Interview with Abel Laureate Sir Andrew Wiles

Martin Raussen (Aalborg University, Denmark) and Christian Skau (Norwegian University of Science and Technology, Trondheim, Norway)

The interview took place in Oslo on 23 May 2016.

Professor Wiles, please accept our congratulations for having been selected as the Abel Prize Laureate for 2016. To be honest, the two of us had expected this interview to take place already several years ago!

You are famed not only among mathematicians, but also among the public at large for, and now we cite the Abel Committee: "the stunning proof of Fermat's Last Theorem, by way of the Modularity Conjecture for elliptic curves, opening a new era in number theory". This proof goes back to 1994, which means that you had to wait for more than 20 years before it earned you the Abel Prize. Nevertheless, you are the youngest Abel Prize Laureate so far.

After you finished your proof of Fermat's Last Theorem you had to undergo a deluge of interviews, which makes our task difficult. How on earth are we to come up with questions that you have not answered several times before? Well, we will try to do our best.

Sir Andrew Wiles received the Abel Prize from Crown Prince Haakon of Norway. (Photo Audun Braastad)

Fermat's Last Theorem: A historical account

We have to start at the very beginning, with a citation in Latin: "…nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere", which means: "it is impossible to separate any power higher than the second into two like powers". That is in modern mathematical jargon: The equation $x^n + y^n = z^n$ has no solution in natural numbers for n greater that two. And then it continues: "cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet", which means: "I have discovered a truly marvellous proof of this, which this margin is too narrow to contain". This remark was written in the year 1637 by the French lawyer and amateur mathematician Pierre de Fermat [1601–1665] in the margin of his copy of Diophantus' Arithmetica. He certainly did not expect that it would keep mathematicians, professionals and amateurs alike, busy for centuries trying to unearth the proof.

Could you please give us a short account of some of the attempts towards proving Fermat's Last Theorem up until the time you embarked on your successful journey? Furthermore, why was such a simple-minded question so attractive and why were attempts to prove it so productive in the development of number theory?

The first serious attempt to solve it was presumably by Fermat himself. But unfortunately we know nothing about it except for what he explained about his proofs in the specific cases of $n=3$ and $n=4$.[1] That is, he showed that you can't have the sum of two cubes be another cube, or the sum of two fourth powers being a fourth power. He did this by a beautiful method, which we call infinite descent. It was a new method of proof, or at least a new way of presenting proofs, in arithmetic. He explained this method to his colleagues in letters and he also wrote about it in his famous margin, which was big enough for some of it at least. After the marginal notes were published by Fermat's son after his father's death, it lay dormant for a while. Then it was picked up by Euler [1707–1783] and others who tried to find this truly marvellous proof. And they failed. It became quite dramatic in the mid-19th century – various people thought they could solve it. There was a discussion concerning this in the French Academy – Lamé [1795–1870] claiming he was just about to prove it – and Cauchy [1789–1857] said he thought he could too, and so on.

In fact it transpired that the German mathematician Kummer [1810–1893] had already written a paper where he explained that the fundamental problem was what is known now as the fundamental theorem of arithmetic. In our normal number system any number can be factorized in essentially one way into prime factors. Take a number like 12; it is 2 times 2 times 3. There is no other way of breaking it up. But in trying to solve the Fermat problem you actually want to use systems of numbers where this uniqueness does not

[1] Strictly speaking Euler was the first to spell out a complete proof in the case $p=3$.

hold. Every attempt that was made to solve the Fermat problem had stalled because of this failure of unique factorization. Kummer analysed this in incredible detail. He came up with the most beautiful results, and the end product was that he could solve it for many, many cases. For example for $n \le 100$ he solved it for all primes except for 37, 59 and 67. But he did not finally solve it. His method was based on the idea that Fermat had introduced – the method of infinite descent – but in these new number systems.

The new number systems he was using spawned algebraic number theory as we see it today. One tries to solve equations in these new systems of numbers instead of solving them with ordinary integers and rational numbers. Attempts in the style of Fermat carried on for a while but somewhat petered out in the twentieth century. No one came up with a fundamentally new idea. In the second half of the twentieth century number theory moved on and considered other questions. Fermat's problem was all but forgotten by the professionals.

Then in 1985, Gerhard Frey, a German mathematician, came up with a stunning new idea where he took a hypothetical solution to the Fermat problem and rewrote it so that it made what is called an elliptic curve. And he showed, or suggested, that this elliptic curve had very peculiar properties. He conjectured that you can't really have such an elliptic curve. Building on this a year later an American mathematician, Kenneth Ribet, demonstrated, using this Frey curve, that any solution of Fermat would contradict another well-known conjecture called the Modularity Conjecture. This conjecture had been proposed in a weak form by Taniyama [1927–1958] and refined by Shimura, but the first real evidence for it came from André Weil [1906–1998] who made it possible to check this precise form of the Modularity Conjecture in some detail. And a lot of evidence was amassed showing that this should certainly be true. So at that point mathematicians could see: Yes, Fermat is going to be true. Moreover, there has to be a proof of it.

What happened was that the Modularity Conjecture was a problem that mathematics could not just put to one side and go on for another five hundred years. It was a roadblock right in the middle of modern mathematics. It was a very, very central problem. As for Fermat you could just leave it aside and forget it almost forever. This Modularity Conjecture you could not forget. So at the point when I heard that Ribet had done this I knew that this problem could be solved and I was going to try.

Concerning speculations about Fermat's claimed proof: Do you think he had the same idea as Lamé, assuming, wrongly it turned out, that the cyclotomic integers have unique factorization?

No, I don't think so, though the idea might be in there somewhere. It is very hard to understand. André Weil wrote about this. All the other problems Fermat considered had to do with curves that were of genus zero or genus one. And suddenly he is writing down a curve that has higher genus. How is he going to think about it?

When I was trying this myself as a teenager, I put myself in Fermat's frame of mind because there was hardly anything else I could do. I was capable of understanding his mathematics from the 17th century, but probably not much beyond that. It seemed to me that everything he did came down to something about quadratic forms, and I thought that might be a way of trying to think about it. Of course, I never succeeded, but there is nothing else that suggests Fermat fell into this trap with unique factorization. In fact, from the point of view of quadratic forms he understood that sometimes there was unique factorization and sometimes there was not. So he understood that difference in his own context. I think it is unlikely that that was the mistake.

In the same book by André Weil that you referred to, titled "Number Theory: an approach through history from Hammurapi to Legendre", it is mentioned that Fermat looked at the equation a cube minus a square equal to 2 [$x^3 - y^2 = 2$], and he showed that it has essentially only one solution, namely $x = 3$ and $y = \pm 5$. André Weil speculates that Fermat at the time looked at the ring $\mathbb{Z}[\sqrt{-2}]$, which does have unique factorization.

Yes, he used unique factorization but the way he did it was in terms of quadratic forms. And I think he also looked at quadratic forms corresponding to $\mathbb{Z}[\sqrt{-6}]$ where there is not unique factorization. So I think he understood. It was my impression when I thought about it that he understood the difference.

A mathematical education

You were apparently interested in mathematical puzzles already as a quite young boy. Have you any thoughts about where this interest came from? Were you influenced by anyone in particular?

I just enjoyed mathematics when I was very young. At the age of ten I was looking through library shelves devoted to mathematics. I would pull out books and at one point I pulled out a book of E.T. Bell [1883–1960] titled "The Last Problem", which on its cover describes the Fermat equation, the Wolfskehl Prize and the romantic history of the problem. I was completely captivated by it.

Were there other things that fascinated you in this book by Eric Temple Bell?

It is entirely about that one equation, really. And it is actually quite wordy. So there is less mathematics in some sense than you might think. I think it was more the equation. Then, when I found this equation I looked for other elementary books on number theory and learned about congruences and solved congruences and so on, and looked at other things that Fermat did.

You did this work besides your ordinary school work?

Yes, I don't think my school work was too taxing from that point of view.

Was it already clear for you at that time that you had an extraordinary mathematical talent?

I certainly had a mathematical aptitude and obviously loved to do mathematics, but I don't think I felt that I was unique. In fact, I don't believe I was in the school I attended. There were others who had just as strong a claim to be future mathematicians, and some of them have become mathematicians, too.

Did you plan to study mathematics and to embark on a mathematical career already at that age?
No, I don't think I really understood you could spend your life doing mathematics. I think that only came later. But I certainly wanted to study it as long as I could. I'm sure that as far as my horizon extended it involved mathematics.

You started to study mathematics as a student at Oxford in 1971. Can you tell us a little bit about how that worked out? Were there any particular teachers, any particular areas that were particularly important for you?
Before I went to college, actually in high-school, one of my teachers had a PhD in number theory. He gave me a copy of Hardy and Wright's *An Introduction to the Theory of Numbers*, and I also found a copy of Davenport's *The Higher Arithmetic*. And these two books I found very, very inspiring in terms of number theory.

So you were on track before you started studying?
Yes, I was on track before. In fact, to some extent I felt college was a distraction because I had to do all these other things, applied maths, logic and so on, and I just wanted to do number theory. You were not allowed to do number theory in your first year. And you could not really get down to it before your third year.

But you were not interested in geometry, not as much as in algebra and number theory, anyway?
No, I was primarily interested in algebra and number theory. I was happy to learn these other things, but I really was most excited about number theory. My teachers arranged for me to take extra classes in number theory, but there was not that much on offer.

At one point I decided that I should put all the years of Latin I had done at school to good use and try to read some of Fermat in the original, but I found that was actually too hard. Even if you translated the Latin, the way they wrote in those days wasn't in the algebraic symbols I was used to; so it was quite difficult.

It must have been a relief when you were done and came to Cambridge to start studying number theory for real, with John Coates as your supervisor?
That's right. I had a year, a preliminary year, in which I just studied a range of subjects, and then I could do a special paper. John Coates was not yet at Cambridge, but I think he helped me – maybe over the summer. Anyway, that summer I met him and started working with him right away, and that was just wonderful. The transition from undergraduate work, where you were just reading and studying, to research, that was the real break for me. It was just wonderful.

Elliptic curves

We assume it was John Coates who initiated you to work on elliptic curves, and to Iwasawa theory?
Absolutely. He had some wonderful ideas and was generous to share them with me.

Did you tell John Coates that you were interested in the Fermat problem?
Perhaps I did. I don't remember. It is really true that there hadn't been any new ideas since the 19th century. People were trying to refine the old methods, and, yes, there were refinements. But it didn't look like these refinements and the solution were going to converge. It was just too hard that way.

At the time you started to work with John Coates, you had no idea that these elliptic curves were going to be crucial for the solution of Fermat's Last Theorem?
No, it's a wonderful coincidence. The strange thing is that, in a way, the two things that are most prominent in Fermat that we remember today are his work on elliptic curves and his famous last theorem. For example, this equation you mentioned, $y^2+2=x^3$, is an elliptic curve. And the two strands came together in the proof.

Could you explain what an elliptic curve is and why elliptic curves are of interest in number theory?
For a number theorist the life of elliptic curves started with Fermat as equations of the form y^2 equals a cubic polynomial in x with rational coefficients. Then the problem is to find the rational solutions to such an equation. What Fermat noticed was the following: Sometimes you can start with one or even two rational solutions, and use them to generate infinitely many others. And yet sometimes there are no solutions. This latter situation occurs, for example, in the case $n=3$ of Fermat's Last Theorem, the equation being in fact an elliptic curve in disguise. Sometimes you can show there are no rational solutions. You could have infinitely many and you could have none. This was already apparent to Fermat.

In the early 19th century one studied these equations in complex numbers. Abel [1802–1829] himself came in at this point and studied elliptic functions and related these to elliptic curves, implying that elliptic curves have a group structure. They were very well understood in terms of doubly periodic functions in the early 19th century. But that is what underlies the complex solutions, solutions to the equation in complex numbers.

The solutions to the equation in rational numbers were studied by Poincaré [1854–1912]. What's now known as the Mordell–Weil theorem was proved by Mordell [1888–1972] and then Weil in the 1920s, answering a question of Poincaré. In our setting it says that the K-rational points on an elliptic curve over a number field K, in particular for K equal to the rationals, form a finitely generated abelian group. That is, from Fermat's language you can start with a finite number of solutions and using those generate all the solutions by what he called the chord-and-tangent process.

Birch and Swinnerton–Dyer, Tate–Shafarevich, Selmer…

By now you know the structure, it is a very beautiful algebraic structure, the structure of a group, but that does not actually help you find the solutions. So no one really had any general methods for finding the solutions, until the conjectures of the 1960s, which emerged from the Birch and Swinnerton–Dyer Conjecture. There are two aspects to it; one is somewhat analytic and one is in terms of what is called the Tate–Shafarevich group. Basically the Tate–Shafarevich group gives you the obstruction to an algorithm for finding the solutions. And the Birch and Swinnerton–Dyer Conjecture tells you that there is actually an analytic method for analysing this so-called Tate–Shafarevich group. If you combine all this together, ultimately it should give you an algorithm for finding the solutions.

You worked already on the Birch and Swinnerton–Dyer Conjecture when you were a graduate student together with John Coates?
Yes, that is exactly what he proposed working on. We got the first result in certain special families of elliptic curves on this analytic link between the solutions and what is called the L-function of the elliptic curve.

These were curves admitting complex multiplication?
Exactly, these were the elliptic curves with complex multiplication.

Was this the first general result concerning the Birch and Swinnerton–Dyer Conjecture?
It was the first one that treated a family of cases rather than individual cases. There was a lot of numerical data for individual cases, but this was the first infinite family of cases.

This was over the rational numbers?
Yes.

We should mention that the Birch and Swinnerton–Dyer Conjecture is one of the Clay Millennium Prize Problems which would earn a person who solves it one million dollars.
That's right. I think it's appealing, partly because it has its roots in Fermat's work, just like the Fermat problem. It is another 'elementary to state' problem, concerned with equations – in this case of very low degree – which we can't master and which Fermat initiated. I think it is a very appealing problem.

Do you think it is within reach? In other words, do we have the necessary tools for somebody daring enough to attack it and succeed? Or do we have to wait for another three hundred years to see it solved?
I don't suppose it will take three hundred years, but I don't think it is the easiest of the Millennium Problems. I think we are still lacking something. Whether the tools are all here now, I am not sure. They may be. There are always these speculations with these really difficult problems; it may be that the tools simply aren't there.

I don't believe that anyone in the 19th century could have solved Fermat's Last Theorem, certainly not in the way it was eventually solved. There was just too big a gap in mathematical history. You had to wait another hundred years for the right pieces to be in place. You can never be quite sure about these problems whether they are accessible to your time. That is really what makes them so challenging; if you had the intuition for what can be done now and what can't be done now you would be a long way towards a solution!

You mentioned the Tate–Shafarevich group and in that connection the Selmer group appears. Selmer [1920–2006] was a Norwegian mathematician, and it was Cassels [1922–2015] who is responsible for naming this group the Selmer group. Could you say a few words about the Selmer group and how it is related to the Tate–Shafarevich group, even if it's a little technical?
It is technical, but I can probably explain the basic idea of what the Selmer group is. What you are trying to do is to find the rational solutions on an elliptic curve. The method is to take the rational points on the elliptic curve – suppose you have got some – and you generate field extensions from these. So when I say generate extensions, I mean that you can take roots of those points on the elliptic curve. Just like taking the n'th root of 5 or the cube root of 2. You can do the same thing on an elliptic curve, you can take the n'th root of a point. These are all points which *added to themselves n times* gives you the point you started with. They generate certain extensions of the number field you started with, so in our case of the rational number field $\mathbb{Q}$.

You can put a lot of restrictions on those extensions. And the Selmer group is basically the smallest set of extensions you can get putting on all the obvious restrictions.

Let me summarize this. You've got the group of points. They generate some extensions; that's too big, you don't want all extensions. You cut that down as much as you can using local criteria, using p-adic numbers; that's called the Selmer group. And the difference essentially between the group generated by the points and the Selmer group is the Tate–Shafarevich group. So the Tate–Shafarevich group gives you the error term if you like, in trying to get at the points via the Selmer group.

Selmer's paper, which Cassels refers to, studied the Diophantine equation, $3x^3+4y^3+5z^3=0$ and similar ones. Selmer showed that it has just a trivial solution in the integers, while modulo n it has non-trivial solutions for all n. In particular, this curve has no rational points. Why did Cassels invoke Selmer's name in naming the group?
Yes, there are quite subtle relationships between these. What happens is you are actually looking at one elliptic curve, which in this case would be $x^3+y^3+60z^3=0$. That is an elliptic curve, in disguise, if you like, and the Tate–Shafarevich group involves looking at other ones

like it, for example $3x^3+4y^3+5z^3=0$, which is a genus one curve, but which has no rational points. Its Jacobian is the original elliptic curve, $x^3+y^3+60z^3=0$. One way of describing the Tate–Shafarevich group is in terms of these curves that have genus one but don't have rational points. And by assembling these together you can make the Tate–Shafarevich group, and that is reflected in the Selmer group. It is too intricate to explain in words but it is another point of view. I gave it in a more arithmetic terminology in terms of extensions. The more geometric terminology was in terms of these twisted forms.

The Modularity Conjecture

What you proved in the end was a special case of what is now called the Modularity Conjecture. In order to explain this one has to start with modular forms, and how modular forms can be put in relation with elliptic curves. Could you give us some explanations?
Yes; an elliptic curve (over the rationals) we have described as an equation $y^2=x^3+ax+b$, where the a and b are assumed to be rational numbers. (There is also a condition that the discriminant should not vanish). As I said, at the beginning of the 19th century you could describe the complex solutions to this equation. You could describe these very nicely in terms of the Weierstrass $\wp$-function, in terms of a special elliptic function. But what we want is actually a completely different uniformization of these elliptic curves which captures the fact that the a and b are rational numbers. It is a parametrization just for the rational elliptic curves. And because it captures the fact that it is defined over the rationals it gives you a much better hold on solutions over the rationals than the elliptic functions do. The latter really only sees the complex structure.

And the place it comes from are modular forms or modular curves. To describe modular functions first: we are used to functions which satisfy the relation of being invariant under translation. Every time we write down a Fourier series we have a function which is invariant under translation. Modular functions are ones which are invariant under the action of a much bigger group, usually a subgroup of $SL_2(\mathbb{Z})$. So, you would ask for a function $f(z)$ in one complex variable, usually on the upper half plan, which satisfies $f(z)$ is the same as $f((az+b)/(cz+d))$; or more generally, is that times a power of $cz+d$.

These are called modular functions and were extensively studied in the 19th century. Surprisingly they hold the key to the arithmetic of elliptic curves. Perhaps the simplest way to describe it is that because we have an action of $SL_2(\mathbb{Z})$ on the upper half plane H – by the action z goes to $(az+b)/(cz+d)$ – we can look at the quotient H modulo this action. You can then give the quotient the structure of a curve. In fact, it naturally gets the structure of a curve over the rational numbers.

If you take a subgroup of $SL_2(\mathbb{Z})$, or more precisely what is called a congruence subgroup, defined by the c value being divisible by N, then you call the curve a modular curve of level N. The Modularity Conjecture asserts that every elliptic curve over the rationals is actually a quotient of one of these modular curves for some integer N. It gives you a uniformization of elliptic curves by these other entities, these modular curves. On the face of it, it might seem we are losing because this is a high genus curve, it is more complicated. But it actually has a lot more structure because it is a moduli space.

And that is a very powerful tool?
That is a very powerful tool, yes. You have function theory, you have deformation theory, geometric methods etc. You have a lot of tools to study it.

Taniyama, the young Japanese mathematician who first conjectured or suggested these connections, his conjecture was more vague, right?
His conjecture was more vague. He didn't pin it down to a function invariant under the modular group. I've forgotten exactly what he conjectured; it was invariant under some kind of group, but I forget exactly which group he was predicting. But it was not as precise as the congruence subgroups of the modular group. I think it was originally written in Japanese so it was not circulated as widely as it might have been. I believe it was part of notes compiled after a conference in Japan.

It was an incredibly audacious conjecture at that time, wasn't it?
Apparently, yes.

But then it gradually caught the attention of other mathematicians. You told us already about Gerhard Frey, who came up with a conjecture relating Fermat's Last Theorem with the Modularity Conjecture.
That's right. Gerhard Frey showed that if you take a solution to the Fermat problem, say $a^p+b^p=c^p$, and you create the elliptic curve $y^2=x(x-a^p)(x+b^p)$, then the discriminant of that curve would end up being a perfect p'th power. And if you think about what that means assuming the Modularity Conjecture – you have to assume something a bit stronger as well (the so called epsilon conjecture of Serre) – then it forces this elliptic curve to have the level N that I spoke about to be equal to one, and hence the associated congruence subgroup is equal to $SL_2(\mathbb{Z})$. But H modulo $SL_2(\mathbb{Z})$ is a curve of genus zero. It has no elliptic curve quotient so it wasn't there after all, and hence there can't be a solution to the Fermat problem.

The quest for a proof

That was the point of departure for your own work, with crucial further ingredients due to Serre and Ribet making this connection clear. May we briefly summarize the story that then follows? It has been told by you many times, and it is the focus of a BBC-documentary.

You had moved to the United States, first to Harvard, then to Princeton University, becoming a professor there. When you heard of Ribet's result you devoted all your research time to prove the Modularity Con-

jecture for semistable elliptic curves over the rationals. This work went on for seven years of really hard work in isolation. At the same time you were working as a professor in Princeton and you were raising small kids.

A proof seems to be accomplished in 1993, and the development culminates in a series of three talks at the Isaac Newton Institute in Cambridge back in England, announcing your proof of Fermat's Last Theorem. You are celebrated by your peer mathematicians. Even the world press takes an interest in your results, which happens very rarely for mathematical results.

But then when your result is scrutinized by six referees for a highly prestigious journal, it turns out that there is a subtle gap in one of your arguments, and you are sent back to the drawing board. After a while you send for your former student, Richard Taylor, to come to Princeton to help you in your efforts. It takes a further ten months of hard and frustrating work; we think we do not exaggerate by calling it a heroic effort under enormous pressure. Then in a sudden flash of insight you realize that you can combine some of your previous attempts with new results to circumvent the problem that had caused the gap. This turns out to be what you need in order to get the part of the Modularity Conjecture that implied Fermat's Last Theorem.

What a relief that must have been! Would you like to give a few comments to this dramatic story?

With regard to my own work when I became a professional mathematician working with Coates I realized I really had to stop working on Fermat because it was time-consuming and I could see that in the last hundred years almost nothing had been done. And I saw others, even very distinguished mathematicians, had come to grief on it. When Frey came out with this result, I was a bit sceptical that the Serre part of the conjecture was going to be true, but when Ribet proved it then, okay, this was it!

And it was a long hard struggle. In some sense it is irresponsible to work on one problem to the exclusion of everything else, but this is the way I tend to do things. Whereas Fermat is very narrow, I mean it is just this one equation, whose solution may or may not help with anything else, yet the setting of the modular conjecture was one of the big problems in number theory. It was a great thing to work on anyway, so it was just a tremendous opportunity.

When you are working on something like this it takes many years to really build up the intuition to see what kinds of things you need and what kinds of things a solution will depend on. It's something like discarding everything you can't use and won't work till your mind is so focused that even making a mistake, you've seen enough that you'll find another way to the end.

Funnily enough, concerning the mistake in the argument that I originally gave, people have worked on that aspect of the argument and quite recently they have actually shown that you can produce arguments very like that. In fact, in every neighbouring case arguments similar to the original method seem to work but there is this unique case that it doesn't seem to work for, and there is not yet any real explanation for it. So the same kind of argument I was trying to use, using Euler systems and so on, has been made to work in every surrounding case but not the one I needed for Fermat. It's really extraordinary.

You once likened this quest for the proof of the Modularity Theorem in terms of a journey through a dark unexplored mansion. Could you elaborate?

I started off really in the dark. I had no prior insights how the Modularity Conjecture might work or how you might approach it. One of the troubles with this problem – it's a little like the Riemann Hypothesis but perhaps even more so with this one – is you didn't even know what branch of mathematics the answer would be coming from.

To start with, there are three ways of formulating the problem, one is geometric, one is arithmetic and one is analytic. And there were analysts – I would not understand their techniques at all well – who were trying to make headway on this problem.

I think I was a little lucky because my natural instinct was with the arithmetic approach and I went straight for the arithmetic route, but I could have been wrong. The only previously known cases where the Modularity Conjecture were known to hold were the cases of complex multiplication, and that proof is analytic, completely analytic.

Partly out of necessity, I suppose, and partly because that's what I knew, I went straight for an arithmetic approach. I found it very useful to think about it in a way that I had been studying in Iwasawa theory. With John Coates I had applied Iwasawa theory to elliptic curves. When I went to Harvard I learned about Barry Mazur's work, where he had been studying the geometry of modular curves using a lot of the modern machinery. There were certain ideas and techniques I could draw on from that. I realized after a while I could actually use that to make a beginning – to find some kind of entry into the problem.

Before you started on the Modularity Conjecture, you published a joint paper with Barry Mazur, proving the main theorem of Iwasawa Theory over the rationals. Can you please tell us what Iwasawa Theory is all about?

Iwasawa theory grew out of the work of Kummer on cyclotomic fields and his approach to Fermat's Last Theorem. He studied the arithmetic, and in particular the ideal class groups, of prime cyclotomic fields. Iwasawa's idea was to consider the tower of cyclotomic fields obtained by taking all p-power roots of unity at once. The main theorem of Iwasawa theory proves a relation between the action of a generator of the Galois group on the p-primary class groups and the p-adic L-functions. It is analogous to the construction used in the study of curves over finite fields where the characteristic polynomial of Frobenius is related to the zeta function.

And these tools turned out to be useful when you started to work on the Modularity Conjecture?

They did, they gave me a starting point. It wasn't obvious at the time, but when I thought about it for a while I realized that there might be a way to start from there.

Parallels to Abel's work

We want to read you a quotation: "The ramparts are raised all around but, enclosed in its last redoubt, the problem defends itself desperately. Who will be the fortunate genius who will lead the assault upon it or force it to capitulate?"

It must been E.T. Bell, I suppose? Is it?

No, it's not. It is actually a quote from the book "Histoire des Mathématiques" by Jean-Étienne Montucla [1725–1799], written in the late 18th century. It is really the first book ever written on the history of mathematics. The quotation refers to the solvability or unsolvability of the quintic equation by radicals.

As you know Abel [1802–1829] proved the unsolvability of the general quintic equation when he was 21 years old. He worked in complete isolation, mathematically speaking, here in Oslo. Abel was obsessed, or at least extremely attracted, to this problem. He also got a false start. He thought he could prove that one could actually solve the quintic by radicals. Then he discovered his mistake and he finally found the unsolvability proof.

Well, this problem was at that time almost 300 years old and very famous. If we move fast forward 200 years the same quotation could be used about the Fermat problem, which was around 350 years old when you solved it. It is a very parallel story in many ways. Do you have comments?

Yes. In some sense I do feel that Abel, and then Galois [1811–1832], were marking a transition in algebra from these equations which were solvable in some very simple way to equations which can't be solved by radicals. But this is an algebraic break that came with the quintic. In some ways the whole trend in number theory now is the transition from basically abelian and possibly solvable extensions to insolvable extensions. How do we do the arithmetic of insolvable extensions?

I believe the Modularity Conjecture was solved because we had moved on from this original abelian situation to a non-abelian situation, and we were developing tools, modularity and so on, which are fundamentally non-abelian tools. (I should say though that the proof got away mostly with using the solvable situation, not because it was more natural but because we have not solved the relevant problems in the general non-solvable case).

It is the same transition in number theory that he was making in algebra, which provides the tools for solving this equation. So I think it is very parallel.

There is an ironic twist with Abel and the Fermat Problem. When he was 21 years old, Abel came to Copenhagen to visit Professor Degen [1766–1825], who was the leading mathematician in Scandinavia at that time. Abel wrote a letter to his mentor in Oslo, Holmboe [1795–1850], stating three results about the Fermat equation without giving any proofs – one of them is not easy to prove, actually. This, of course, is just a curiosity today.

But in the same letter he gives vent to his frustration, intimating that he can't understand why he gets an equation of degree n^2, and not n, when dividing the lemniscate arc in n equal pieces. It was only after returning to Oslo that he discovered the double periodicity of the lemniscate integral, and also of the general elliptic integral of the first kind.

If one thinks about it, what he did on the Fermat equation turned out to be just a curiosity. But what he achieved on elliptic functions, and implicitly on elliptic curves, turned out later to be a relevant tool for solving it. Of course, Abel had no idea that this would have anything to do with arithmetic. So this story tells us that mathematics sometimes develops in mysterious ways.

It certainly does, yes.

Work styles

May we ask for some comments about work styles of mathematicians in general and also about your own? Freeman Dyson, a famous physicist and mathematician at IAS in Princeton, said in his Einstein lecture in 2008: "Some mathematicians are birds, others are frogs. Birds fly high in the air and survey broad vistas of mathematics out to the horizon. They delight in concepts that unify our thinking and bring together diverse problems from different parts of the landscape. Frogs live in the mud below and see only the flowers that grow nearby. They delight in the details of particular objects and they solve problems one at a time".

Freeman Dyson didn't say that birds were better than frogs, or the other way around. He considered himself a frog rather than a bird.

When we are looking at your work, it seems rather difficult for us to decide where to place you in his classification scheme: among the birds, those who create theories, or among the frogs, those who solve problems. What is our own perception?

Well, I don't feel like either. I'm certainly not a bird – unifying different fields. I think of frogs as jumping a lot. I think I'm very, very focused. I don't know what the animal analogy is, but I think I'm not a frog in the sense that I enjoy the nearby landscape. I'm very, very concentrated on the problem I happen to work on and I am very selective. And I find it very hard to even take my mind off it enough to look at any of the flowers around, so I don't think that either of the descriptions quite fits.

Based on your own experience could you describe the interplay between hard, concentrated and persevering work on the one side, and on the other side these sudden flashes of insights that seemingly come out of nowhere, often appearing in a more relaxed setting. Your mind must have worked unconsciously on the problem at hand, right?

I think what you do is that you get to a situation where you know a theory so well, and maybe even more than one theory, so that you have seen every angle and tried a lots of different routes.

It is this tremendous amount of work in the preparatory stage where you have to understand all the details, and maybe some examples, that is your essential launch pad. When you have developed all this, then you let the mind relax and then at some point – maybe when you go away and do something else for a little bit – you come back and suddenly it is all clear. Why did you not think of that? This is something the mind does for you. It is the flash of insight.

I remember – this is a trivial example in a non-mathematical setting – once someone showed me some script, it was some gothic script, and I couldn't make head or tail of it. I was trying to understand a few letters, and I gave up. Then I came back half an hour later and I could read the whole thing. The mind somehow does this for you and we don't quite know how, but we do know what we have to do to set up the conditions where it will happen.

This is reminiscent of a story about Abel. While in Berlin he shared an apartment with some Norwegian friends, who were not mathematicians. One of his friends said that Abel typically woke up during the night, lighted a candle and wrote down ideas that he woke up with. Apparently his mind was working while asleep.

Yes, I do that except I don't feel the need to write them down when I wake up with it because I know I will not forget it. But I am terrified if I have an idea when I am about to go to sleep that I would not wake up with that idea, so then I have to write it down.

Are you thinking in terms of formulas or in terms of geometric pictures, or what?

It is not really geometric. I think it is patterns, and I think it is just parallels between situations I have seen elsewhere and the one I am facing now. In a perfect world, what is it all pointing to, what are the ingredients that ought to go into this proof, what am I not using that I have still in my pocket? Sometimes it is just desperation. I assemble every piece of evidence I have and that's all I've got. I have got to work with that and there is nothing else.

I often feel that doing mathematics is like being a squirrel and there are some nuts at the top of a very tall tree. But there are several trees and you don't know which one. What you do is that you run up one and you think, no, it does not look good on this one, and you go down and up another one, and you spend your whole life just going up and down these trees but you've only got up to thirty feet. Now if someone told you the rest of the trees – it's not in them, you have only one tree left, then you would just keep going until you found it. In some sense it is ruling out the wrong things that is really crucial. And if you just believe in your intuition, and your intuition is correct, and you stick with your one tree then you will find it.

Problems in mathematics

Felix Klein [1849–1925] once said: "Mathematics develops as old results are being understood and illuminated by new methods and insights. Proportionally with a better and deeper understanding new problems naturally arise." And David Hilbert [1862–1943] stressed that "problems are the lifeblood of mathematics". Do you agree?

I certainly agree with Hilbert, yes. Good problems are the lifeblood of mathematics. I think you can see this clearly in number theory in the second half of the last century. For me personally obviously the Modularity Conjecture, but also the whole Langlands Program and the Birch and Swinnerton–Dyer Conjecture: These problems give you a very clear focus on what we should try to achieve. We also have the Weil Conjectures on curves and varieties over finite fields and the Mordell Conjecture and so on.

These problems somehow concentrate the mind and also simplify our goals in mathematics. Otherwise we can get very, very spread out and not sure what's of value and what's not of value.

Do we have as good problems today as when Hilbert formulated his twenty-three problems in 1900?

I think so, yes.

Which one do you think is the most important problem today? And how does the Langlands program fit in?

Well, I think the Langlands program is the broadest spectrum of problems related to my field. I think that the Riemann Hypothesis is the single greatest problem from the areas I understand. It is sometimes hard to say exactly why that is, but I do believe that solving it would actually help solve some of these other problems. And then of course I have a very personal attachment to the Birch and Swinnerton–Dyer Conjecture.

Intuition can lead us astray sometimes. For example, Hilbert thought that the Riemann Hypothesis would be solved in his lifetime. There was another problem on his list, the 7th, that he never thought would be solved in his lifetime, but which was solved by Gelfond [1906–1968] in 1934. So our intuition can be wrong.

That is right. I'm not surprised that Hilbert felt that way. The Riemann Hypothesis has such a clear statement and we have the analogue in the function field setting. We understand why it is true there, and we feel we ought to be able to translate it. Of course, many people have tried and failed. But I would still myself expect it to be solved before the Birch and Swinnerton–Dyer Conjecture.

Investing in mathematics

Let's hope we'll find out in our lifetimes!

Classical mathematics has, roughly speaking, two sources: one of them coming from the physical sciences and the other one from, let's for simplicity call it num-

ber theoretical speculations, with number theory not associated to applications.

That has changed. For example, your own field of elliptic curves has been applied to cryptography and security. People are making money with elliptic curves nowadays! On the other hand, many sciences apart from physics really take advantage and profit from mathematical thinking and mathematical results. Progress in industry nowadays often depends on mathematical modelling and optimization methods. Science and industry propose challenges to the mathematical world.

In a sense, mathematics has become more applied than it ever was. One may ask whether this is a problem for pure mathematics. It appears that pure mathematics sometimes is put to the side lines, at least from the point of view of the funding agencies. Do you perceive this as a serious problem?

Well, I think in comparison with the past one feels that mathematicians two, three hundred years ago were able to handle a much broader spectrum of mathematics, and a lot more of it touched applied mathematics than would a typical pure mathematician do nowadays. On the other hand that might be because we only remember the very best and most versatile mathematicians from the past.

I think it is always going to be a problem if funding agencies are short-sighted. If they want to see a result in three years then it is not going to work. It is hard to imagine a pure development and then the application all happening within three to five years. It is probably not going to happen.

On the other hand, I don't believe you can have a happily functioning applied maths world without the pure maths to back it up, providing the future and keeping them on the straight and narrow. So it would be very foolish not to invest in pure mathematics.

It is a bit like only investing in energy resources that you can see now. You have to invest in the future; you have to invest in fusion power or solar power or these other things. You don't just use up what is there and then start worrying about it when it is gone. It is the same with mathematics, you can't just use up the pure mathematics we have now and then start worrying about it when you need a pure result to generate your applications.

Mathematical awards

You have already won a lot of prizes as a result of your achievements, culminating in proving Fermat's Last Theorem. You have won the Rolf Schock Prize, given by the Swedish Academy, the Ostrowski Prize, which was given to you in Denmark, the Fermat Prize in France, the Wolf Prize in Israel, the Shaw Prize in Hong Kong – the prize that has been named the Nobel Prize of the East; and the list goes on, ending with the Abel Prize tomorrow. May we ask you whether you enjoy these awards and the accompanying celebrations?

I certainly love them, I have to say. I think they are a celebration of mathematics. I think with something like Fermat it is something people are happy to see in their lifetime. I would obviously be very happy to see the Riemann Hypothesis solved. It is just exciting to see how it finally gets resolved and just to understand the end of the story. Because a lot of these stories we won't live to see the end of. Each time we do see the end of such a story it is something we naturally will celebrate. For me I learned about the Fermat problem from this book of E.T. Bell and about the Wolfskehl Prize attached to it. The Wolfskehl Prize was still there – only just I may say – I only had a few years left before the deadline for it expired.

This gives us the lead to talk a little about that prize. The Wolfskehl Prize was founded in 1906 by Paul Wolfskehl [1856–1906], who was a German physician with an interest in mathematics. He bequeathed one hundred thousand Reichmarks (equivalent to more than one million dollars in today's money) to the first person to prove Fermat's Last Theorem. The prize was, according to the testament, valid until September 13, 2007, and you received it in 1997. By then, due in part to hyperinflation Germany suffered after World War I, the prize money had dwindled a lot.

For me the amount of money was unimportant. It was the sentimental feeling attached to the Wolfskehl Prize that was important for me.

Graduate students

You have had altogether twenty-one PhD-students and you have attracted very gifted students. Some of them are really outstanding. One of them, Manjul Bhargava, won the Fields medal in 2014. It must have been a pleasure to be advisor to such students?

Yes, I don't want to take too much credit for it. In the case of Manjul I suggested a problem to him but after that I had nothing much more to do. He was coming up with these absolutely marvellous discoveries. In some sense you get more credit if you have very gifted students, but the truth is that very gifted students don't really require that much help.

What is the typical way for you of interacting with graduate students?

Well, I think the hardest thing to learn as a graduate student is that afterwards you need to carry on with the rest of your professional life; it's hard to pick problems. And if you just assign a problem and they do it, in some sense that hasn't given them terribly much. Okay, they solved that problem, but the hard thing is then to have to go off and find other problems! So I prefer it if we come to a decision on the problem together.

I give them some initial idea and which area of mathematics to look at, having not quite focused on the problem. Then as they start working and become experts they can see a better way of pinning down what the right question is. And then they are part of the process of choosing the problem. I think that is a much better investment for their future. It doesn't always work out that way, and sometimes the initial problem you give them turns out to be the right thing. But usually it is not that way, and usually it's a process to find the right problem.

Hobbies and interests

We always end the Abel interviews by asking the laureate what he enjoys doing when he doesn't work with mathematics. What are your hobbies and interests outside of mathematics?
Well, it varies at different times. When I was doing Fermat, and being a father with young children, that combination was all-consuming.

I like to read and I like various kinds of literature, novels, some biographies, it is fairly balanced. I don't have any other focused obsessions. When I was in school I played on chess teams and bridge teams, but when I started to do serious mathematics I completely lost interest in those.

What about music; are you fond of music?
I go and listen to concerts, but I am not myself actively playing anything. I enjoy listening to music, classical, preferably.

Are you interested in other sciences apart from mathematics?
I would say somewhat. These are things I do to relax, so I don't like them to be too close to mathematics. If it is something like animal behaviour or astrophysics or something from a qualitative point of view, I certainly enjoy learning about those. Likewise about what machines are capable of, and many other kinds of popular science, but I'm not going to spend my time learning the details of string theory. I'm too focused to be willing to do that. Not that I would not be interested, but this is my choice.

We would like to thank you very much for this wonderful interview. That is first of all on behalf of the two of us, but also on the behalf of the Norwegian, the Danish and the European Mathematical Society.

Thank you so much!
Thank you very much!

From left to right: Sir Andrew Wiles, Martin Raussen and Christian Skau. (Photo: Eirik F. Baardsen, DNVA.)

Martin Raussen is a professor with special responsibilities (mathematics) at Aalborg University, Denmark. Christian Skau is a professor of mathematics at the Norwegian University of Science and Technology at Trondheim. Together, they have held interviews with all the Abel Laureates since 2003.