The meaning of positive and negative

Sometimes, in an abstract setting, when one wants to define what it means for a number to be positive, one will say that this means it is a sum of squares.

We all know that if we describe the square root of 2 algebraically, the solutions include two numbers, symmetric under an automrophism, which are negatives of each other. We were taught, if we are to think of positive numbers, one of them is extraneous.

It is a question, related to consistency of arithmetic, whether there is a purely algebraic proof that a sum of nonzero rational numbers which are positive by this definition cannot be zero.

Twisted schemes

When one is considering a subring of $\mathbb{Z}^n$, corresponding to a union of copies of $Spec(\mathbb{Z})$, there do exist nontrivial line bundles on such a union. If we consider two copies of $Spec(\mathbb{Z})$ meeting transversesly at the prime indexed by 5 in both, say, then we can construct a locally principal module by twisting the gluing identification by an element of $\mathbb{Z}/(5\mathbb{Z})^\times$. A twist by 1 or 4 would be inessential, because it lifts to an automorphism of either factor. And a twist by 2 and 3 would have the same effect, but there do exist twists of the free module, and I have not proven that the restricted canonical sheaf is not of this type.

Relation with the canonical sheaf

Let X be 'modular' corresponding to a finite index subgroup of $\Gamma(2)$, not required to be a congruence subgroup. Suppose ω_X is locally free (at non-cusp points). Let ω_0, ω_1 as usual be the basic elements (modular forms of weight to for $\Gamma(2)$, the usual coordinates on $\mathbb{P}^1$). choose numbers A, B, C, D with $AD - BC = 1$ so that the zero point of $A\omega_0 + B\omega_1$ is not a cusp, and let F be the fiber in X that point. Let $\mathcal{L} = \mathcal{M}_2(X)$, our line bundle spanned by ω_0, ω_1.

1. Lemma The residue

$$\delta = Res\ d\ log\ \frac{A\omega_0 + B\omega_1}{C\omega_0 + D\omega_1}$$

corresponds naturally to a section of the restriction to the fiber of $\omega_X \otimes \mathcal{L}^{\otimes 2}$; the ratio $\delta\omega_X^{-1}\mathcal{L}^{-2}$ is naturally an ideal in $\mathcal{O}_F$ and the module of one-forms on F, which is $\omega_X \otimes \mathcal{L}^{\otimes 2}/(\delta\mathcal{O}_F)$, is a locally prinicpal module of rank one over the ring $\mathcal{O}_F/(\delta\omega_X^{-1}\mathcal{L}^{-2})$. Finally, it happens to be prinicpal since the Picard group of $\mathcal{O}_F/(\delta\omega^{-1}\mathcal{L}^{-2})$ is trivial.

This lemma does not need proof, it is a statement of things we've said already, but before having been more vague about naturality.

That is, what I've called the different element ϕ in case the restriction of ω_X to a fiber happens to be principal (I do not know whether it always is), is the generator of the ideal in $\mathcal{O}_F$ which is defined by the formula

$$\Phi = \omega_X^{-1} \otimes \mathcal{L}^{-2} \otimes Res\ d\ log\ \frac{A\omega_0 + B\omega_1}{C\omega_0 + D\omega_1}$$

with $\mathcal{L}$ the line bundle spanned by ω_0, ω_1. It does not matter whether we use a lower case or upper case ω here, one sometimes denotes the canonical sheaf and the other the sheaf of Kahler differentials, but they are identical here as we assume Ω is locally free, an assumption which will be legitimized by inverting an appropriate integer. The fiber F' defined by $C\omega_0 + D\omega_1 = 0$ is disjoint from F and is to be disregarded, though $F + F'$ represents the pullback of the anticanonical class.

Tensor indecomposability

We mentioned that the Fermat curve X maps to the pullback of X/S_3 and $\mathbb{P}^1$ over $\mathbb{P}^1/S_3$, and it follows that the ring $\mathcal{O}_F$, a free abelian group of rank $6p^2$, of the fiber F over a rational (noncuspidal) value of j contains, as finite index within it, a tensor product of one of rank 6 with one of rank p^2.

The construction of the tensor factor of rank 6 depended on $a = -B, b = A$, and c adding to zero.

We can always tensor together the two factors abstractly, to make a ring of rank $6p^2$. However, the relation between adding and taking powers is that we may not embed the Spec of the tensor product as a closed subscheme of any curve with locally principal canonical sheaf unless the direct sum of the pulled back Kahler differentials modules is again locally principal. And, since it is supported on a discrete scheme with trivial Picard group, we may equally say 'principal.' However, we have this lemma.

2. Lemma. Let $\mathcal{F}, \mathcal{G}$ be locally principal sheaves on a Noetherian scheme. Then $\mathcal{F} \oplus \mathcal{G}$ is locally principal if and only if $\mathcal{F} \otimes \mathcal{G}$ is zero.

The proof is just to consider the specialization to one closed point, where we are speaking about one-dimensional vector spaces. Since the sum of the Kahler differentials modules from the separate factors is locally prinicipal (and even principal), it then requires that the support schemes of the two pulled back modules must be disjoint. Being on different sides of the tensor factor even requires

3. Lemma The spectrum of the tensor product of two algebras cannot be embedded as a closed subscheme any curve (over $\mathbb{Z}$) with locally principal canonical sheaf unless the discriminants of the factors are coprime.

Note that it is perfectly possible to embed a finite extension of the spectrum of such a tensor product, so this prohibition disappears after normalizing.

Duality

Let's look at the case $p = 2$. The ring of rank 4 is one which we constructed as a fiber over a λ value. It has a basis the four monomials $1, xy, xz, yz$.

The structure constants of the ring are determined by the rules $x^2 = a, y^2 = b, z^2 = c$, even while the ring does not contain any elements labelled with the letters x, y, z.

It is instructive to write the elements in rows according to the degree in which they previously had in the graded ring, even though there is not any grading anymore. We write

$$xy \quad xz \quad yz$$

$$1$$

and for instance $(xy)(yz) = bxz$.

Our element δ is represented by $(xyz)^{p-1} = xyz$, which is not in the ring. But we can construct a basis of ω_X over the fiber, using the monomials

$$x, y, z, xyz.$$

If we write all the monomials in the rows we have

$$xyz$$

$$xy \quad xz \quad yz$$

$$x \quad y \quad z$$

$$1$$

The rows of even height are sections of $\mathcal{O}_F$ while the rows of odd height are sections of ω_X on F. So for instance the equations

$$(xz)(y) = xyz$$

$$(xz)(z) = cx$$

describe ring elements acting on sections of ω_X and converting them to new sections.

Our different element, over $\mathbb{Z}[1/2]$, is $(xyz)^{p-1} = xyz$, since $p = 2$.

In any such diagram, the monomials in row $p-3$ are g in number where g is the genus of the ambient curve; they extend to a basis of the global sections of ω_X. For instance in case $p = 2$ there are none, and when $p = 3$ the monomal in the same position as 1 corresponds to the unique differential called dz on an elliptic curve.

Transpositions of negative eigenvalue

As for the ring of rank six, working over $\mathbb{Z}[1/6]$, it has different element

$$6(x^2-y^2)(x^2-z^2)(y^2-z^2)(x^2+xy+y^2)^2$$

assuming that $x+y+z=0$.

Here, we can see a picture proof of what this is saying. If we compare

$$[x:y:-x-y]$$

$$[y:x:-x-y]$$

then all three size two minor determinants are $\pm(x^2-y^2)$ In terms of the symmetric group action on $\mathbb{Z}^2$ a transposition fixes two integer lines, one each with eigenvalue $1,-1$.

But because

$$(x^2-y^2)=(x-y)(x+y)=(y-x)z$$

we see that there is an intersection, a congruence, with the cusp, which is the other type of ramification.

After pulling back, we have an equation instead

$$(x^{2p}-y^{2p})=(y^p-x^p)z^p.$$

This is geometrically explaining why the different element of the fiber in $\mathcal{L}^{\otimes 2}\otimes\omega_X[\frac{1}{6p}]$ divided by the different element of the disjoint union of its six parts was

$$6x^py^pz^p(x^p-y^p)(x^p-z^p)(y^p-z^p)(x^{2p}+(xy)^p+y^{2p})^2.$$

That is, it would have been better to write it as

$$6(x^{2p}-y^{2p})(x^{2p}-z^{2p})(y^{2p}-z^{2p})(x^{2p}+(xy)^p+y^{2p})^2.$$

Then the 6 seems to be describing the degree of the branched cover just as the factor of p^2 did on the other side (although this may be a coincidence), and the three next factors describe one each, a fixed line in $\mathbb{Z}^3$ with positive and negative eigenvalue for one of the transpositions, and finally we see the two fixed non rational lines, with eigenvalue $\pm e^{2\pi i/3}$.

'Specialization'

Before, we mentioned that if the fiber F over a λ value has any rational point, then on each of the $p+2$ components of that fiber, each of x, y, z 'specializes' to an integer times a p'th root of unity. More rigorously, each monomial in x, y, z of degree a multiple of p corresponds to an element of $\mathcal{O}_F$, and each rational monomial of degree congruent to zero modulo p also does. These must specialize to p'th roots of the corresponding rational monomials in a, b, c and so must equal the rational p'th root times a p'th root of unity. For example $(x/y)^p - (a/b)$ specializes to zero, and x/y must be one of the roots of $T^p - (a/b)$, which are a rational p'th root of a/b times a root of unity on each component. Then 'specialization' of x, y or z itself is an intersection of fractional ideals induced from $\mathbb{Z}$; the ideals are induced from $\mathbb{Z}$ so is the intersection, defining x, y, or z as an element of $\mathbb{Z}$ up to sign.

The case of a rational solution.

If the fiber has a rational point, then one of the λ values lying over its j value is rational; they are symmetric under S_3 so all six λ values are rational, and fiber over the j value is just a union of six copies of this union of $p+2$ components, intersecting various ways. We may not have the same choices of a, b, c as λ changes, but if there is a rational point in a fiber over a lambda value, then it is true for all the isomorphic fibers over the other lambda values lying over the same j value, that they too have this property, although for each there will be a different permutation.

So x on one component of one fiber may map to "a" times a root of unity and on a component of a part of the fiber lying over a different lambda value, but for the same j, will map to b times a different root of unity.

What that means, though, is that xyz always maps to abc times a root of unity on every component.

The issue about the different element not belonging to the ring is exactly that when we calculate the expression

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

of degree $10p$, each separate term, on each of a, b, c is corresponding to some integer times a root of unity, and here those roots of unity aren't even present in a^p, b^p, c^p. But we must multiply this by the inverse of the fractional ideal on the fiber which is generated by all degree $10p$ monomials. Now, they happen to generate the unit ideal; this has no significance, as it relates to our original choice of section which we call 1 which related to our choice of C and D in the matrix A, B, C, D.

But it means that the different element really is this integer, *under the assumption that the fiber contains a rational point.*

And the other factor $p^2(abc)^{p-1}$, the different element of the disjoint union of the 6 parts, likewise represents an integer times a (plus or minus) p'th root of unity as the different element, and also as an element of the ring, generating the ideal on the other side, describing the support of the ramification on the other branched cover.

So the only subtlety is that as you move around and consider different lambda values correponding to one j value, the factors like $(a^{2p} - b^{2p})$ permute among themselves. But this does not affect the fact that you can factor out $(abc)^p$ and that is constant on all components.

Now, the different elements of the algebras of rank p^2 and 6 were exactly these. This matches the product of the different elements of the two algebras, tells us also that the fiber has the same discriminant as does the tensor product.

Now, the ring of rank four which is the fiber in X/S_3 over j is contained in the ring of rank four over a λ value over j, and we have inverted 6 so that it is isomorphic to the S_3 invariants in the full fiber over j.

When we factorized the different element of the fiber over a rational j value as

$$[(abc)^{p-1}][(a^{2p}-b^{2p})(a^{2p}-c^{2p})(b^{2p}-c^{2p})(a^{2p}+(ab)^p+b^{2p})^2] \in \mathcal{O}_F[(1/6p)],$$

the factor on the left corresponded exactly with the different element of the disjoint union of six fibers over the corresponding λ values; and the factor on the right agrees with the pullback of the different element of the fiber in the λ projective plane over j.

If we actually tensor the coordinate ring of the fiber over one λ value, an algebra of rank p^2, with the coordinate ring of the fiber in the λ projective line over the corresponding j value, an algebra of rank 6, the discriminant of the tensor product would equal the actual discriminant of the whole fiber over the j value, and the two parts would come from tensor factors exactly matching this factorization. They are not coprime because the different element in the second factor can be rewritten, for instance we can factorize out z^p from $(x^{2p} - y^{2p})$, it corresponds to a transposition which interchanges two negative points in the affine cone, and fixes a point in the projective variety.

In fact this illustrates that the affine coordinate ring of a fiber is not the same as the specialization of the affine coordinate ring of a projective variety. Let's discuss this in the next section.

Modules on the fiber.

Let $R = R_0 \oplus R_1 ...$ be the homogeneous coordinate ring of a projective variety by a very ample line bundle $\mathcal{L}$, and let $f, g \in R_d$ be elements of degree d. Suppose that f, g generate $\mathcal{L}^d$.

For each matrix of integers A, B, C, D with $AD - BC = 1$ we can reduce the graded ring R modulo relations $Af + Bg = 0, Cf + Dg = 1$ for $AD - BC = 1$, and obtain the $\mathbb{Z}/d\mathbb{Z}$ graded ring

$$T = R \otimes_{\mathbb{Z}[f,g]} \mathbb{Z},$$

or, we can consider the fiber F of the map to $\mathbb{P}^1$. defined by $Af + Bg = 0$. Let $V = \mathcal{O}_{\mathcal{F}}$. We also have the locally sheaf I on F defined to be

$$I = i^* \mathcal{L},$$

which we can interpret as a locally free module over V.

Then

5. Lemma. There is an equivalence of categories between the category of $\mathbb{Z}/d\mathbb{Z}$ graded modules over T and all modules over V. There is a homomorphism

$$\psi : \mathbb{Z}/d\mathbb{Z} \to Pic(V)$$

such that for each $i \in \mathbb{Z}/d\mathbb{Z}$, the automorphism of the category of T modules which consists of shifting the grading by i corresponds to the automorphism of the category of V modules consisting of tensoring with the ideal $I^{\otimes i}$. We have $T \cong V \oplus I \oplus ... \oplus I^{d-1}$. Finally, if $\phi(1 \ mod \ d) \in Pic(F)$ is zero, there is an ideal $J \subset T$ which is complement of V.

Projective versus affine ramification

The Fermat curve has as its homogeneous coordinate ring

$$e_1 = x + y + z$$

$$e_2 = xy + xz + yz$$

$$e_3 = xyz$$

$$f_p = x^p + y^p + z^p = 0$$

$$f_{2p} = (xy)^p + (xz)^p + (yz)^p$$

$$f_{3p} = (xyz)^p.$$

This can be interpreted as an inefficient system of generators and relators, only one relator is needed. The homogeneous coordinate ring for the line bundle $\mathcal{O}(p)$ on the projective plane consists of terms of degree a muliple of p if x, y, z are given degree 1.

The homogeneous coordinate ring of the specialization at a j is the terms of degree a multiple of p in the ring with two further relations

$$Af_{2p}^3 + Bf_{3p}^2 = 0$$

$$Cf_{2p}^3 + Df_{3p}^2 = 1$$

with A, B, C, D integers with $AD - BC = 1$.

The subrings generated by x^p, y^p includes z^p of course, and it is a copy of the homogeneous coordinate ring of the specialized and unspecialized λ plane. Assume that the λ value is rational, so there is an integer point $[a^p : b^p : c^p]$.

If $\psi(1 \ mod \ d) = 0$ we can ignore the grading, reduce modulo the complementary ideal J, and consider the result to be an algebra over $\mathbb{Z}$. We can construct an isomorphic copy of the rank six subalgebra by writing down as columns the ways of permutating a^p, b^p, c^p

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

and take the subalgebra of $\mathbb{Z}^6$ generated the the three rows. In other words, sending x^p, y^p, z^p to the three rows describes an isomorphism with a rank six subalgebra of the underlying ungraded algebra of the homogenous coordinate ring of the specialized Fermat curve modulo J. The subalgebra has index $(a^p - b^p)^3(b^p - c^p)^3(c^p - a^p)^3$ in $\mathbb{Z}^6$. As an abstract un-graded algebra once reduced modulo J and tensored with $\mathbb{Z}[1/((a^p - b^p)(b^p - c^p)(c^p - a^p))]$ it decomposes into a cartesian product of six copies of that base ring, containing six different primitive idempotent elements. Let Y be the scheme in the $\mathbb{P}^1$ which parametrizes λ values, corresponding to this j The very ample line bundle for this rank six subalgebra is one of the p^2 summands of the pushforward of $\mathcal{O}(p)$ on F, giving the implication for the maps

$$\psi_F : \mathbb{Z}/(6\mathbb{Z}) \to Pic(F),$$

$$\psi_Y : \mathbb{Z}/(6\mathbb{Z}) \to Pic(Y),$$

$$\psi_F(1 \ mod \ 6) = 0 \Rightarrow \psi_Y(1 \ mod \ 6) = 0.$$

This in turn implies that $Y \subset \mathbb{P}^1$, once $(a^p - b^p)(b^p - c^p)(c^p - a^p)$ is inverted, will consist of six disconnected copies of the localized $Spec(\mathbb{Z})$.

Then the whole fiber F, the inverse image of Y, correspondingly decomposes into a disjoint union of the copies over the six individual λ values.

We calculated the different elements of the disjoint union, which was $p^2(abc)^{p-1}$. The different element of the whole fiber was $6p^2(abc)^{p-1}(abc)^p(a^p - b^p)(a^p - c^p)(b^p - c^p)(a^{2p} + (ab)^p + b^{2p})^2$. The factors $(a^p b^p c^p)(a^{2p} + (ab)^p + b^{2p})$ where a^p, b^p, c^p are rational integers, must then be divisors of a power of $6p(a^p - b^p)(a^p - c^p)(b^p - c^p)$. Thus

6. Theorem. For every rational value of j which lifts to a rational λ value, let F_j be the fiber over j in the Fermat curve. The element $\psi(1 \ mod \ 6) \in Pic(F_j)$ cannot zero except, possibly in special cases when $j \in \mathbb{P}^1$ is one of the three cusps or each of a^p, b^p, c^p is a power of $2, 3$, or p.

The case $p = 1$.

We are still assuming that there is a rational λ value. The fiber over j is a subscheme of $\mathbb{P}^2$ comprised of six copies of $Spec(\mathbb{Z})$, and the different element, a section of $\mathcal{O}(10)$ is perhaps best written now

$$(xy - yz)(yz - zx)(zx - xy)(xy + yz + zx)(yx + xz + zy).$$

This is a tensor product of five sections of $\mathcal{O}(2)$, and in the restriction to each irreducible component, it describes the five Cartier divisors where that component meets the five other components. The components are in two sets of three, and the decomposition is preserved by all the permutations. Note that the last two factors are equal. Two components of the same type (transformable to each other by an even element of S_3) meet each other only at the subscheme where $xy + yz + zx$ is zero, but there are two such subschemes, interchanged by any transposition. The Cartier divisor defined by this section is principal, being defined also by the rational integer $(ab - bc)(bc - ca)(ca - ab)(ab + bc + ca)(ba + ac + cb)$.

Since this section of $\mathcal{O}(10)$ or indeed the product of the first three and last four factors separately, describe a principal Cartier divisor, it seems likely that so does $\mathcal{O}(2)$ and that $\psi(2 \ mod \ 6) = 0$.

The case $p = 2$

It seems that, rather than using localizations, we can find a useful simplification by using partial normalizations which are a local isomorphism near a subscheme of interest, defining a type of etale neighbourhood (I'm not sure if I'm using the correct word here).

Since $p - 1 = 1$, the different element

$$(xyz)^{p-1}(x^2y^2 - y^2z^2)(y^2z^2 - z^2x^2)(z^2x^2 - x^2y^2)(x^2y^2 + y^2z^2 + z^2x^2)^2$$

again has an easy interpretation. The last five factors tensor together to give a section of $\mathcal{O}(20)$ which is just what we've seen already, just pulled back from the λ projective line. Any one of the 24 components belongs to a fiber over one λ value, and we already know that that fiber consists of four irreducible components, each meeting the other three transversely according to the Cartier divisors x, y, z one each. But also now we have intersections when one of the four components for one λ value meets one of the four components for another λ value.

Explicitly, the ring of rank 24 can be constructed as the subring of $\mathbb{Z}^{24}$ which is the image of the homogeneous polynomials of degree a multiple of 12 where we send $p(x, y, z)$ to a tuple

$$(p(a, b, c), p(-a, c, b), ...$$

where included is every possible permutation or assignment of signs to a, b, c which is essentially different (negating all variables is an inessential change).

The different element is not given to us as an element of this ring. Let's look at just some factors of the different element.

$$x(z^2x^2 - x^2y^2) = x \otimes x^2 \otimes (z^2 - y^2)$$

We can do a partial normalization so that we can ignore other factors of the different (and $c^2 - b^2$ is coprime to a^2) and arrive at a triple intersection point where our one component meets one other component lying over the same λ value, and two components over different λ values, and the remaining different element is $x \otimes x^2$.

I believe that the x^2 on the right is there because after a transposition, there is a meeting between the conjunction of two components in the one fiber and a symmetrically opposite conjunction of two components over the other λ value.

Now there are four components, and the coordinate ring of their union as the subring of $\mathbb{Z}^4$ spanned by all

$$(p(a,b,c), p(-a,b,c), p(a,c,b), p(-a,c,b))$$

for $p(x,y,z)$ homogeneous of degree a multiple of 12.

A neighbourhood of the relevant subscheme – the one defined by a in our originally chosen component, is isomorphic to a neighbourhood of the same scheme in the whole fiber.

The ring is the image of the invariants of the Klein four group acting on the cartesian product of four copies of $Spec(A)$ where A is the ring comprising all homogeneous polynomials of degree divisibe by twelve in $\mathbb{Z}[x,y,z]$. The group is generated by two elements τ, σ with

$$\tau(p(x,y,z), q(x,y,z), r(x,y,z), s(x,y,z)) = (q(-x,y,z), p(-x,y,z), s(-x,y,z), r(-x,y,z))$$

$$\sigma(p(x,y,z), q(x,y,z), r(x,y,z), s(x,y,z)) = (r(x,z,y), s(x,z,y), p(x,z,y), q(x,z,y)).$$

The rough intuition should be that multiple intersections cause split extensions of one forms rather than nontrivial extensions.

The Klein four group actually acts on our rank 24 ring, that action is just induced by permutations of the factors in $\mathbb{Z}^{24}$.

The images of particular types of polynomials (of various degrees in the grading and transforming according to particular characters) describe the four eigenspaces in the algebra. Without a different type of understanding of it, we cannot see a contradiction to the notion that the one forms module is principal. It seems most likely that from the direct description we would deduce that it is a copy of the augmentation ideal of the group algebra $\mathbb{F}_p K$ for K the group, whereas local principality of ω_X would force that it is a copy of $\mathbb{F}_p K$ modulo the augmentation ideal.

Let's consider this type of question without the hypothesis of a group action in the next section.

Local rings and principal differentials

7. Theorem. Let R be a local Noetherian ring containing $\mathbb{Z}$. Let m be the maximum nonunit ideal of R and suppose $\mathbb{F}_p \subset R/m$ is surjective (equality). Suppose Ω_R is a principal module. Then there is an element $\eta \in m/m^2$ so that

$$m/m^2 = \mathbb{F}_p(p \ mod \ m^2) \oplus \mathbb{F}_p\eta.$$

Proof. First we write

$$m/(m^2 + pR) \to \Omega_R \otimes_R \ R/m$$

$$m \mapsto dm.$$

This is well-defined because if $q, s \in m$

$$d(qs) = ds \otimes q + dq \otimes s = ds \otimes 0 + dq \otimes 0 = 0,$$

and for $r \in R$

$$d(pr) = dp \otimes r + dr \otimes p = 0 \otimes r + r \otimes 0$$

the last because $p \in m$.

It is also surjective because $\mathbb{Z} + m = R$, as this surjects onto $\mathbb{F}_p$ and contains the kernel of $R \to \mathbb{F}_p$.

Finally let's show the kernel of this map is zero. A linear combination of dm which maps to zero, would be reducible to zero by the Leibniz relation $d(rm) = dm \otimes r + dr \otimes m$. For r which belong to m it just says $d(rm) = 0$. In the remaining terms r can be replaced by an integer, and the relation asserts no more than that d commutes with addition. An expression reducible to zero by the relation must already be zero.

Now, if Ω_R is principal, so is $m/(m^2 + pR)$ and we may choose a single element $\eta \in m/m^2$ mapping to a generator. Then $m/m^2 = \mathbb{F}_p(p \ mod \ m) \oplus \mathbb{F}_p\eta$.

8. Corollary. Under these conditions, if in addition $R/(pR)$ has p^m elements, $R/(pR) \cong \mathbb{F}_p[T]/(T^m\mathbb{F}_p[T])$.

Proof. It is a finite local $\mathbb{F}_p$ algebra with residue field $\mathbb{F}_p$ and principal maximum ideal.

9. Corollary. Let X be a curve over $\mathbb{Z}$ and x a closed point such that that ω_X is (locally) principal in a neighbourhood of x. Suppose that there is a rational prime p so that where the residue field at x is $\mathbb{F}_p$. Suppose that R is isomorphic to the local ring at p of the subring of $\mathbb{Z}^m$ for some number m which is $\{(n_1, ..., n_m) : n_1 \equiv n_2 \equiv ... \equiv n_m \ mod\ p\}$. Then $m = 1$ if x is a nonsingular point of $Spec(R)$ and otherwise $m = 2$.

Proof. When we localize at p, the maximum ideal of such a ring is its intersection with the ideal generated by $(p, p, ..., p)$ in $\mathbb{Z}^m$, but it has minimal generating set $\{(p, 0, 0, .., 0), (0, p, 0, 0, ..., 0), ..., (0, 0, 0, 0..., p)\}$ in the smaller ring. If m is the maximal ideal, these form a basis of m/m^2, whose dimension must be at most 2.

The case $p = 2$. Beginning of the proof.

We actually construct the subring of $\mathbb{Z}^4$ which we mentioned, spanned, for all monomials $m(x, y, z)$ of degrees a multiple of $6p = 12$, by the

$$(m(a, b, c), m(-a, b, c), m(a, c, b), m(-a, c, b)).$$

For example for $a, b, c = 3, 5, -8$, chosen at random, we obtain[1] the ring with basis

$(1, 1, 1, 1)$
$(0, -6, -160123546270109207662978759452839116799999944378468394 1, 160123546270109207662978759452839116799999944378468393 5),$
$(0, 0, -39, -158287728857484136338279553561597748991080982044313953660613499061446209860493452838857581 5),$
$(0, 0, 0, -234)$

[1] assuming things stabilize after degree 108, and thanks to Matt Crumley http://silentmatt.com/ for putting BigInteger.js on sourceforge!

The multiplication operation is component-wise integer multiplication, and a matrix representation of the ring is given by the four matrices (shrunk so they fit on the page)

When these are reduced modulo $a = 3$ they become

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

The last three are a basis of the maximal ideal, which is nilpotent of order only three, not four. Then as the conclusion of Corollary 8 does not hold, it is impossible for such a ring to exist at a closed point of the quadric where the differentials are locally free.

The numbers $3, 5, -8$ are not numbers whose squares add to zero (they happen to add to zero themselves instead). We cannot test what the construction would do if we applied it to three nonzero numbers whose squares add to zero, becuase no such triple of numbers is known.

The point about the partial normalization is that it was an isomorphism on the local ring level. Before I had been trying inverting integers. This is implicitly inverting coordinate functions somewhere ambiently, but it is just easiest to consider that we can take a partial normalizatin that does not affect a neighbourhood of the closed point we're considering.

The index of this ring in its normalization is divisible by a^4, it is $4(b-c)^2a^4$ many (but not all) examples. Such a ring is not just having the relations saying that the four integers are mutually congruent mod a. There is one more relation.

Our quick way of verifying that there is no element η in the max ideal so that $m/m^2 = F_p(p\ mod\ m^2) \oplus F_p\eta$ was to mod out by p and see if you get the only type of algebra that maps to $\mathbb{F}_p$ and has principal maximum nonunit ideal.

Those four 4×4 matrices, we'd have to make η out of a linear combination of those, yet every linear combination of those is nilpotent of order less than four.

There are examples where the index of R in $\mathbb{Z}^4$ is smaller than a^3 while the spectrum is not connected.

So, even though we can't – apparently – find 3 nonzero numbers whose squares add to zero, to test this, the only thing that is in contention is the argument which said that those four components would have to meet.

This is where we did need the different element calculation. Since the ideal in $\mathcal{O}_F$ (really the different element times the inverse of ω_X) is induced from the characteristic subring locally, and the part we are considering which is $(xyz)^{p-1}$ times $(xyz)^p$ is invariant under symmetry, this is induced from the characteristic subring globally.

Then, those two components over one λ value that meet at the subvariety defined by the integer a in both, the different element from the disjoint union of the six parts gave that ignoring other components this is an intersection defined in each by just $a^{p-1} = a$.

The other factor, if we just interpret it as we may using the specialization technique, gives us $a^p = a^2$.

This is part of a symmetric expression, so no matter which component we look at it is constant a^2.

That means this double intersection must meet components at this same subvariety of $Spec(\mathbb{Z})$ which are on other parts of the six, i.e. over other lambda values.

And because it is the subvariety defined by a, and not something like $b - c$, or $(ab + bc + ca)$ it has to come from a transposition of negative eigenvalue.

It is really hard to see numerically how this could happen.

But, the point is to make a clear proof that it cannot happen.

We know, provably, and from examples, that if that local ring R at the closed point at a prime dividing p into a has that R/pR is anything other than $\mathbb{F}_p[T]/T^m$ for some m, that this will never occur.

In examples if we put in random numbers for a, b, c in every case when the four components actually meet at a, it is not of type $F_p[T]/T^m$.

But it still needs a proof, that, to make it easier, if the subring R of $\mathbb{Z}^4$ spanned by all four tuples

$$(m(a,b,c), m(-a,b,c), m(a,c,b), m(-a,c,b))$$

for m ranging over monomials a multiple of 12, the a-primary component of the index divisible by a^3, then the order of nilpotency of the image of that maximum ideal is at most three.

Thus, to be clear we can state it as a conjecture:

Conjecture. Let a, b, c be pairwise coprime and ≥ 2. Let R be the subring of $\mathbb{Z}^4$ spanned by all

$$(m(a,b,c), m(-a,b,c), m(a,c,b), m(-a,c,b))$$

for which m is a monomial of degree a multiple of 12. Let q^e be the highest power of a prime q dividing a. Suppose that R contains no idempotent element besides 0 and 1 (which I think is equivalent to saying $[\mathbb{Z}^4 : R]$ is divisible by q^{3e}). Let m be the kernel of $R \to \mathbb{F}_q$. Then the conjecture is that the order of nilpotency of the image of m in R/qR is no larger than 3.

It is this conjecture which implies that $a^2 + b^2 + c^2$ cannot be zero.

For, if $a^2+b^2+c^2 = 0$ the different calculation would tell us that R is connected, a local ring rather than semi local. Then the conjecture tells us that the order of nilpotency is no more than 3, and this means that R/pR can't have a principal max ideal. Then the max ideal of R cannot be generated by p and one other element, and therefore the Kahler differentials the local ring cannot be principal. Then it cannot occur on the quadric $a^2 + b^2 + c^2 = 0$.

In other words, we still have to show that this always happens under the hypotheses which we've established would be true under the hypothesis of existence of a noncuspidal rational point.

Overview of a proof.

It is interesting to see that the calculation of the subring of $\mathbb{Z}^4$, in examples, when it has index divisible by a^3 the order of nilpotency modulo a prime divisor of a is never as much as four. Even for the Fermat triples one sees this. For $5, 4, 3$ with a playing the role of 5, the index in $\mathbb{Z}^4$ is divisible by a^2 only, and for $3, 4, 5$ the index is divisible by a^3 but the order of nilpotency is three.

Here is an overview of the proof which is at hand. It's just a matter of explaining how the parts fit together.

Twisted modules.

The issue here was that I can make a ring where two copies of $Spec(\mathbb{Z})$ are glued along $\mathbb{Z}/5\mathbb{Z}$. This just means the *ring* is pairs of numbers congruent mod 5. But a *module* can be pairs of numbers with one double the other mod 5.

This seems like a harmless difference but if we do not know a priori that the restriction of $\mathcal{O}(p)$ to a fiber isn't like that, we have not a method of generators and relators to describe the ring structure.

Structure of fiber

We know that only particular very restrictive combinatorial types can occur. We don't know much about the Fermat fiber combinatorial type, but the fact that the thing analytically is a pullback is suspicous because it can't be algebraically if it is to have a rational point, for the same reason 2 partial derivatives of a 2 variable function can't both be zero at a point of a smooth curve they define.

However because of the previous point, it would be beyond computer calculation to know anything at all about the whole thing.

S_3 symmetry and different element and 'Specialization.'

These are going to be used only because, in combination, they tell us which components meet which others at which points. They imply that there has to be a configuration of four components meeting at one point. Then the partial normalization which is the image of the (actual) coordinate ring in $\mathbb{Z}^4$ is a partial normalization faithfully representing the relevant local ring and we know a priori it is connected, i.e. a local ring not semilocal.

Because $\mathcal{O}(p)$ is not principal, the different element doesn't reliably tell us everything but the multiplicity of (abc) is reliable since it is constant everywhere hence induced from the characteristic subring.

Then once we know this, we can discard the S_3 symmetry, ignore the different element.

Degree of nilpotence, index in normalization.

We can get away using only limited information now. The S_3 symmetry etcetera told us that the thing is connected so we can assume the index of the subring of $\mathbb{Z}^4$ is at least divisible by the thrice the power of primes dividing a. And embeddability requires that the ring mod q for such a prime q has to be of the type $\mathbf{F}_p[T]/T^4$, i.e. the order of nilpotency of the max ideal of the ring mod p has to be the maximum value of 4.

We now can throw out the assumption of any K_4 symmetry.

Structure of argument

Now we are down to a question about subrings R of $\mathbb{Z}^4$, and for each a, b, c we have a description of it, it is the span of $(m(a,b,c), m(-a,b,c), m(a,c,b), m(-a,c,b))$ for m monomials in a, b, c of degree a multiple of 12. If we can prove that for a prime power divisor q^e of a, when its index is at least divisible by q^{3e} (and that it disconnected otherwise) the degree of nilpotency of the max ideal of R/p is less than 4, we are done with the quadric.

Even these rings for things like the Pythagorean triples $3, 4, 5$, are beyond hand calculation. But we've preserved the absurdity of having a very high intersection multiplicity geometrically, with a high order of nilpotency mod p.

We've needed to make essential use of the S_3 symmetry and the existence of a rational point, and in some ethical sense we have seen from the beginning why these contradict each other but now even in this more focussed algebraic question, it is beyond hand calculation to solve it.

But it is absurd except in weird special cases to have high nilpotency *and* high number of components. It is a matter of showing that this class of subrings of $\mathbb{Z}^4$ is far enough from generic to include any sort of weird counterexample like that. Just throwing random numbers in for a, b, c one sees basically two patterns, where either the index is divisible by a^2 only and it is disconnected, or divisible by a^3 or a^4 and the degree of nilpotency is three.

Beginning of the proof for general primes p.

Let's construct the whole map $\mathbb{Z}/((6p)\mathbb{Z}) \to Pic(F)$ and the coordinate ring of the fiber. Orbit representatives for $\mathrm{Aff}(F_p)$ acting on F_p^3 consist of the triples (i,j,k) such that $i = 0, j \in \{0,1\}$, and if $j = 0$ then $k \in \{0,1\}$. These are $p+2$ in number. We can make a matrix with columns obtained from (a,b,c) by applying any permutation and any assignment of p'th roots of unity with exponents prescribed by the orbit representatives, and let x, y, z be the three rows. Thus for example if $p = 5$

$$x = (a, a, a, a, a, a, a, b, b, b, b, b, b, b, a, a, a, a, ...)$$
$$y = (b, b, b\omega, b\omega, b\omega, b\omega, b\omega, a, a, a\omega, a\omega, a\omega, a\omega, a\omega, c, c, c\omega, c\omega, ...)$$
$$z = (c, c\omega, c, c\omega, c\omega^2, c\omega^3, c\omega^4, a, a\omega, a, a\omega, a\omega^2, a\omega^3, a\omega^4, b, b\omega, b, b\omega, ...)$$

The coordinate ring of the fiber over the corresponing j value is the free commutative group J spanned by all monomials of degree multiples of $6p$ in the three elements x, y, z in its normalization $\overline{J} = (\mathbb{Z} \times \mathbb{Z}[\omega]^{p+1})^6$. The commutative subgroup $\mathcal{L}$ of the $\overline{J}$ spanned by monomials in x, y, z of degree congruent to 1 modulo $6p$ is a rank one projective module over J, and the map

$$\mathbb{Z}/(6p\mathbb{Z}) \to Pic(J)$$

sends i to $\mathcal{L}^{\otimes i}$ which is represented as the span of monomials in x, y, z of degree congruent to i modulo $6p$.

Thus the elements of x, y, z do not belong to J, they belong to the sections module $\mathcal{L}$ of a line bundle and for example if we choose the section x, the module $\mathcal{L}/(x)$ is locally cyclic; on any open set where $\mathcal{L}$ restricts to a free module, the ring of endomorphisms $End(\mathcal{L}/(x))$ is a commutative algebra and its $Spec$ is the principal divisor where the divisor of x is trivialized on the open subset.

The different element is a section of $\mathcal{L}^{\otimes 13p-3} \cong \mathcal{L}^{\otimes p-3}$ and its divisor describes on each of the $6 + 6(p+1)$ irreducible components of the fiber, the locus where that component meets the union of the other components. Because it is a symmetric polynomial, if we interpret it as just an element of $\overline{J}$, it evaluates to a p'th root of unity in that ring times the rational integer

$$p^2(abc)^{p-1} \cdot 6(a^p b^p - b^p c^p)(b^p c^p - c^p a^p)(c^p a^p - a^p b^p)(a^p b^p + b^p c^p + c^p a^p)(b^p a^p + c^p b^p + a^p c^p)$$

where note the first factor after the $\cdot$ is divisible by $(abc)^p$, and the last two factors are equal.

We only interpret it as an element of $\mathbb{Z}[1/(6p)]$ (so the factors of p^2 and 6 don't matter) and in that sense, this number raised to the $\frac{1}{2}(6+6(p+1)(p-1)) = 3p^2$ power must be the index $[\overline{J} : J]$, as an element of $\mathbb{Z}[1/(6p)]$ well defined up to multiplication by a unit.

Also the fact that it is a rational integer times a root of unity in the normalization means that $Spec(J)$ has a type of symmetry, the locus where each component meets the union of others is induced from a rational integer.

The fiber is the union of the fibers over the six lambda values lying over j, and the different element of each part of the disjoint union is the part of the expression before the $\cdot$. Because we can rearrange the second part to be a multiple of $(xyz)^p$ which is not coprime to the first part, something has to change locally at the point where two components over one λ value meet, when unioned with the components over some other λ value.

It may be surprising that compoents lying over distinct λ values can meet, but this is what the different element implies, and we can see this by ignoring all but four components, writing instead

$$\begin{array}{c} x = (a, a, a, a) \\ y = (b, b\omega, c, c\omega) \\ z = (c, c\omega, b\omega, b\omega^2) \end{array} .$$

We may take J to be the span of monomials of degree congruent to zero modulo $2p$ and $\mathcal{L}$ to be the span of monomials of degree congruent to 1 modulo $2p$. For any prime divisor q of a there is a prime lying over q in each component of the normalization whose intersection with J is one and the same maximal ideal. We can embed the coordinate ring of the first coordinate $\mathbb{Z}$ in $\mathbb{Z}[\omega]$ and then apply Galois automorphims to the four components to bring the ideals to the same place, and then (after exponentiating ω separately in each of the four components) we just seek a single maximal Q with $q \in Q \subset \mathbb{Z}[\omega]$ such that the size two determinantal minors belong to Q. The whole first row does and two of the remaining minors have determinant zero, so it is just ensuring $b^2\omega - c^2 \in Q$. If we call the correspnding maximal ideal of J by the name $\mathcal{Q}$ – it is the inverse image of Q under the projection to any component – and if we call the local ring at $\mathcal{Q}$ by the name $J_{\mathcal{Q}}$, we have seen that for $p \neq q$ smoothness of the Fermat curve requires $J/(qJ_{\mathcal{Q}}) \cong F[T]/(T^m)$ for F a field and m the dimension of that algebra. In fact this also can be deduced directly from the fact that the single element y/z generates an algebra which is dense in the completion of J at $\mathcal{Q}$.

For each of the other factors of the different we can do a similar local calculation. For the factor which is the second elementary symmetric function $s_2(a^p, b^p, c^p)$ we obtain each of x, y, z by multiplying each row of

$$\begin{matrix}(a, b, c)\\(b, c, a)\\(c, a, b)\end{matrix}$$

by a p'th root of unity in $\mathbb{Z}[\omega]^3$. The Fermat hypothesis implies a, b, c are coprime to $s_2(a^p, b^p, c^p)$ and indeed x, y, z are coprime to that integer. The projective module $\mathcal{L}$ is spanned as a commutative group by monomials in x, y, z of degree congruent to 1 modulo $3p$, and the condition which the roots of unity must satisfy for the three components all to meet is that if we take our maximal ideal to be the same Q on each component, the entries of x/y – an element initially of the semilocalization of J at q – which are of the form

$$(\frac{a}{b}\omega, \frac{b}{c}\omega', \frac{c}{a}\omega'')$$

must themselves have ratios in the same proportion modulo Q. Thus it concerns ratios between ratios. The p'th power of each entry is a cube root of unity modulo Q and it is a nontrivial cube root of unity because q is coprime to $(a^p - b^p)(b^p - c^p)(c^p - a^p)$. Then each entry modulo Q is a product of a possibly trivial p'th root of unity and the same nontrivial cube root of unity τ, and is a $6p$ root of unity. Again the completion of the subalgebra at $\mathcal{Q}$ is topologically generated by just the element $\frac{y}{z}$ and we can re-deduce $J_{\mathcal{Q}}/(qJ_{\mathcal{Q}})$ is of the type $F[T]/(T^m)$ as we predicted. The reason there were two such factors in the different is because there are two types of rotations of a, b, c.

When we do look at the factor $(a^p - b^p)(b^p - c^p)(c^p - a^p)$ it defines a locus containing closed points where components over distinct λ values meet but just in pairs I think.

In all cases, if we choose a maximal ideal $\mathcal{Q} \subset J$ correspnding to a point of intersection between four components, in the case of a transposition, or three components, in the case of a rotation, and complete each component of the normalization at its corresponding maximal ideal, we find that J is contained in the prime subring, the completion $\mathbb{Z}_q$ of the rational integers $\mathbb{Z}$ at the rational prime contained in Q. That is to say, although individual components of J can have nontrivial residual extensions when we complete at prime ideals of $\mathbb{Z}\omega$, there is no nontrivial residue field extension when we complete at maximal ideals coming from these particular intersection points, and the whole of the correspnding ring J (the whole of the projection on these components) is contained in $\mathbb{Z}_q^m$ where m is the rank. For example, if q is a divisor of a and we take the two meeting components where

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

then $b^2\omega^j - c^2$ must belong to the prime ideal Q in the third component forcing ω to reduce modulo Q to an integer (note b, c are coprime to q by the Fermat hypothesis).

Therefore the completion of J at Q is a subalgebra of a complete ring $\mathbb{Z}_q^m$ and it contains $\mathbb{Z}_q \cdot (1,1,1,..,1)$. The powers of any monomial in x, y of degree congruent to 1 modulo $6p$ form a van-der-monde matrix, its determinant is prime to Q. For instance the entries of powers of $x^{6p+1}y^{6p-1}$ which we may write $\frac{x}{y}$ in $\mathbb{Z}_q^m$ form a van-der-monde matrix, its determinant is prime to q if q is a divisor of $s_2(a^p, b^p, c^p)$ or of $s_3(a^p, b^p, c^p)$ and it follows that if the entries of $\frac{x}{y}$ are distinct, that one element generates the algebra topologically, which is then the closure of $\mathbb{Z}_q[\frac{x}{y}]$ in $\mathbb{Z}_q^m$. By Artin-Rees some power of $\mathcal{Q}$ is trivial modulo $qJ_{\mathcal{Q}}$ and therefore $J_q/(qJ_{\mathcal{Q}})$, a homomorphic image of the completion, is generated by one element over F_q, and is isomorphic to $F_q[T]/(T^m)$ where m is the number of components meeting at $\mathcal{Q}$.

I had expected anomalous behaviour when two components over one lambda value meet two components over a different lambda value, because classically analytically they cannot meet, and if the could, one would expect a tensor decomposition, and this finite algebra could not be monogenic. Now we have proved it to be from elementary principles.

What I had expected was that we'd see a tensor decomposition preventing a rational point from existing, analogous to why one cannot speak of a single ground state electron, when an emission line of an atom is labelled by two term symbols, unless one of the symbols is type S. I had made a similar mistake before: Robert May had used Lotka-Volterra to contradict a report claiming that a new road subdividing a natural park would benefit species diversity. I had wanted to model virtual animals springing into existence when a road were removed, had not understood that the idea was not 'let's all use Lotka-Volterra from now on.' In that sense, every model is a disaster model.

We now understand the what must have been the precise and full isomorphism type of the Fermat fiber over one rational j value if it existed and need to think further. There might be global contradiction involving the isomorphism types of projective modules. There is no 'local' contradiction. Also, the things I am saying here have been checked in many examples on the computer; and I have carefully written down the theory of the different element in terms of logarithmic differentials and residues. It seems almost identical to the theory of dualizing sheaves, we describe a global section of a line bundle whose restriction on affine parts is rigorously proved to be a Noether different.

The assumption that our permutations of a, b, c are merely discrete would be removed if we think about monodromy a little. We can understand Weierstrass models in terms of line bundles if we wished; we can think of λ as an integer point of the projective line which is variable. One way to do this is to imagine $[x : y]$ as ratios of two sections of a line bundle over $\mathbb{P}^1$, and the one-point compactification of that line bundle is precisely $\mathbb{P}^2$.

This expresses $\mathbb{P}^2$ as the result of contracting an exceptional line in a $\mathbb{P}^1$ bundle over $\mathbb{P}^1$, and each line in the line bundle embeds although the image of all the projective lines in the line bundle is the pencil of lines through one point of $\mathbb{P}^2$. We can speak of the cross ratio of $0, x, y, \infty$ in each line fiber, and this is a λ value of the elliptic curve which double covers the projective line fibers at those points, however, it is not possible to simultaneously double cover all the lines to create a surface, even after blowing up the base locus of the pencil to create the surface, because the class of the union of the four lines is not even in the Picard group. In 'Primer on Elliptic Curves' I called this Weierstrass' mistake. It means we cannot easily extend our analysis of principal parts and the different element.

A similar problem afflicts the nicest 'universal bundle' approach. Once chosen four points of the Riemann sphere, we can allow them to vary in a complete linear system. This means we embed the Riemann sphere as a degree-four rational curve in $\mathbb{P}^3$ such that the four points are the intersection with a hyperplane, and then all possible configurations of four points with multiplicity correspond to all possible hyperplanes, the dual projective three-space $\mathbb{P}^{3*}$.

There is a natural hypersurface in $\mathbb{P}^3 \times \mathbb{P}^{3*}$ consisting of incident pairs of a point and hyperplane, the hypersurface describes a $\mathbb{P}^2$ bundle over $\mathbb{P}^3$. Its intersection with our Riemann sphere in the first component cross the whole of $\mathbb{P}^{3*}$ in the second describes a degree-four branched covering of $\mathbb{P}^{3*}$ contained in the trivial $\mathbb{P}^1$ bundle, but again here the divisor is not even, and we cannot construct a 'universal' bundle of elliptic curves this way.

In 'Primer on elliptic curves' I mentioned a slightly more involved construction. In simplest terms, to form the branched cover of $\mathbb{P}^2$ over four fixed and general lines not containing a point, and fiber by a pencil of lines through that point.

Choosing four global sections of the line bundle with section sheaf $\mathcal{O}(1)$ on the Riemann sphere is the same as choosing four lines in $\mathbb{P}^2$ not through one point, because $\mathbb{P}^2$ is the one-point compactification of that line bundle. In turn, there is a global section of a line bundle of type $\mathcal{O}(4)$ on $\mathbb{P}^2$ which meets $\mathbb{P}^2$ as the zero section at these four lines, and its inverse image under the map of line bundles which induces $\mathcal{O}(2) \otimes \mathcal{O}(2) \to \mathcal{O}(4)$ is a projective elliptic surface; instead of meaninglessly permuting a, b, c there is the period map sending each point of the Riemann sphere in the base, or, rather, a six-sheeted cover over that Riemann sphere when six coincidence points are deleted, to the cross-ratio of the four distinct points where the closure of the line fiber over that point meets each of the four lines.

Two general lines of each 'slope' in $\mathbb{P}^2$ correspond to the same cross-ratio and so there is a degree-two period map $\mathbb{P}^2 \to \mathbb{P}^1$ which must be considered.

It would be an interesting project to bring the arithmetic analysis we've done just for one fiber of the Fermat curve into the projective elliptic surface.

Use of scheme theory.

It was really somehow helpful to visualize things like $Spec(\mathbb{Z})$ as a subset of the Riemann sphere even though it is not. When particular closed points are considered, there they are analytically, right in the point where you had to visualize them. The issue is similar to applying a Galois automorphism to $\mathbb{Z}[\sqrt{2}]$ and worrying about the discontinuity of it, and it is tempting to work in $\mathbb{R}[T]/(T^2-2)$ and use the classical topology, things like the analytic class number formula. To use lattices and volumes, and the Euclidean norms. But there is now a second tradition which is very different from doing that.

The second tradition has to do with a type of vague attempt to make things more symmetrical under dualizing, to imagine that integers are functions with domain some type of hybrid anaytic object. It is known that it is still totally rigorous to use differential calculus on these things but it is disturbing that something seems dishonest or ghostly about the visualization of $Spec(\mathbb{Z})$.

Without wanting to be pretentious about it, I'd say that it is evidence of self-deception in the past, an un symmetrical division between discrete things and continuous things; between analysis and algebra.

Conclusion.

I wasn't going to send any more of these to anyone, hard-copy pdf's, but here is why I changed my mind about it.

One thing is, even though it's probably still wrong, I haven't actually deleted any pages, each missing part just got added...

Different things...I looked up Olga Taussky-Todd's article about sums of squares. Very responsible, thorough, hard-working it is, ... No matter how old or tired she is, how much she's had to do, you know she's going to read even Mazur, Artin, all the new things, include a really intelligent synthesis, and finish it by the time of the article deadline.

Also was thinking about how we lost a Teaching Quality Assessment point; I had been assigned to be the 'Aims and Objectives Barber of Seville,' to write aims and objectives for everyone who didn't write aims and objectives for himself.

It is actually hilariously funny, we lost the point because my own work was in the Aims and Objectives room. The inspectors focused on that. It was a Galois theory problem on my own exam, which had been self-contradictory. I'm probably putting a false spin on it; last night it was upsetting me, or depressing me about having let everyone down. It reminded me of Holden Caufield's having, supposedly, left all the fencing equipment in the subway on the way to a match. I think that book was supposed to be about something meaningful.

I was reading about Monsanto, and debating about it with people, all the history about Saccharine, PCB's, agent Orange, Dioxin. Supposedly still now GMO's are the 'only way to feed the rapidly increasing population.' I wanted to explain in some way that the argument is upside-down. It is perfectly explained in my economics book, because all I did is quote things people said that actually make sense, and that show how people can actually understand sometimes..

I included the six BCC people, now since it is the last one, I'm including as BCC's maybe non-math friends, Bill, John K, Jacob, Callan, Sam, Felix, Jamie.

Just to give an example, not to explain it all, but to give an example, when I had a summer job, Bill took all the work out of my desk drawer, when I got back to University, and discarded it without telling me. Another summer job, he tried to get me to go on the Staten Island Ferry on my lunch hour, knowing if I went with him, I'd never get back to work in time.

Jacob had seminars about – really it must have been whatever we were reading, I think they were Saturday Morning even, or maybe Thursday at 10:00. I was reading a few pages of Corps Locaux. The thing is, none of the permanent staff ever knew Jacob did this. Equally important in my mind, more important, than any seminar that happened under the eyes of the establishment, powerful weekly seminars, were these.

I don't understand how I can call it non-mathematical friendship, when it is within Mathematics that this took place, in every case.

Anyway, the reason I decided to actually post a hard-copy .pdf as an email attachment is, I had decided *not* to.

And then I fell asleep tonight, and was dreaming.

I dreamed that we had gone to get the puppy, it was a little white puppy, and we took it with us to Stratford. As we did in real life.

And that suddenly I remembered in the past, when we were with it before, having seen the puppy with its mother, drinking the warm milk.

And it occurred to me, I have no way to feed it. I just hadn't thought about it.

I mentioned my worry to Dimitra, I was desperate about it, we have to go back! And she was her usual, it might be inconvenient 'absolutely not' attitude....

I wondered, after all this time, how can it be OK?

I used to have dreams that I was supposed to be teaching a class, back at Columbia, one of those precalculus classes maybe, and I'd forgotten to go *again* and it woud be about racing around, trying to find the list of times, weeks, trying to find the room. And some students would be waiting for me to explain meaningful things, and I'd give a lecture, but then later realize, it has been four more weeks, and I have not been there, and I wonder if they are *still* waiting.

But not any more, dreaming about abandoning students or anything.

The puppy looked content enough, but I noticed its tail was loose, it is a white puppy with a brownish tail, like Skiffles has.

And it just was somehow, maybe I was trying to pet it, or maybe to comfort it somehow, or to heal it, or see if it was OK, and it was on the couch. The tail had become disconnected. The puppy was ill, from having been taken away.

And it looked ill too, and it looked like other parts might fall off, and I was feeling sick with worry about it.

I got some water from the faucet onto my hand, and let it drip onto my knee, and the puppy started licking it. It stopped for a while, and I started to panic that it wasn't right, then it started again.

My only wish was to bring it back where it always belonged.

It's hard to explain how poignant it was, that it didn't seem to be worried, from what I could determine, but I was the one who was worried, and I held it for a little while, it was talking to me.