Easy things which number theorists know

With the push to find the forefront of research, it is sometimes nice to think about things that were done in the past, points of view which at the time seemed to work, and to solve every problem.

Two such notions are the notion of a ring of algebraic integers, and the notion of a rational point on a projective variety.

In the case of a ring of algebraic integers, what was noticed is that the sequence of numbers $n^2 + n + 41$ for $n = 1, 2, ...$ (and also $n = 0$, but that is not important) begins with a list of 30 or 40 prime numbers.

It surely also was noticed the reason, that

1. Proposition. The prime numbers which occur as divisors of any one of the n^2+n+41 when n is a *whole number* are no different than the ones that occur as the entire numerator of the same expression $n^2 + n + 41$ when n is a *rational number*.

The explanation for this is to allow n to be an actual *complex number*. There are as always two choices of n which give the only possible prime answer of zero.

Fix either one of these values of n. The ring it generates is known to have unique factorization, so any ordinary integer prime divisor of any $41 + m + m^2$, when m is any ordinary integer, factors $(q - rn)(q - r\overline{n}) = r^2(x^2 + x + 41)$ where x now means the rational number q/r.

Analogy with rational curves

A second thing that number theorists know well is the analogy between finding rational solutions to equations and finding sections of a rational function, viewed as a rational map to $\mathbb{P}^1$.

That is, let V be any complex projective variety, and let f be any rational function on V, that is, any element of the rational function field. We think of f as a rational map

$$V - \to \mathbb{P}^1$$

and if q, r are the numerator and denominator this is indeterminate where q and r are both zero.

Really the zero set of q and r are two elements of a pencil of hyperplanes, and the indeterminacy locus is the base locus of a one-dimensional linear system of hyperplanes. That is, the notion of numerator and denominator depends on a particular choice of a basis for the two dimensional vector space whose projectivication is $\mathbb{P}^1$, but the notion of a rational map $V - \to \mathbb{P}^1$ does not.

And there is a unique best way to resolve the indeterminacy if we wish to do this, as is well-known, obtaining then an actual map $V' \to \mathbb{P}^1$ where V' is the blowup of V along a sheaf of ideals.

Now, I forgot to start at the beginning here, which is that we are supposed to be searching in V for a smooth curve of genus 0, that is a curve abstractly isomorphic to $\mathbb{P}^1$.

And that we want not only to find the curve, but to parametrize it by a map $\mathbb{P}^1 \to V$.

So what we will do is to search for rational functions on V for which the lost rational curve is not totally contained in the indeterminacy locus. Then it lifts to a curve C in V'. And what we will do is to say that we'll look for f so that the composite $C \to V' \to V \to \mathbb{P}^1$ is an isomorphism. This is the same as saying that the fibers of $V' \to \mathbb{P}^1$ are transverse to C. The inverse isomorphism is the parametrization of C, and note that since $\mathbb{P}^1$ is already normal the copy of C in V' is isomorphic to the one in V.

Now, Grothendieck mainly noticed that the very same type of analysis works if we replace $\mathbb{P}^1$ with $\mathbb{Z}$. That is, starting with an irreducible projective variety over $\mathbb{Q}$, it is (I think always) the base extension of a reduced and irreducible scheme V of finite type proper over $\mathbb{Z}$, and an integer point of V is a map $Spec\ \mathbb{Z} \to V$. The fact that we needed to perform a blowup to get a morphism is not needed here, and the fact that the composite

$$Spec\ \mathbb{Z} \to V \to Spec\ \mathbb{Z}$$

is an isomorphism does not need to be checked, it is automatically true.

But, if we find first an unknown irreducible closed subspace $C \subset V$ it is still true that the condition for it to map isomorphically to $Spec\ \mathbb{Z}$ is that it meets every fiber transversely. That is, that the sheaf of Kahler differentials of C is identically zero, and C is not merely contained in one fiber. Thus,

2. Proposition An Zariski closed subset V of projective space over the integers has an integer point if and only if it contains an irreducible closed subspace which is not contained in any single fiber but has a trivial sheaf of Kahler differentials.

This is because $V \to Spec\ \mathbb{Z}$ is proper and that a minimum integer polynomial of degree larger than 1 can't have discriminant 1 or -1. Note that a rational point of the original variety is the same as a rational point of V which is the same as an integral point of V.

Logarithmic forms

Let $E \to Y$ be any finite type morphism of schemes with E reduced and irreducble. Let $\mathcal{F}$ be a coherent sheaf on E. The principal parts sheaf of $\mathcal{F}$ can be defined various ways. If $\mathcal{F}$ embeds in K the constant sheaf of rational functions on E we can let $\mathcal{P}_{E/Y}(\mathcal{F})$ to be the subsheaf of $K \oplus \Omega_{K/Y}$ generated by local sections $f \oplus df$.

The map of sheaves

$$\nabla : \mathcal{O}_E(D) \to \mathcal{P}_{E/Y}(\mathcal{F}),$$

given on local sections

$$f \mapsto f \oplus df.$$

satisfies, for f a local section of $\mathcal{O}_E$ and g a local section of $\mathcal{F}$ the rule of a connection

$$\nabla(fg) = fg \oplus d(fg) = f(g \oplus dg) + (0 \oplus gdf)$$

$$= f\nabla(g) + gdf.$$

In the general case, let V be the Fibré vectoriel of $\mathcal{F}$. Then $\mathcal{P}_{E/Y}(\mathcal{F})$ is the restriction (in the coherent sheaf sense) to the zero section E of the one-forms on V relative to Y which restrict to zero (in the differntial forms sense) as one-forms on E, and ∇ is the restriction of the deRham differential. Let $D \subset E$ now be a Cartier divisor and $\mathcal{F} = \mathcal{O}_E(D)$.

3. Lemma. Let $g_1, ..., g_c \in \Gamma(E, \mathcal{O}_E(D))$ be a regular sequence of global sections defining (by intersection with the zero section of the corresponding line bundle) a subscheme $C \subset E$. Then there is an exact sequence

$$0 \to \mathcal{O}_C\nabla(g_1) \oplus ... \oplus \mathcal{O}_C\nabla(g_c) \to j^*\mathcal{P}_{E/Y}(\mathcal{O}_E(D)) \to \mathcal{P}_{C/Y}(\mathcal{O}_C(D))) \to 0.$$

The lemma follows from

4. Lemma. Let $f : E \to Y$ be a morphism, let D be a Cartier divisor on E. Let $g_1, ..., g_c \in \Gamma(E, \mathcal{O}_E(D))$ be a regular sequence, defining a subscheme C. Let V be the line bundle on E with section[1] sheaf $\mathcal{O}_E(-D)$ and let V' be the restriction of it along $C \to E$. Let j be the inclusion $V' \to V$. Then the cotangent sheaf of V' relative to Y with logarithmic poles on C is presented by the short exact sequence

$$0 \to \mathcal{O}_{V'}(C)dg_1 \oplus ... \oplus \mathcal{O}_{V'}(C)dg_c \to j^*\Omega_{V/Y}(log\ E) \\ \to \Omega_{V'/Y}(log\ C) \to 0.$$

The restriction along the inclusion $i : E \to V$ of the Kahler differential d is the connection ∇.

Twisting by $-E$ and pulling back along $i : E \to V$ or equivalently pulling back along $i : E \to V$ and twisting by D gives the exact sequence claimed in Lemma 3 where now j refers to the inclusion $C \to E$.

[1] When E is not normal, D may have embedded components, then $\mathcal{O}(-D)$ should be taken to be the actual defining ideal sheaf

The case $c = 1$

Let's look carefully at the case of a sequence $g_1, ..., g_c$ consisting of just one term g_1.

When I speak of the sheaf $\mathcal{O}_E(D)$ I mean the sheaf of rational functions which are allowed poles matching at worst D. But z is a geometric section of a line bundle, and the intersection of the set of values of z with the zero section of that line bundle is the divisor D, with the multiplicities, necessarily positive, describing the actual order of tangency plus one of the intersection of two hypersurfaces (the zero section and the section z), with the convention that two hypersurfaces which do not meet at a point have order of tangency -1 at that point.

Intuitively, at each point of E the sheaf spanned by the fdz is spanned by one particular element fdz where the poles of the meromorphic function f exactly cancel the zeroes of dz. So at each point the inclusion of the span of the fdz in the span of the fdz and zdf should be complementary to the span of the zdf which is the whole of $\Omega_E(D)$.

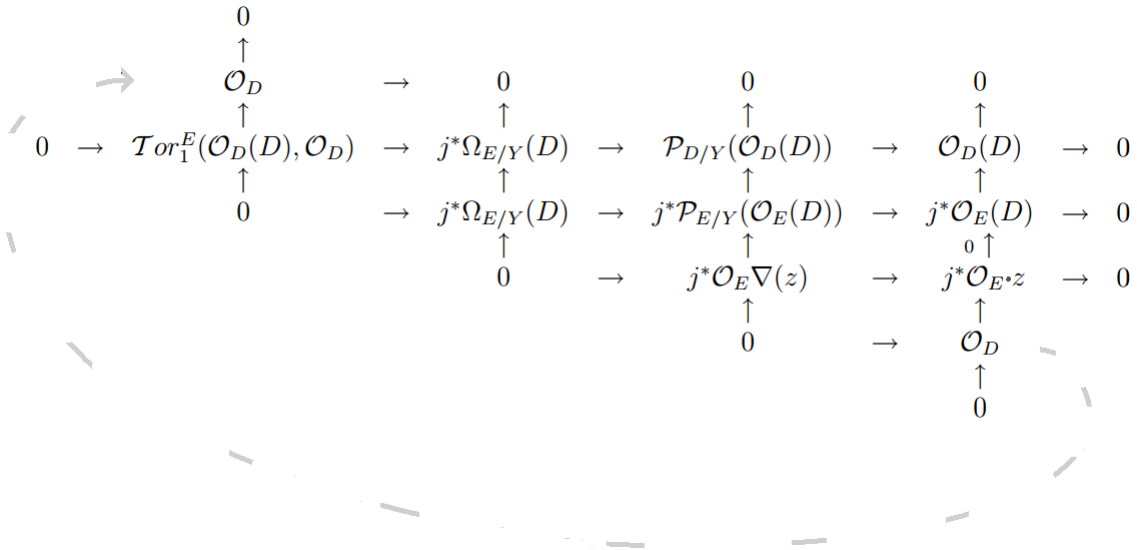
Let us look at the same thing homologically to make the argument rigorous. We have the diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \to \Omega_{E/Y}(D) & \to & \mathcal{P}_{E/Y}(\mathcal{O}_E(D)) & \to & \mathcal{O}_E(D) & \to & 0 \\ & & & \uparrow & & \uparrow & & \\ & & 0 \to & \mathcal{O}_E\nabla(z) & \to & \mathcal{O}_E z & \to & 0 \\ & & & \uparrow & & \uparrow & & \\ & & & 0 & & 0 & & \end{array}$$

The corollary 8 says that when we take the cokernel of this upward map of rows and pull back along $j : D \to E$ we obtain in the middle place $\mathcal{P}_{D/Y}\mathcal{O}_D(D)$. Homologically speaking, when we pull back the cokernel sequence we get a non exact sequence with kernel $\mathcal{T}or_1^{\mathcal{O}_E}(\mathcal{O}_D(D), \mathcal{O}_D)$. This is is the same as $\mathcal{T}or_1^{\mathcal{O}_E}(\mathcal{O}_D, \mathcal{O}_D)$ twisted by $\mathcal{O}_E(D)$, and so it is a copy of the trivial sheaf $\mathcal{O}_D$. Thus we obtain

$$0 \to \mathcal{O}_D \to j^*\Omega_{E/Y}(D) \to \mathcal{P}_{D/Y}(\mathcal{O}_D(D)) \to \mathcal{O}_D(D) \to 0.$$

And the exact diagram



The exact diagram implies a natural 'serpent lemma' or 'E_3 differential' which is an isomorphism from the copy of $\mathcal{O}_D$ on the lower right to the one in the upper left.

Before applying j^*, we had that $\mathcal{O}_E\nabla(z)$ embeded as a subsheaf of $\mathcal{O}_E(D)$, once we apply j^* the image of the copy of this sheaf in $j^*\mathcal{P}_{D/Y}(\mathcal{O}_D(D))$ is the same as the image $\mathcal{O}_D$ of the Tor term, which is the kernel of $j^*\Omega_{E/Y}(D) \to \mathcal{P}_{D/Y}(\mathcal{O}_D(D))$.

5. Corollary. For a map of schemes $E \to Y$ with E normal and a Cartier divisor D on E, when $g \in \Gamma(E, \mathcal{O}_E(D))$ and $D_g = (g) + D$, then for all i the i-forms on D_g relative to Y are the tensor product of coherent sheaves on E

$$\Lambda^i\Omega_{D_g/Y} \cong \mathcal{O}_{D_g}(-iD - D) \otimes \Lambda^{i+1}C_g.$$

where C_g is the cokernel of $\mathcal{O}_E \cdot \nabla(g) \to \mathcal{P}(\mathcal{O}_E(D))$.

Note that for each particular choice of g the sheaf $\Omega_{D_g/Y}$ is is the cokernel of

$$\mathcal{N}_g \subset j^*\Omega_{E/Y}$$

where $\mathcal{N}_g$ is the conormal sheaf of D_g in E relative to Y.

6. Corollary. Let E be a reduced, irreducible, locally factorial scheme proper flat and finite type of relative dimension one over $Spec\ \mathbb{Z}$. Let $D = e_1X_1 + ... + e_sX_s$ be an effective Cartier divisor on E with X_i distinct and irreducible. Suppose that

i) $e_1 = 1$,

ii) $\mathcal{O}_{X_1}(D - X_1)$ is basepoint free.

Then the ramification locus of $X_1 \to Spec\ Z$ is

$$\bigcap_{h \in \Gamma(E, \mathcal{O}_E(D - X_1))} X_1 \cap Support\ \Lambda^2\ \frac{\mathcal{P}(\mathcal{O}_E(D))}{\mathcal{O}_E \cdot \nabla\ h}$$

where ∇h is the principal part of the global section h of $\mathcal{O}_E(D - X_1)$ when viewed as a section of the larger sheaf $\mathcal{O}_E(D)$.

Proof. By Corollary 5 the support of the given sheaf is

$$Ram_{X_1/Spec\ Z} \bigcup \bigcap_h Supp((h) + e_2X_2 + ... + e_sX_s) \cap X_1.$$

The basepoint free condition ensures that the second term is empty.

7. Corollary. Let E be a projective scheme, normal and locally factorial, of finite type and flat of relative dimension one over $Spec\ \mathbb{Z}$. Each algebraic point corresponds to a divisor X_1. For any ample divisor H on E there is[2] a number m and an element $D \in |mH|$ satisfying i) and ii). For any such D the point corresponding to X_1 is rational if and only if the indicated intersection over elements h in the finitely-generated free abelian group $\Gamma(E, \mathcal{O}_E(D - X_1)) = \Gamma(E, \mathcal{O}_E(mH - X_1))$ is empty.

[2] see Serre's theorem, 5.17 in Hartshorne's book

Plane curves

Let $f \in \mathbb{Z}[x, y, z]$ be any irreducible polynomial. We do not need to assume that the the scheme E defined by $f = 0$ in the integer projective plane is normal or locally factorial. Let $h \in \mathbb{Z}[x, y, z]$ be any other homogeneous polynomial not a multiple of f.

The primary decomposition over the integers of the scheme defined by $f = h = 0$ includes associated associated primes of three types. First, there is one prime ideal sheaf corresponding to each algebraic conjugacy class of intersection points of the complex curves . Secondly, there are some associated primes which are individual fibers of the map to $Spec\ \mathbb{Z}$. These can occur even if the coefficients of h have no common divisor. Thirdly there are embedded components of the scheme $f = h = 0$.

Those of the first type define schemes which are the Zariski closure of (closed) points of rational projective space where $f = 0$ and $h = 0$. When the scheme defined by $f = 0$ is normal those of the third type do not occur.

If we don't assume that E is locally factorial, or even normal, and if we choose as D just a multiple of a hyperplane section, going from E to X_1 with two applications of Corollary 5 gives

8. Corollary. Let $f \in \mathbb{Z}[x_1, x_2, x_3]$ be irreducible homogeneous of degree at least one. Let $a_1, a_2, a_3 \in \mathbb{Z}$ with not all zero, and suppose $f(a_1, a_2, a_3) = 0$. Then for every homogeneous polynomial

$$h \in P = (a_i x_j - a_j x_i)$$

either

i) There is a number N such that $(x_1, x_2, x_3)^N h$ is contained in the unique primary ideal of $(f, (a_i x_j - a_j x_i)(a_k x_l - a_l x_k))$ which is associated to P, or

ii) Letting $P = P_1, P_2, ..., P_s$ be the associated primes of (f, h). There are is a number N such that

$$(P_2 P_3 ... P_s)^N \subset (a_i x_j - a_j x_i, \frac{\partial f}{\partial x_i}\frac{\partial h}{\partial x_j} - \frac{\partial f}{\partial x_j}\frac{\partial h}{\partial x_i}).$$

with the convention that if $s = 1$ the empty product signifies the inessential ideal (x_i).

Remarks. Part i) is equivalent to saying that $f = 0$ and $h = 0$ meet non-transversely at $[a_1 : a_2 : a_3]$ in the complex analytic sense. It is also equivalent to saying that h is contained in the second symbolic power of the height one prime ideal sheaf $P/(f)$, and it is equivalent to saying that the images of h and f are linearly dependent over k in $P/P^2 \otimes k$ for k the rational function field of the subscheme of the integer projective plane defined by P.

Part ii) is equivalent to saying that every associated prime of the ideal on the right (except the inessential ideal if $s = 1$) includes at least two associated primes of (f, h).

Normal plane curves

In the case when the scheme defined by $f = 0$ is normal, the intersection scheme defined by $f = h = 0$ is Cohen Macaulay (equivalently h is not identically zero on the unique component of $f = 0$) and no embedded components occur. The ideals in the graded polynomial ring which do not have the inessential ideal (x_1, x_2, x_3) as an associated prime correspond bijectively with all the ideal sheaves on the integer projective plane; so that $P_1, ..., P_s$ in statement ii) are all minimal over (f, h) except one of them might be the inessential ideal which can be ignored unless $s = 1$.

Geometric analogy

If we wished to prove that a real surface in three space contained no smooth curve (in some class of curves), the first thing we might try is to find a function constant on each relevant curve, whose gradient is parallel to the gradient defining the surface at one point of that curve.

This would not always work, for instance the coordinate function z in three space (x, y, z) is parallel to the gradient of $z - x^2 + y^2$ at the origin, and constant along the whole of the line $z = x - y = 0$. But that line has no singular point.

In the real case, in this example, it is caused by the fact that the index of the quadratic form $x^2 - y^2$ is $(1, 1)$ rather than $(2, 0)$ or $(0, 2)$. In the complex or arithmetic case we have not recourse to a notion of index, and so we merely revert to requiring that the point p where the gradient of the auxiliary function is parallel to the gradient of the equation of the surface must lie on only one of the components of the curve in the surface where the function takes the same value as it does at p.

10. Corollary. Let $f_1, ..., f_c \in \mathbb{Z}[x_0, ..., x_n]$ be homogeneous polynomials defining a reduced, irreducible, normal subscheme of $\mathbb{P}^n_{\mathbb{Z}}$ of codimension c. Let $a_0, ..., a_n$ be algebraic numbers, not all zero, such that $(a_0, ..., a_{n+1})$ is a common solution of the equations $f_i = 0$.

Let T be a set and let $h_{c+1}, ..., h_n$ be functions $T \to \mathbb{Z}[x_0, ..., x_n]$ so that the $h_i(t)$ are homogeneous for each $t \in T$ and the point $[a_0 : ... : a_n] \in \mathbb{P}^n_{\mathbb{C}}$ is a transverse intersection point of the n complex hypersurfaces defined by the equations $f_1 = 0,\ f_2 = 0,\ ...\ f_c = 0,\ h_{c+1}(t) = 0,\ ...\ h_n(t) = 0$.

Also for each $t \in T$ let $S(t)$ be the union of the subschemes of affine $n+1$ space over $\mathbb{Z}$ defined by the all the associated[3] prime ideals of the subscheme of affine $n+1$ space defined by the same n equations, with the exception of the prime ideal describing the generic point of the further intersection with the subscheme A determined by the ratio $[a_0 :, ..., : a_n]$ (note A contains the cone locus $Spec\ \mathbb{Z}$ and its normalization is an affine line over a ring of algebraic integers); and let $\omega(t)$ be the differential n form on affine $n+1$ space which is given by the equation

$$\omega(t) = df_1 \wedge ... \wedge df_c \wedge dh_{c+1}(t) \wedge ... \wedge dh_n(t).$$

Suppose that the intersection

$$\bigcap_{t \in T} S(t)$$

meets A nowhere but the cone locus $Spec\ \mathbb{Z}$. For each t let $V(t)$ be the (closed) subscheme of affine space where $\omega(t)$ is zero. Then the ratio $[a_0 : ... : a_n]$ is rational if and only if the subscheme

$$\bigcup_{t \in T} (\ V(t) \setminus S(t)\ )$$

is also disjoint from A away from the cone locus.

[3] they are all minimal; i.e. irreducible components

Two Comments

One comment is that it would be good to understand the role of the auxiliary equation in the Gauss, Hilbert, Artin, Brauer, Manin obstruction. It began with the equation $ax^2 + by^2 = cz^2$. I do not at all know whether this an example of the type of auxiliary polynomial h above.

A second comment is that whereas Corollary 6 gives an equivalent condition for an algebraic point to be rational, the more explicit Corollary 8 is not an equivalent condition for anything, it is a necessary condition only. It is the statement that if there is a rational point, there must be this and this and this baggage coming along with it.

The reason, is that Corollary 6 is an equivalence in an illusory way. If we do not care about non-rational points it does not matter whether the entity under consideration is a non-rational point, or nothing at all.

I have tried for a few days to understand things and I believe that the issue is that it doesn't make sense to 'given a solution q of an equation $f(q) = 0$, find the necessary and sufficient condition for q not to exist.'

I do not mean this in the sense of a word game, I mean that one is asking, what is the necessary and sufficient condition for the existence of q to lead to a contradiction, to be false. In Corollary 6 we can say, assume that q is an algebraic solution, what is the necessary and sufficient condition for it not to be a rational solution. But if we do not care about irrational solutions, why can we not deduce from Corollary 6 an explicit corollary?

We can restrict Corollary 6 to rational solutions. Then it says that if q is a rational solution a necessary and sufficient condition for a contradiction is the existence of a divisor D such that i) and ii) hold.

A necessary and sufficient condition for a contradiction is merely a false statement. Once Corollary 6 is restricted to rational points it says that a particular statement is not true.

It seems to me that the hope had been a statement necessary and sufficient for a general class of equations to have a solution. But this too is not possible. There cannot be any sensible plan to have a theorem saying, 'here is the necessary and sufficient condition for the solution of an equation to actually exist.'

Such a statement would explain causality; it can only have meaning with reference to a non-mathematical context. The Brauer-Manin obstruction may be different, as a Hasse principle does not actually get as far as answering the question of existence of rational solutions of equations. But at some point on the chain of using an auxiliary polynomial to detect non-existence of rational points there always has to be a broken link.

So that one can define 'class field theory' and say that it is worthy of study, and one can say that the forefront of research is there, and agree that progress defining the limits of class field theory is worthwhile. But if one hopes to extend those limits, and to extend the domain of truth of that theory, one has to understand that the actual limits, the actual boundary, is not a mathematical boundary.

Epilogue: The P=NP problem.

It asks, is there a natural number c and an algorithm A which can decide in $(n+m)^c$ steps whether any given statement of m words has a proof of n words. Here we refer to words in a fixed mathematical language.

If we ignore the number of words in the proof, there is no algorithm at all that can decide whether each statement has a proof, by a familiar diagonal argument. Therefore if we put the statments in alphabetical order, $s_1, s_2, ...$ then any algorithm A has a number $i(A)$ so that it cannot decide provability of $s_{i(A)}$. A human being may tweak the algorithm, replacing it by a new algorithm which can decide provabilty of that statement, and then the new algorithm will reach a new statement s_j which it cannot decide.

It is a different question whether the process of human beings tweaking (=replacing) the algorithm would reach a statement whose provabilty cannot be decided. Then there would be an algorithmic limit of the projection of human knowledge on that scale, depending on the ordering of the s_i.

We know that humans will be extinct; if we ignore that practical limitation, there is the limitation that the cognitive capacity of the human population may be limited. Yet even thought in small populations of people, or small seminars of study, propogating through generations, might undergo a very vast conceptual simplification, so that any particular even very long statement, billions of words in length in an original formulation, could if it were of importance to them be simplified and understood by people, and its provability decided by people. That question is whether there is any limit at all on the number of words.[4]

[4]Apart from knowing things, there is the question whether there is an analagous limit of human endeavour. Articles and textbooks do usually stress how it is extremely important to understand particular ideas or formulations. There is then an assumed concept that human endeavour causes things. The question, thinking about subsequent people who will in some sense inherit the work which we all all do now, is whether there are any things we care about that would take place, for example, in the last few generations before people become extinct. The separation between 'rational' and 'irrational' solutions or in the exponents 'positive' and 'negative' solutions, or after taking inverse images 'real' and 'imaginary,' etc., is that part of understanding abstraction is the difference between when it is there and when it is not there. It sometimes seems that mathematics succeeds in creating an ideal world, easily and instinctively; then the question is to understand what to tell people. If we see them as children, that is forgivable.

It is whether mathematical languages change over time with no significant change in the lengths of statements. Or with lengths of individual statements chang by a rapidly growing or rapidly decreasing function.

Now, however, the problem P=NP asks whether one particular algorithm, while we know that it cannot decide abstract provability, can, when it gets stuck, without any human intervention, at least rule out the existence of a proof of length n significantly more rapidly than considering all grammatically correct statements of length n. If the algorithm were replaced by a person it would need to have an intuition about relevance of statements, to reject classes of statements as being irrelevant not able to be proofs, on more accurate grounds than grammatical correctness, while not knowing whether a proof even exists. The person would have to be able to say, after receiving information about a possible proof, but not hearing the whole proof, 'I'm just not going to listen anymore.'

To a person, the reply would be, 'how can you know, on grounds other than grammar, that the things I am telling you won't amount to a proof of length n of the statement, when you admit that you do not know and cannot ever know without insight from me, whether there is a proof at all?'

The reason that people seem to believe without proof that $P \neq NP$ is that in such a situation, the problem would have required the algorithm to answer a question which a person can't answer.

Idea of a proof of $P \neq NP$

Here is an idea which might lead to a proof that $P \neq NP$.

What one wants to do is to trick the algorithm into wasting time. Thus, one might first formalize for each $i = 1, 2, 3, 4, ...$ the statement

$$P(i) = \text{“No algorithm can prove me in less than } i \text{ steps.”}$$

Next one should choose a number $d > 1$, and here it is likely that $d = 2$ is not significantly different than any other choice. Let W be the number of words in the language. Thirdly, one should construct a proof of $P(i)$ which has length $L(i)$ such that

$$W^{L(i)} < i^d.$$

Since $P(i)$ has a proof of length $L(i)$, an alphabetic search algorithm finds it in $W^{L(i)}$ steps, with each step finding and checking one statement; and the inequality guarantees that an algorithm can find a proof of $P(i)$ in i^d steps. Fourthly one should show that it would be absurd for an algorithm to find a proof in less than i steps; that it would actually lead to a grammatical mistake in the proof.

The $P = NP$ statement implies, I think, as I mentioned, that there is a number c and an algorithm A which can decide in $(n+length(P(i))^c$ steps whether $P(i)$ has a proof of length n. In fact we can also ask the algorithm to produce a proof if it says that one exists, it is still equivalent to P=NP.

Take $n = d \cdot log_W(i)$. Since this is larger than $L(i)$ there is a proof of shorter length than n. The algorithm then cannot prove that there is no proof of length n. In order to do what P=NP asks of the algorithm, it must find a proof of $P(i)$ of length n in fewer than $(n + length(P(i)))^c$ steps. Since it cannot find a proof in less than i steps

$$i \leq (n + length(P(i))^c = (d\ \log_W(i) + length(P(i)))^c.$$

The length of $P(i)$ is a constant e plus the length of an expression of the natural number i in the language, so $length(P(i)) = e + log_W(i)$. It would remain to show that for fixed $c, d, e, W \geq 1$ this fails for large i :

$$i \leq ((d + 1)log_W(i) + e)^c$$

It is easy to do all of this if we interpret 'algorithm' in a limited way, such as an alphabetic search. One would like to formulate things with a general enough definition of 'algorithm' that the non-existence of the algorithm about proofs for each c actually does imply the non-existence of a travelling salesman algorithm for each c.

The proof of $P(i)$ in the third step can't be just us saying in English, "If an algorithm proved $P(i)$ in less than i steps $P(i)$ would be false and therefore unprovable." It is required that an algorithm, in the sense that the word is used in the statement $P(i)$, can search through all the $W^{L(i)}$ statements of length $L(i)$ and find among those statements a proof of $P(i)$. Since the proof must use the words 'algorithm,' 'steps,' and 'prove,' the proof must refer to a definition of what an algorithm is within the formal language, and it must refer to a definition of what a step of an algorithm is within the formal language, and it must refer to a definition of what a proof is within the formal language.

For the fourth step, we have to prove that the proof of length $L(i)$ which we've mentioned in the third step has $i \leq W^{L(i)}$. An outline argument is that an algorithm going through the statements of length $L(i)$ would find the proof we've been trying to construct in step 3. We need to prove that having stepped through at most $W^{L(i)}$ steps in this situation, and it having found what we have called the formal language proof of $P(i)$, the algorithm would be able to look at its own actions, to see that the steps that it has taken are the steps of an algorithm, and that the contradiction which we as people see between the existence of that sequence of steps of length less than i proving $P(i)$ on the one hand, and the statement of $P(i)$ to the effect that there is no such sequence of steps leading to a proof of $P(i)$ on the other hand, actually imply that when the algorithm considers that particular statement, it actually does not decide according to the definition of prove which it is using, that the statement of length $L(i)$ which it has found could possibly be a proof of $P(i)$.

Also, the definition of algorithm which the proof uses cannot allow any cheating algorithm, devious enough to overlook a quick alphabetic search for a short proof. The algorithm needn't be able to prove that there is no short proof, but we need to know that it would have found a short proof in appropriate exponential time if one had existed.

One difficulty with the idea is that at one point of the argument we are in a situation of considering $P(i)$ which has a proof in a formal language, and which can be found by an algorithm but not any algorithm with less than i steps. A human being might run an alphabetic search to find the proof, discard that algorithm, and write a new algorithm which just has that proof stored in memory, produces it, an checks validity. This is not a difficulty if it only affects a finite number of values of i. Once the $P(i)$ are all formalized, however, it cannot be possible for a human being to write an algorithm which will in this way prove all $P(i)$ in fewer than i steps. For, the formal proof that there is no such algorithm would be valid. The issue is that while we believe that the relevant diagonal argument can't be conquered by an algorithm, algorithmic formulations of the $P(i)$ which lead to a diagonal argument that can would not lead to a proof that $P \neq NP$.

11. Example. This example is calculated with the help of the Singular computer project at Technische Universitat Kaiserslautern, using the library primdecint.lib which is able to perform primary decomposition of rings over the integers. I wish to thank Yue Ren, professors Pfister and Schoenemann, and Andy Macheta in Warwick IT services all for working personally to make such a wonderful work available to me.

The example uses Corollary 8 to show that a particular algebraic point is not rational. Take $f = x^3 + y^3 - z^3$, and let's take the auxiliary polynomial $h = x+y+z$. The associated primes of (f, h) in the graded ring are the homogeneous ideals $(z, x+y)$ and $(h, 3y^2+3yz+3z^2)$, both minimal primes over (f, h). Both primary components of (h, f) happen to be prime and so i) of Corollary 8 cannot hold. The vanishing locus of $df \wedge dh$ on the corresponding union of two subschemes is described by two maximal ideal sheaves $(3, z, x + y)$ and $(5, y - 2z, x - 2z)$. (A third primary component in the graded ring is a copy of the inessential ideal which we ignore). These correspond to $[1 : -1 : 0]$ in the projective plane over $\mathbb{F}_3$ and $[2 : 2 : 1]$ in the projective plane over $\mathbb{F}_5$. The second of these is on only one of the components, so condition ii) of Corollary 8 does not hold; this proves that the point $[2 : 2 : 1]$ with values in the prime field of characteristic five, must be the reduction modulo a ramified prime of a non-rational point, and that while $[1 : -1 : 0]$ is a rational solution, the fact that this does not reduce modulo 5 to $[2 : 2 : 1]$ implies that there can be no rational solution whatsoever lifting $[2 : 2 : 1]$ *mod* 5.

In this case there is an easier way of showing that there is no rational solution of $f = h = 0$ when z is nonzero, as the real curves clearly do not intersect unless $z = 0$. It is interesting that there is also now the argument which only involves comparing two of the 31 $\mathbb{F}_5$ rational points in the integer projective plane.

I do not know how one might understand the relevance of the prime 5 without already knowing which integer polynomials are irreducible; Corollary 10 is an attempt to separate the questions, first seeing whether there are enough points like $[2:2:1]$ $mod\ 5$ lying on a single component and then considering the $df \wedge dh$ for the corresponding h afterwards.

You can enter h and n into a website which will call primdecZ for you in the appropriate way, by clicking this link:

`http://www.warwick.ac.uk/~masbf/php3/test.html`

Lines through a rational point of a Fermat curve

The specialization of Corollary 8 to the case of rational lines through a Fermat curve $x^p + y^p = z^p$ for p prime is the following argument:

Suppose I choose a rational point of a Fermat curve, and then a rational line through that point. You choose a prime number q, but you incorrectly think that q is zero. If you can deduce (in usual ways) that the rational line is nothing but a tangent line, you can argue that unless the Fermat curve is equal to its own tangent line, the intersection point occurs with multiplicity at least two.

This actually means that one of the prime ideals lying over q in the ring of algebraic integers corresponding to a second one of the algebraic intersection points of the line with the Fermat curve actualy has residue degree one. And that is what Corollary 8 is saying for line sections of Fermat curves:

12. Corollary. Let p be a prime number and $x_0, y_0, z_0 \in \mathbb{Z}$ not all zero such that $x_0^p + y_0^p = z_0^p$. Then for any rational line $ax + by = cz$ in the projective plane which passes through the point $[x_0 : y_0 : z_0]$ such that $[a : b : c] \neq [x_0^{p-1} : y_0^{p-1} : z_0^{p-1}]$

a) If $[a : b : c] \not\equiv [1 : 1 : 1]$ *mod* p then the number field associated to each conjugacy type of intersection point of the line with the curve $x^p + y^p = z^p$ is totally ramified at p.

b) For any prime $q \neq p$ such that $[a : b : c] \equiv [x_0^{p-1} : y_0^{p-1} : z_0^{p-1}]$ *mod* q, the line $ax + yb - zc = 0$ meets at least one other conjugacy type of point of the curve $x^p + y^p - z^p = 0$ whose corresponding number field has a prime of residue degree 1 lying over q.

Both statements have an elementary direct proof using projection from a point; in fact a) has an even easier proof. However we will deduce both parts from Corollary 8.

First note that since the Fermat curves are normal there are no embedded components. The condition that $[a : b : c] \neq [x_0^{p-1} : y_0^{p-1} : z_0^{p-1}]$ ensures that the line where $h = ax + by - cz$ satisfies $h = 0$ is not a tangent line complex analytically, and this ensures that condition i) of Corollary 8 does not hold. Since $[x_0 : y_0 : z_0]$ is rational then ii) of Corollary 8 must hold. The closed points of the scheme corresponding to $[x_0 : y_0 : z_0]$ are bijective with the prime numbers in $\mathbb{Z}$. The closed points of the subscheme corresponding to $[x_0 : y_0 : z_0]$ where $\nabla f \wedge \nabla g = 0$ correspond to the prime p together with all the prime numbers q such that the congruence of ratios holds $[a : b : c] \equiv [x_0^{p-1} : y_0^{p-1} : z_0^{p-1}]$ *mod* q. Each of these closed points must lie on a second associated component of the scheme defined by $f = h = 0$ besides the component corresponding to $[x_0 : y_0 : z_0]$. Since the subscheme of the integer projective plane defined by $f = 0$ is normal there are no embedded components so each such closed point lies on two irreducible components.

If $[a : b : c] \equiv [1 : 1 : 1]$ *mod* p then h is zero on the whole fiber defined by the equation $p = 0$ and this itself is a component of $f = h = 0$ meeting the scheme $[x_0 : y_0 : z_0]$ at the closed point corresponding to the prime p. If $[a : b : c] \not\equiv [1 : 1 : 1]$ then h is not zero on the whole fiber and there must exist a non-fiber component of the scheme defined by $h = f = 0$ which meets the scheme corresponding to $[x_0 : y_0 : z_0]$ at the closed point corresponding to p. Since f is a p'th power modulo p the intersection multiplicities must sum to $p-1$ and it follows that the ramification indices of the closed points in the rings of algebraic integers corresponding to the algebraic points (=conjugacy types of complex points) must add to $p - 1$. Since the degrees over $\mathbb{Q}$ add to $p - 1$ it follows that all the components meeting the scheme corresponding to $[x_0 : y_0 : z_0]$ are totally ramified at the point corresponding to p.

As for primes q besides p, the argument is analagous but the conclusion is simpler. For each $[a : b : c]$ – still assuming it is not actually equal to $[x_0^{p-1} : y_0^{p-1} : z_0^{p-1}]$ – and for each prime number $q \neq p$ such that $[a : b : c] \equiv [x_0^{p-1} : y_0^{p-1} : z_0^{p-1}]$ *mod* q there must be an algebraic point on the intersection of the line $h = 0$ with the scheme $f = 0$ not equal to $[x_0 : y_0 : z_0]$ and which has residue degree one at some prime in the corresponding ring of algebraic integers lying over q.

In other words, in this case the two components intersecting at a closed point where $\nabla f \wedge \nabla g = 0$ give to two rings of algebraic integers, one of them corresponding to $[x_0 : y_0 : z_0]$ and the second corresponding to a possibly non-rational point $[x_1 : y_1 : z_1]$ and the intersection point describes a prime of residue degree one lying over q in both rings of algebraic integers.

Remark.[5] The two parts a) and b) of the corollary can be combined if one thinks of it like this: choose a rational line through a rational point $[x_0 : x_1 : x_2]$ of a normal irreducible plane curve which meets the curve complex analytically transversely at that point, and choose and any prime q for which the reduction modulo q of the line is tangent to the curve and contains at least one point not on the curve. Then the line section divisor on the two dimensional scheme which is the curve over $\mathbb{Z}$ contains at least two components which meet at the closed point $[x_0 : x_1 : x_2]$ *mod* q.

[5] In *The meaning of positive and negative* this notion will be refined to give an elementary proof of the Fermat theorem except in a special case when x, y, z are each a power of $2, 3, p$.

Let's leave the special case of the Fermat question aside promising to look at it later, and look back at Lemma 3. Let us take for D a complete curve in the projective plane E, and for C the scheme defined by a complete intersection $f = h = 0$ as we have been considering, but now taking f and h to have the same degree. The divisor D_h will be the divisor $D + (h/f)$.

For C the intersection scheme of D and D_h let's first just coarsely calculate $ch(\Omega_C)$ as an algebraic cycle using Lemma 3. The exact sequence of the lemma maps onto an exact sequence where the kernel is replaced by its saturation and the cokernel is just $\mathcal{O}_C(D)$. Therefore the Chern character of the saturation of $\mathcal{O}_C\nabla\ f \oplus \mathcal{O}_C\nabla\ h$ is

$$ch\ \mathcal{O}_C \cdot ch\ (\mathcal{P}\mathcal{O}_E(D) - ch\ \mathcal{O}_E(D)).$$

Subtracting 2 $ch\ \mathcal{O}_C$ for the Chern character of the trivial sheaf of rank two gives

$$ch\ \Omega_C(D) = ch\ \mathcal{O}_C \cdot (ch\ \mathcal{P}\mathcal{O}_E(D) - ch\ \mathcal{O}_E(D)) - 2\ ch\ \mathcal{O}_C$$

$$= (1 - e^{-D})^2 \cdot (ch\ \Omega_E(D) - 2)$$

Using $ch\ \Omega_E = 3e^{-H} - 1$ for H a hyperplane we get

$$ch\ \Omega_C = (1 - e^{-D})^2(3e^{-H} - 1 - 2e^{-D})$$

$$= 2D^3 - 3D^2H.$$

Now if we are working in the Chow ring, the next step would be to observe that D^3 and D^2H are integer multiples of H^3, and if we interpret H^3 as the intersection of three projective lines, there are no triple points of the intersection even in the projective plane over the integers. The expression above represents zero in the Chow ring. The geometric phonemenon of two irreducible components of the scheme $f = h = 0$ intersecting in an essential way is lost during the calculation if we allow the full relations in the Chow ring of the integer projective plane.

Partial explanation of class field theory

If $\mathcal{O}$ is a normal cyclic cover of $\mathbb{Z}$ of order n, an observation in number theory is that for a suitably large integer c the primes which split completely are those which belong to a subgroup H of $\mathbb{Z}/c\mathbb{Z}^\times$ of index n. And that the primes are equidistributed in terms of Dirichlet density among the cosets of H.

The first assertion is from Kroneker's theorem that $\mathcal{O}$ is a subring of of the cyclotomic ring generated by the primitive c'th roots of unity for some c so that the Galois group of $\mathcal{O}$ is $(\mathbb{Z}/c\mathbb{Z}^\times)/H$ for a subgroup H of index n, and each irreducible component of fiber of $Spec\ \mathcal{O}$ over an unramified prime p has cyclic stabilizer with a distinguished generator which is the Frobenius element. So that the primes which split completely are those whose Frobenius element belongs to H. The second is from Dirichlet's theorem, which states that primes in $\mathbb{Z}$ reducing modulo c to elements of element of $\mathbb{Z}/c\mathbb{Z}^\times$ are equidistributed,

The approach of number theory is to to work 'intrinsically' without reference to a particular cyclotomic field. Just as $Spec\ \mathcal{O}$ is a disjoint union of $Spec\ \mathcal{O}_c$ and $Spec\mathcal{O}[1/c]$ where $\mathcal{O}_c$ is the semilocal ring, and c is let us say a power of the discriminant of $\mathcal{O}$, then given $\lambda \in \mathbb{Z}_c^\times$, there are two ways we could check whether its image is trivial in the cyclic group $C = (\mathbb{Z}/c\mathbb{Z}^\times)/H$ (equivalent to the condition that λ splits completely if it happens to be a prime of $\mathbb{Z}$ unramified in $\mathcal{O}$).

Concerning the ramified part, one could check whether if λ is a norm from the completion $\widehat{\mathcal{O}}_c \times (\mathcal{O} \otimes \mathbb{R})$ (including both non-archimedian and archimedian).

Concerning the unramified part, one could work only on the level of divisors and see whether the divisor (λ) is a norm of a divisor in the (infinitely generated) divisor group of $\mathcal{O}[1/c]$.

While neither check alone is sufficient to characterise H, both together are. That is, since $0 = H^1(K^\times) = H^1(I_{\mathcal{O}})$ where $K = frac\ \mathcal{O}$ the cyclic group C is the pushout of the diagram of surjections [6]

$$\begin{array}{ccc} Br\ \mathcal{O}_c/\mathbb{Z}_c & \to & H^2\ I(\mathcal{O}[1/c]) \\ \downarrow & & \\ Br(\widehat{\mathcal{O}}_c/\widehat{\mathbb{Z}_c}) \oplus Br((\mathcal{O}\otimes\mathbb{R})/\mathbb{R}) & & \end{array} .$$

It follows from work of Artin that the cyclic group C never was anything besides the Galois group.

The analysis of cyclic covers generalizes in two different directions for noncyclic groups.

Firstly, Lang's book recounts a proof of Tebotarev density by Deuring, the totally split primes have density $1/n$ in any degree n extension of number fields, this is proved by reducing to the case here, using the fact that primes of the smaller ring of integers which are totally split over $\mathbb{Z}$ are themselves dense.

And secondly, any central simple algebra over $\mathbb{Q}$, even if not initially defined using a cyclic field, arises from a class in $Br\ K/\mathbb{Q}$ for K cyclic as it is here.

[6] In a bit more detail, from $0 = H^1(K^\times) = H^1(I_{\mathcal{O}})$ and the definitions, $0 \to H^1(\mathcal{O}^\times) \to I_{\mathcal{O}}^{\sigma}/I_{\mathbb{Z}} \to Cl(\mathcal{O})^\sigma \to Br(\mathcal{O}/\mathbb{Z}) \to \kappa \to Cl(\mathcal{O})_\sigma \to 0$ is exact where ${I_{\mathcal{O}}}^\sigma, Cl(\mathcal{O})^\sigma$, and $Cl(\mathcal{O})_\sigma$ are the invariant ideals and ideal classes and the coinvariant ideal classes, and κ is the kernel of $Br(K/\mathbb{Q}) \to H^2(I_{\mathcal{O}})$. Since ${I_{\mathcal{O}}}^\sigma/I_{\mathbb{Z}} \cong \prod_{p|c} \mathbb{Z}/e_p\mathbb{Z}$ the order of κ is the order of this group times the Herbrand quotient of $\mathcal{O}^\times$, the latter being e_∞/n with e_∞ the ramification at the infinite place (times the Herbrand quotient of $Cl(\mathcal{O})$ which equals 1). The product of Brauer groups of the complete local rings has order $e_\infty \prod_{p|c} e_p$. With horizontal kernel a subquotient of κ, the pushout has has order at least n. The image of $\mathbb{Z}_c^\times$ in the pushout is a finite abelian group under multiplication which corresponds to a partition of the prime divisors in $I(\mathbb{Z}[1/c])$ into at least n parts of equal density, with one part having density $1/n$. Thus the pushout has order n exactly; and the map to C is an isomorphism. Note that when -1 is a norm from $\mathcal{O}$ so that $0 = Br(\mathcal{O}/\mathbb{Z})$ then κ is merely the coinvariant ideal classes.

By our conventions, $Br\widehat{\mathcal{O}}_c$ refers to the second Galois cohomology of $\widehat{\mathcal{O}}_c^\times$. For c prime this has order equal to the ramification degree.

Here the Azumaya algebras are over copies of the p-adic integers for primes p such that the map to $Spec\ \mathbb{Z}$ has some ramification ov er p. Once tensored with $\mathbb{Q}_p$ they also admit a maximal commutative su bfield which is unramified and correspond to a power of p, rather than a p-adic unit, and modulo norms from a different unramified field extension. Performing the composite with the unramified extension is a process of adjoining roots of unity prime to p to the p-adic field. This explains the Hilbert product formula:

In the construction of the cyclic group C as a pushout, the elements of $\mathbb{Z}_c^\times$ map to the subgroup of order e of the Brauer group of each completion of ramification index e, although there was no requirement that the non-archimedian completions should be totally ramified, and the Brauer group of the complete local ring is the subgroup whose index is the 'local residue degree' in the cyclic Brauer group of the completed field.

Let us for simplicity ignore the unramified part when there is mixed ramification, and consider when $\mathcal{O}$ is totally ramified at a prime $p|c$, and we choose a prime q which is relatively prime to c and residue degree n. We write $\mathcal{O}_P = \mathbb{Z}_p[T]/P(T)$ with $P(T)$ an Eisenstein polynomial, and let t be the image of T. The image of q in $Br(\mathcal{O}_p[q^{1/n}]/\mathbb{Z}_p)$ is the central simple algebra

$$\mathbb{Z}_p[t, q^{1/n}]$$

in which $tq^{1/n} \equiv \omega q^{1/n} t\ mod p$.

Here $\omega = -1$, though in more general cases, when we are working over the integers of a number field in place of $\mathbb{Z}$, interchanging the role of p and t replaces ω by its inverse or complex conjugate.

This shows that if we choose to identify C with the Galois group in such a way that the Frobenius automorphism at q maps to the generator under $Br(\mathcal{O}_q/\mathbb{Z}_q) \to C$ then the class of q in $Br(\mathcal{O}_p/\mathbb{Z}_p)$ corresonds to the inverse of the Frobenius of q, and when we take the product in C the result is equal to one.

It seems that if we wished to understand the product formula geometrically, it should concern a pencil of Severi-Brauer varieties through the spectrum of a common maximal commutative subring of an Azumaya algebra, in some way analagous to the way we considered the pencil of rational lines through a rational point of a Fermat curve.

The Archimedian valuation

The relation between primary decomposition and the Archimedian and non-Archimedian valuations is that Lasker's primary decomposition theorem can be interpreted as saying that for a finitely-generated module over a commutative Noetherian ring R there are finitely many prime ideals so that the module embeds in a cartesian product of Artinian modules over the completions at the primes. In other words that the topology induced by the powers of the prime ideals in the completed module is the discrete topology.

Conjecture. The same statement holds for non-commutative Noetherian rings.

This interpretation however does not explain the Archimedian ramification, and an example of the issue is the explanation for why the group of units of $\mathbb{Z}\sqrt{2}$ is infinite while that of $\mathbb{Z}\sqrt{-2}$ is finite. In an earlier section called 'geometric analogy' I mentioned that the index of the quadratic form $x^2 - y^2$ explains why the differential of the form is zero at the origin while the irreducible components of the curve $x^2 - y^2 = 0$ are smooth. Here we have the expression for the norm of an element of $m + n\sqrt{2} \in \mathbb{Z}\sqrt{2}$ for $m, n \in \mathbb{Z}$ and it is

$$m^2 - 2n^2,$$

it is exactly again here the issue that the Archimedian valuation is aware of the index of the norm form.

In both cases the single prime ideal 0 suffices to induce the discrete topology in the completion, completing at 0 has no effect. However the statement that the induced topology is discrete does not tell us about the index of the norm form.

This does seem to be at least partly captured in the Brauer groups. The nontrivial class in $H^2(\mathbb{Z}\sqrt{-2}^{\times})$ is represented by an Azumaya algebra which is the cross-product algebra which we would make by a tensor product of $\mathbb{Z}\sqrt{-2}$ with the Gaussian integers $\mathbb{Z}[i]$ according to the rule

$$i\sqrt{-2} = -\sqrt{-2}i.$$

The analagous construction for $\mathbb{Z}[\sqrt{2}]$ gives a matrix algebra, the endomorphism ring of $\mathbb{Z}[\sqrt{2}]$ over $\mathbb{Z}$. We represent i as the endomorphism ϕ sending 1 to $1+\sqrt{2}$ and $\sqrt{2}$ to $-2-\sqrt{2}$, so that

$$\phi \circ \phi = -1, \quad \phi\sqrt{2} = -\sqrt{2}\phi.$$

It is a question whether the Archimedian valuation has ever been a necessary part of number theory, or whether it was never more than an artefact of the prejudice for Euclidean norms; whether some mysterious relations among whole numbers can never be understood, or proven, without imposing a total order by a real absolute value.

When non-mathematicians describe their hopes for 'nonlinear' mathematics, they seem not to really understand what we mean when we speak of the difference between something linear and something non-linear. But what the layman means may be more admirable. The introduction of Weil's 'Basic Number Theory' speaks of bringing Archimedian and non-Archimedian valuations 'under one roof' and 'making them cooperate for a common purpose,' and admits that Riemann-Roch may be independent of Archimedian valuations – perhaps just as Hirzebruch and Grothendieck proved later. Long ago Physics dispensed with any notion that space is explained by coordinates in a totally ordered real line. But we do not have explanations for all phenomena that have arisen historically in number theory besides interpreting whole numbers as increments of exactly such an uncountable continuous line. It would be an interesting experiment to complete an ideal of Hirzebruch and Grothendieck, to find a non vacuous interpretation of Hilbert's product formula which does not refer to an Archimedian valuation. Economists interpret real values as though they are intrinsic to thought, perhaps trusting mathematicians who tell them that as far as we know they may really be intrinsic to any human-scale understanding of historical problems about numbers.

John Atwell Moody
4 March 2013
Warwick Mathematics Institute