Intuition of the Fermat and related equations

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

$$\beta = b \ mod \ a^p$$
$$\gamma = c \ mod \ a^p \ .$$

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 conditition 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 $\mathrm{Aff}F_p$ 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.