ring of $\mathbb{Z}$ at q of J are now $\frac{x}{y}$ and $\frac{z}{y}$ and these are also a pair of generators

$$b\frac{x}{y} = a \cdot (1, \omega^{-1}, \frac{b}{c}, \frac{b}{c}\omega^{-\frac{1}{p-1}}, \frac{b}{c}\omega^{-\frac{1}{1}}, \frac{b}{c}\omega^{-\frac{1}{2}}, \frac{c}{b}\omega^{-1/3}, ...\frac{c}{b}\omega^{-\frac{1}{p-2}})$$

$$\frac{c}{b}\frac{z}{y} = (1, 1, \frac{c^2}{b^2}\omega, \frac{c^2}{b^2}\omega, ..., \frac{c^2}{b^2}\omega).$$

Again, $\omega^{-\frac{1}{p-1}}$ is just ω but the expression shows that the last p entries $b\frac{x}{y}$ just consist of $a \cdot \frac{c}{b}$ multiplied by every possible p'th root of unity while the last p entries of $\frac{c}{b}\frac{z}{y}$ are constant $\frac{c^2}{b^2}\omega$.

We can interpret the entries now as if they were in one copy of $\mathbb{Z}[\omega]$ and when we subtract the constant $(1, 1, 1...)$ from $\frac{c}{b}\frac{z}{y}$ the choice of ω is the one which makes all entries belong to one and the same maximal ideal of $\mathbb{Z}[\omega]$, determined by the congruence $\frac{b^2}{c^2}\omega \equiv 1$.

Now as q is a divisor of $b - c$ as long as q is not 2 it cannot be a divisor of $b^p - c^p$ as it is already a divisor of $b^p + c^p = a^p$. Then from $b^2\omega \equiv c^2$ we have $b^{2p} - c^{2p} = (b^p - c^p)(b^p + c^p) \equiv 0$ so $b^p + c^p \equiv 0$ and from our assumption that q is a divisor of the difference quotient $b^{p-1} - cb^{p-2}... + c^{p-2}$ and therefore not of $b + c$ we have $b\omega + c \equiv 0$. So our choice of maximal ideal of J is consistent with the rule that $b\omega + c$ belongs to our maximal ideal on each non-rational component (the first component is the only rational component).

In fact, each entry of $\frac{c}{b}\frac{z}{y} - 1$ now has order at Q which is p times the order of a at q, since $-a^p = b^p + c^p$. To express it as a power series in $b\frac{x}{y}$ which has nonzero order at our maximal ideal, being a multiple of a, we just need to use the van-der-monde determinant

which applies as long as we can verify that all entries are distinct. We need to verify that no power of ω times $\frac{c}{b}$ is equal to 1 or ω^{-1}. This just needs that the rational number $\frac{c}{b}$ is not precisely equal to any p'th root of unity and is true. We also need that the ratio of order at Q is at least as large as the number of entries which is $p+2$, so we need

$$\frac{v_q(a^p)}{v_q(a)} \geq p+2.$$

The element q is a uniformizer in each component, and so we are trying to express $q^{pm}(0,0,1,1,1,...,1)$ as a polynomial in $q^m(1,\omega^{-1},\frac{c}{b}\omega^0,\frac{c}{b}\omega^1,...,\frac{c}{b}\omega^{p-1})$. I have taken the liberty to re-arrange the last p components and multiply by units.

It is now a linear algebra problem. Of course, as I might have mentioned before, an easy way to approach this is to say, if we call our elements $q^m\alpha$ and $a^{pm}\beta$, that if we can find a polynomial $P(T)$ of degree at most p so that $P(\alpha)=\beta$ then we can find a homogeneous polynomial of degree p $Q(X,Y)$ in two variables such that $Q(1,T)=P(T)$, and then $Q(q^m,q^m\alpha)=q^{pm}Q(1,\alpha)=q^{pm}P(\alpha)=q^{pm}\beta$. But the question is, can we find a polynomial $P(T)$ of degree at most p such that

$$P(0)=0$$

$$P(\omega^{-1})=0$$

$$P(\frac{b}{c}\omega^i)=1,\ i=0,1,...,p-1$$

Let's write down a square matrix for which the last column must be in the span of the earlier columns for the solution to exist. It is

$$\begin{pmatrix}
1 & 1 & 1 & 1 & ... & 1 & 1 & 1 & 0\\
1 & \omega^{-1} & \omega^{-2} & \omega^{-3} & ... & \omega^{p+2} & \omega^{p+1} & \omega^p & 0\\
1 & \frac{b}{c}\omega^0 & \frac{b^2}{c^2}\omega^0 & \frac{b^3}{c^3}\omega^0 & ... & \frac{b^{p-2}}{c^{p-2}}\omega^0 & \frac{b^{p-1}}{c^{p-1}}\omega^0 & \frac{b^p}{c^p}\omega^0 & 1\\
1 & \frac{b}{c}\omega^1 & \frac{b^2}{c^2}\omega^2 & \frac{b^3}{c^3}\omega^3 & ... & \frac{b^{p-2}}{c^{p-2}}\omega^{p-2} & \frac{b^{p-1}}{c^{p-1}}\omega^{p-1} & \frac{b^p}{c^p}\omega^p & 1\\
 & & & & ... & & & & \\
1 & \frac{b}{c}\omega^{p-1} & \frac{b^2}{c^2}\omega^{2(p-1)} & \frac{b^3}{c^3}\omega^{3(p-1)} & ... & \frac{b^{p-2}}{c^{p-2}}\omega^{(p-2)(p-1} & \frac{b^{p-1}}{c^{p-1}}\omega^{(p-1)(p-1)} & \frac{b^p}{c^p}\omega^{p(p-1)} & 1
\end{pmatrix}$$

The next-to-last column is $(1, 1, \frac{b^p}{c^p}, ..., \frac{b^p}{c^p})$ The first column represents $\frac{b}{a}\frac{x}{y}$ so its valuation at Q or equivalently at q is $-m$, and the last represents $\frac{1}{\frac{b^2}{c^2}\omega - 1}(\frac{b}{c}\frac{z}{y} - 1)$ where we are on components where $\frac{z}{y} = \frac{b}{c}$. So each nonzero entry of the last column represents

$$\frac{\frac{b^2}{c^2} - 1}{\frac{b^2}{c^2}\omega - 1}$$

and its valuation at q or equivalently at Q is $-mp$.

The last column is $\frac{c^p}{b^p}$ times the difference between the next-to-last and the first columns. Thus again one element can be expressed in terms of the other, and we have local topological monogenicity demonstrated without an evident contradiction.

Three elementary conjectures

We have not seen how to rule out every counterexample using a notion of tensor decomposition, but we will not delete the foregoing as it still guides our intuition; at intersection points of components of the Fermat fiber the local monogenicity predicted by understanding the different element can be deduced directly from the hypothesis of existence of the counterexample curve, and yet this looked most surprising when we looked at the cyclic rotation.

1. Conjecture. Let a, b be coprime positive integers, p an odd prime, and let $N = a^{2p} + a^p b^p + b^{2p}$. Let ω be an integer such that $1 - \omega^p + \omega^{2p} \equiv 0 \ mod \ N$. Let j be a positive integer such that

$$j \equiv \omega a \ mod \ N.$$

Then $j \geq ab$.

Remark. The ω such that $1 - \omega^p + \omega^{2p} \equiv \ 0 \ mod \ N$ are just the numbers ω such that ω^p reduces to a primitive sixth root of unity modulo any nontrivial divisor of N with the possible exception of 3, and such that if 3 is a divisor of N then $\omega^p \equiv -1 \ mod \ 3$.

Remark. The conjecture if true would imply the Fermat theorem. Starting with $a^p + b^p + c^p = 0$ with p an odd prime, from the fact $a, b > 0$ we have $c < 0$ and we may take $j = -c$. Then $j = (a^p + b^p)^{\frac{1}{p}} \leq ab$ and we have $j \equiv \omega a \ mod \ N$ where we take $\omega = ja^{-1}$ and it remains to show that ω^p satisfies the equation $1 - T + T^2 \equiv 0$ For

this it suffices to show the same when pre-multiplied by a^{2p} where we are just evaluating $a^{2p} + a^p c^p + c^{2p}$.

If we wish to get rid of any notion of the magnitude of j, instead of reducing modulo expressions like $a^2 + ab + b^2$ we instead conjecture this:

2. Conjecture. Let a be a nonzero integer. Let n be an odd number larger than 1. Then each integer b is uniquely determined by the set of m coprime to a such that $(\frac{b}{a})^n \; mod \; m$ is idempotent.

Here reduction modulo m refers to the reduction map $\mathbb{Z}[1/a] \to \mathbb{Z}/(m\mathbb{Z})$.

Remark. This conjecture implies the Fermat theorem because negating b shows that starting with the assumption that b determines the appropriate set of numbers m, this set does in turn determine $|a^n b^n + b^{2n}|$ while

$$a^n b^n + b^{2n} = a^n c^n + c^{2n}$$

would follow if $b^n c^n + a^n b^n + b^{2n} = b^n c^n + a^n c^n + c^{2n}$ or in other words if $0 = (b^n - c^n)(a^n + b^n + c^n)$. As n is odd and a, b, c are pairwise coprime integers this would be true if $0 = a^n + b^n + c^n$.

Also,

3. Conjecture. Let a, b, c be pairwise coprime integers and p an odd prime. In the cartesian product of cyclotomic fields $\mathbb{Q}[\omega_3] \times Q[\omega_{3p}]$ where ω_3 is a primitive third root of unity and ω_{3p} is a primitive $3p$ root of unity, let $\omega = (\omega_3, \omega_{3p})$ Then the norm of $\frac{a+b\omega}{a+c\omega}$ is not equal to 1.

The final conjecture is not at all new, it is merely a reformulation of Fermat's original assertion, as the norm difference of the numerator and denominator is again $b^p a^p + b^{2p} - a^p c^p - c^{2p} = b^p c^p + b^p a^p + b^{2p} - b^p c^p - a^p c^p - c^{2p} = (b^p - c^p)(a^p + b^p + c^p)$. The notion of a norm ratio equal to 1 is reminiscent of the theory of cyclotomic units and their relation with the algebraic K group K_1. Here we know in detail how it does imply the strong condition of local monogenicity in the completion of the Fermat fiber at each factor of its different element. The locally free module $\mathcal{L}$ has a class in the algebraic K

group K_0. The analogous strenghtening of the K groups in which we do not assume the underlying ring to be commutative already relates to Kaplansky's questions about units, zero-divisors, nilpotent and idempotent elements, which are already significant abstractions of von Neumann's formalization of least-squares analysis.