Overview and a new conjecture.

Combinatorial group theory and Taniyama's conjecture.

The curve $\Gamma_0(N)\backslash\mathbb{H}$ 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 bi-uniquely 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 $z^4 + s_2z^2 - s3z$ 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

$$b = 49$$

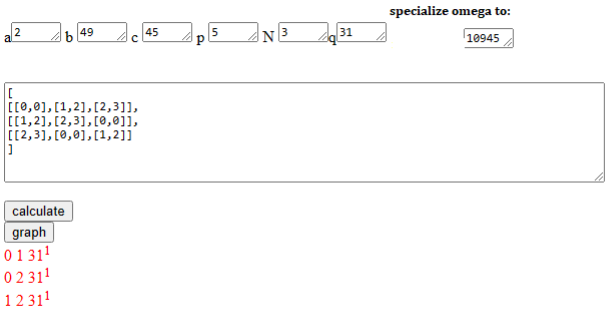
$$c = 45$$

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

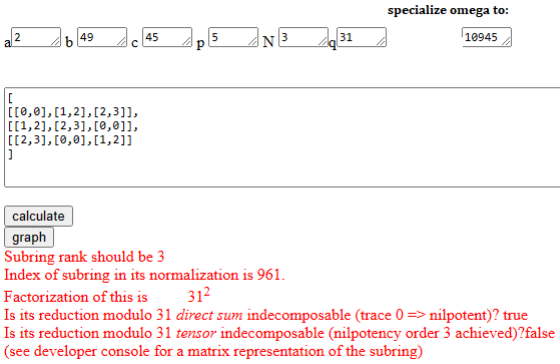
$$(a, b\omega^2, c\omega^3)$$
$$(b\omega^2, c\omega^3, a)$$
$$(c\omega^3, a, b\omega^2)$$

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



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



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 $Z^6 x Z[\omega]^{6p+6}$, 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 nonrational 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

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

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

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

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

$$\frac{-1}{a^{2p}b^{2p}} + \frac{1}{b^p c^p a^p c^p}$$

$$= \frac{-a^p b^p c^{2p} + a^{2p} b^{2p}}{a^{3p} b^{3p} c^{2p}}$$

$$= \frac{a^p b^p - c^{2p}}{(abc)^{2p}}$$

$$= \frac{s_2(a^p, b^p, c^p)}{s_3^2(a^p, b^p, c^p)}$$

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

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

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 $\mathrm{Aff}(F_p)$ 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 $\mathrm{Aff}(F_p)$ 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

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

(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

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

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. 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. An analogous strenghtening of the K groups in which we do not assume them to be commutative relates to Kaplansky's questions about units, zero-divisors and idempotent elements, which were abstractions of von Neumann's formalization of least-squares analysis.