Stockholms Matematiska Kollokvium
tisdag, 5 oktober 2004
Matematiska Inst, Stockholms Universitet,
Kräftriket, hus 5, sal 14, kl 17.00 - 18.00

Prof. A. Stolin (Chalmers/GU)

Fermat's Last Theorem and the Kervaire-Murthy conjectures

Abstract: In my talk I will explain that one and the same method of algebraic number theory can be used in the proofs both of some cases of Fermat's Last Theorem and of the Kervaire–Murthy conjecture in algebraic K-theory.

The aim of my talk is to explain some connections between Fermat's Last Theorem and one of the conjectures in algebraic K-theory.

The main objects of my talk will be the equation $x^n + y^n = z^n$, class groups and Picard groups of certain rings.

We begin with some simple observations about the equation: a) in order to prove that the equation has no integer solutions it is enough to consider cases $n = 4$ and when is n an odd prime number. Further, since the cases $n = 3, 4$ were considered a long time ago (Fermat, Euler), we can assume that n is a prime number p greater than 3. b) We consider two different cases: the first case $\gcd(xyz, p) = 1$ and the second case $\gcd(xyz, p) = p$. Moreover in the second case we can assume that p divides z while $\gcd(xy, p) = 1$.

Now let ζ be a primitive p-root of unity. We can rewrite the equation as

$$\Pi_k(x + y\zeta^k) = z^p \tag{1}$$

Let us consider the following ring of algebraic integers:

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + ...a_n\zeta^n | \; a_i \; are \; integer \; numbers\}.$$

This ring has no zero divisers. Suppose $\mathbb{Z}[\zeta]$ is a unique factorization domain (for this we need to define prime numbers and we say that $a \in \mathbb{Z}[\zeta]$ is prime if any presentation $a = bc$ implies that either b or c is an invertible element in $\mathbb{Z}[\zeta]$. If any element can be uniquely presented (up to multiplication by units) as a product of primes then our ring is a unique factorization domain). Then if $\gcd(xyz, p) = 1$ one can easily show that

$$x + y\zeta = \epsilon r^p, \tag{2}$$

for some $\epsilon, r \in \mathbb{Z}[\zeta]$, where ϵ is invertible in $\mathbb{Z}[\zeta]$.

After some manipulations one can prove that the latter equality is impossible and therefore the first case of Fermat's Last Theorem is proved.

However for $p > 19$, $\mathbb{Z}[\zeta]$ is not a unique factorization domain!

Fortunately there is a way out of this situation and for this we need class groups invented by Gauss and Kummer. Let I_1, I_2 be two ideals in $\mathbb{Z}[\zeta]$. Define their product $I_1 I_2$ as the ideal generated by all products $i_1 i_2$ with $i_1 \in I_1$ and $i_2 \in I_2$. Of course the whole ring $\mathbb{Z}[\zeta]$ is an identity for this multiplication. Moreover, it is possible to prove that our multiplication of ideals satisfies the cancellation law and therefore can be used to create a group, which we denote by $I(p)$. One can prove that $I(p)$ is a free abelian group generated by the maximal ideals of $Z[\zeta]$ (*)

It contains a natural subgroup P generated by the principal ideals and it is possible to prove that the group $I(p)/P$ is finite (Minkowski). The group $I(p)/P$ is called the class group of $\mathbb{Z}[\zeta]$. In the sequel we will be interested in its p-Sylow subgroup, which we denote by Cl_0.

Kummer suggested the following way to prove the first case of Fermat's Last Theorem. Assume that for some p the group Cl_0 is trivial. Such primes are called regular and the rest are called irregular.

Let p be regular. Then it follows from (1) and (*) that the ideal generated by $(x + y\zeta)$ is the p-th power of some ideal. Since Cl_0 is trivial one can deduce that (2) holds in this case. It proves the first case because the fact that (2) leads to a contradiction does not require regularity of p. The second case also was proved for regular p by Kummer.

Tables and probabilistic arguments suggest that around $2/3$ of all primes are regular. For instance there are only 3 irregular primes less than 100: $37, 59, 61$. However is has not been proved yet that the number of regular primes is infinite while the number of irregular primes is known to be infinite.

Regularity of prime numbers can be expressed in terms of Bernoulli numbers. For a given p consider the even Bernoulli numbers $B_2, B_4 ..., B_{p-3}$. It turns out that p is regular if and only if none of the numerators of the B_{2i} above are divisible by p.

To proceed I would like to describe a phenomenon, which I informally call "the phenomenon of gaps". Let a be an integer such that $a^p \equiv 1 \mod (p)$. Then Fermat's Little Theorem says that $a \equiv 1 \mod (p)$ and it follows that $a^p \equiv 1 \mod (p^2)$. In other words if we look at p-th powers in the arithmetic progression $1 + pt$, we will see some gaps because $a^p = 1 + p^2 t$. Even this simple observation enables one (of course after some additional considerations!) to prove that the equation $x^p + y^p = (pz)^p$ has no solutions in integers x, y, z such that $\gcd(xyz, p) = 1$.

It turns out that a similar gap phenomenon takes place in $\mathbb{Z}[\zeta]$. It is known that p is not a prime in $\mathbb{Z}[\zeta]$ and more exactly that $p = \epsilon(1-\zeta)^{p-1}$ for some unit ϵ.

Theorem 1. *Let $q \in Z[\zeta]$ satisfy $q \equiv 1 \mod (1-\zeta)^{p-1}$ and suppose the ideal generated by q is the p-th power of some ideal. Then, $q \equiv 1 \mod (1-\zeta)^p$.*

To make further steps we have to introduce the so-called semi-regular primes.

The group of order 2, $< 1, s >$, acts on $\mathbb{Z}[\zeta]$ where s acts as complex conjugation. This action induces an action of $< 1, s >$ on the Sylow p-subgroup of the class group, Cl_0.

Since Cl_0 is a p-group, it splits into 2 summands, $\mathrm{Cl}_0 = (\mathrm{Cl}_0)^+ \oplus (\mathrm{Cl}_0)^-$, where $(\mathrm{Cl}_0)^+ := \{a \in \mathrm{Cl}_0 \mid s(a) = a\}$ and $(\mathrm{Cl}_0)^- := \{a \in \mathrm{Cl}_0 \mid s(a) = -a\}$.

A prime number p is called semi-regular if $(\mathrm{Cl}_0)^+ = 0$.

Vandiver's conjecture says that all primes are semi-regular and it has been numerically verified for all primes up to around 10 000 000.

Clearly regular primes are semi-regular.

Our "gap" theorem above implies the following

Theorem 2. *Let p be semi-regular and let $q \in Z[\zeta]$ satisfy the conditions of the "gap" theorem. Then $q = \epsilon r^p$ for some invertible ϵ.*

This theorem enables us to make some further advances in Euler-Kummer's way of proving Fermat's Last Theorem.

Theorem 3. *Let p be semi-regular. Then the equation $x^p + y^p = (p^2 z)^p$ has no solutions in integers x, y, z such that $gcd(xyz, p) = 1$.*

Outline of the proof. We use an idea from the following well-known telegram: "I managed to prove Fermat's Last Theorem. The main idea is to put the term x^p on the right hand side. Details will be sent with a letter!"

So we rewrite the equation as $x^p - (p^2 z)^p = (-y)^p$ or $\Pi_k(x - \zeta^k p^2 z) = (-y)^p$.

The "gap" theorem implies that $x - \zeta(p^2 z) = \epsilon r^p$.

If in the last equality ζ had an integer coefficient co-prime to p, then this would mean the end of the proof. In our case some work with the equality leads to that of p divides z. Therefore the equation $x^p + y^p = (p^2 z)^p$ has no solutions if $gcd(xyz, p) = 1$.

Now I would like to discuss another problem, where the "gap" theorem is applicable.

As I mentioned before, class groups appeared in Kummer's work as a tool to prove Fermat's Last Theorem. Later it turned out that the class group of an algebraic number field is one of the most important notions in algebraic number theory. In particular the class group is isomorphic to the Galois group of the maximal abelian unramified extension of its field and hence is very important in so-called Class Field Theory, one of the highlights of mathematics in the first half of the twentieth century.

In the sequel I will need not only the ring $\mathbb{Z}[\zeta]$ but also $\mathbb{Z}[\zeta_n]$, where ζ_n is a primitive p^{n+1}-root of unity.

Similarly we introduce Cl_n, the Sylow p-component of the class group of $\mathbb{Z}[\zeta_n]$.

The norm map $N : Z[\zeta_n] \to Z[\zeta_{n-1}]$ induces an epimorphism (also denoted by N) $N : \mathrm{Cl}_n \to \mathrm{Cl}_{n-1}$.

The corresponding projective limit $\ldots \to \mathrm{Cl}_n \to \mathrm{Cl}_{n-1} \to \ldots \mathrm{Cl}_0$ is called the Tate module of rational numbers and is denoted by $T_p(Q)$.

Let us consider the Galois group $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta))$. It is easy to show that it is isomorphic to the cyclic group of order p^n denoted by C_n. It obviously acts on Cl_n and this action enables one to define an action of the projective limit of groups $\Gamma := \ldots \to C_n \to C_{n-1} \to \ldots \to C_1$ on $T_p(Q)$.

Therefore, $T_p(Q)$ becomes a $\mathbb{Z}_p[\Gamma]$-module. Here $\mathbb{Z}_p$ is the ring of p-adic integers.

Iwasawa proved the following result: if p is semi-regular, then $T_p(Q)$ has one generator as a $\mathbb{Z}_p[\Gamma]$-module. Moreover, he also described the annihilator of this action and it has a relation to a certain p-adic L-function.

So, the structure of Cl_n as a module over $Z_p[\Gamma]$ is well understood. However the module structure of Cl_n does not provide a description of Cl_n as an abelian group. It only follows from Iwasawa theory that there are two integer constants λ and γ such that Cl_n has $p^{n\lambda+\gamma}$ elements for n large.

The structure of Cl_n as an abelian group remains unknown.

Some light on this structure comes from the Kervaire-Murthy conjecture in algebraic K-theory.

We proceed with a definition of Picard groups of commutative rings. Let A be a commutative ring with unity. If P is an A-module, we say that P is invertible if there exists another A-module N such that $P \otimes N$ is isomorphic to A^1. Here A^n is a free A-module with n generators. Clearly invertible A-modules form a group, in which A^1 is a unity. This group is called the Picard group of A and it is denoted by $\mathrm{Pic}(A)$.

One can show that $\mathrm{Pic}(\mathbb{Z}[\zeta_n])$ is isomorphic to the class group of $\mathbb{Z}[\zeta_n]$.

In the late 60s and 70s Kervaire and Murthy studied $\mathrm{Pic}(Z[C_n])$, the Picard group of the integer group ring of the cyclic group of order p^n. In his talk at the International Congress of Mathematicians in Nice in 1970 Swan made an announcement that Kervaire and Murthy had completely described $\mathrm{Pic}(Z[C_n])$. However their paper appeared much later, in 1977, where Kervaire and Murthy made very important steps in the description of $\mathrm{Pic}(Z[C_n])$ but the problem was far from being solved.

In fact Kervaire and Murthy did the following:

First of all it is easy to construct a homomorphism

$f : \mathrm{Pic}(Z[C_{n+1}]) \to \mathrm{Pic}(Z[C_n]) \oplus \mathrm{Cl}_n$

This can be done with the help of the so-called Mayer-Vietoris exact sequence, and further consideration of this sequence shows that the above map is surjective. Let $V_n = \ker(f)$. Computations show that it is a p-group of exponent p^n (each element in power p^n is trivial).

Let us recall that the group $< 1, s >$ acts on Cl_n and the action of s comes from complex conjugation. Since the groups C_k can be interpretated as the groups of p^k-roots of unity, $< 1, s >$ acts on $\mathbb{Z}[C_k]$ for each k. Then it follows that $< 1, s >$ acts on V_n. Since V_n is a p-group it follows that $V_n = V_n^+ \oplus V_n^-$

Kervaire and Murthy obtained the exact structure of V_n^- as an abelian group, proved that V_n^+ is trivial if the prime number p is regular and, using the Iwasawa theory, constructed an embedding $V_n^+ \to \mathrm{Cl}_{n-1}$ if p is semi-regular. They also conjectered that in fact V_n^+ and Cl_{n-1} are isomorphic for semi-regular primes.

Using a "gap" theorem for $Z[\zeta_n]$ we proved, together with Ola Helenius, a weak version of this conjecture, namely that these two groups have the same number of generators if p is semi-regular.

In some cases we proved the conjecture and obtained an explicit description of Cl_{n-1} or if you wish V_n^+. Of course we assume that p is semi-regular. We also need the so-called generalized Bernoulli numbers $B_{1,i}, i = 2, 4, ..., p-3$, which we do not define here. It is known that the numerator of $B_{1,i}$ is divisible by p if and only if the numerator of B_i is divisible by p. In what follows we need the following assumption on $B_{1,i}$: its numerator is not divisible by p^2. We proved the following result.

Theorem 4. *Let p be semi-regular and suppose that the numerators of $B_{1,i}, i = 2, 4, ..., p-3$, are not divisible by p^2. Then*

$$V_n^+ = Cl_{n-1} = (C_n)^r \oplus (C_{n-1})^{\lambda - r}.$$

Here r is the number of Bernoulli numbers among $B_2, B_4 ... B_{p-3}$ with numerators divisible by p, λ is one of the Iwasawa invariants above. In numerical computations made up to $p \sim 10\ 000\ 000$ the numerators are not divisible by p^2 and $\lambda = r$.