London Mathematical Society Impact150 Stories 1 (2016) 59–62
doi:10.1112/i150lms/t.0004

How Number Theory Enables a Secure Internet

Nigel P. Smart

If you use a mobile phone, have a games console, or use a variety of Internet services then most likely you are utilizing the results of over 200 years of research in the mathematics of elliptic curves. Elliptic curve based cryptography is all around us, yet it is the outcome of hundreds of years of research into basic pure mathematics. It is a great story of how the impact of mathematics cannot be predicted; indeed we shall see that not even mathematicians can predict impact of their work 5-10 years ahead of time.

For want of sounding like an episode from The Big Bang Theory; Our story starts in ancient Greece. It is well known that ancient Greek mathematics was concerned with geometry and in particular that of the circle. In high school we learn about the functions sine, cosine and tangent, which enable us to perform calculations with the circle. For example by computing arc lengths, areas and the like. In addition the Greeks examined the geometry of the other conic sections; the parabola and the ellipse. Both the circle, parabola and the ellipse can be described by quadratic equations; and one of the most famous ancient Greek results was the work of Pythagoras on integer solutions to the equation

$$x^2 + y^2 = z^2.$$

We now jump forward hundreds of years to a series of what looks like disparate different generalizations of the above ancient work. On one hand we have the famous generalisation of Pythagoras by Fermat; namely "Fermat's Last Theorem" where he examined the integer solutions to the equation

$$x^n + y^n = z^n.$$

On the other hand there was an interest in generalizing sine, cosine etc to the case of dealing with arc lengths and areas of ellipses. An endeavor which led to the creation of the elliptic functions; these are functions which are the natural extension of the sine and cosine functions from school; and they arise in many areas of mathematics; for example in the solution of various differential equations.

A final generalisation came from extending the quadratic equations considered by the ancients to cubic equations. This turned out to be related to the elliptic functions above; just as elliptic functions could be combined (or added) to form new elliptic functions it turned out that on a wide class of cubic equations the solutions of the equation could also be combined (or added) to form new equations. The equations which had this property ended up being called "elliptic curves", and it was found that the operation of obtaining new points from old ones endowed the solutions of an elliptic curve with a group law.

We now fast forward to the 1970's. In the intervening years the pure mathematical study of these results appeared to grow further and further away from reality. The study of Fermat's Last Theorem produced some amazingly beautiful mathematics in the area known as Number Theory; but none of this work would seem to have any application in what we would now call "impact". Indeed the famous British number theorist, writing around the time of the Second World War, G.H. Hardy wallowed in the uselessness of number theory.

Received 27 Feb 2013.

2010 *Mathematics Subject Classification* 11Y16, 11T71, 94A60.

Much of United Kingdom number theory from the Second World War onwards has been focused on understanding the theory of elliptic curves. From early work of Mordell in Cambridge [**11**] (whose work was then generalized by Weil), through to the work of Cassels on the Selmer group attached to an elliptic curve [**5**]. The early computing era allowed Birch and Swinnerton-Dyer to conduct (using the EDSAC computer in Cambridge) a series of ground breaking experiments in trying to understand the theoretical properties of these curves [**1**, **2**]. Indeed by the 1970's the pure mathematics community realized that elliptic curves provided an area for investigation into some of the great unifying theories of pure mathematics; aiming to find subtle connections between analysis, algebra and geometry.

Let us pause to just list some of the topics from pure mathematics developed up to the point of the 1970's which would probably be considered of little value at the time, but which were related to these theoretical questions: p-adic numbers, modular curves, the Weil and Tate pairings, class groups, class field theory,

We now turn to three different developments ranging over the decade of between 1975 and 1985. In the first development, Hardy's puritan view of number theory was overturned when Diffie, Hellman, Rivest, Shamir and Adleman [**6**, **12**] invented the concept of public key cryptography. This is a form of cryptography which seems intertwined with number theory; the first schemes developed in the 1970's were based on the difficulty of factoring large numbers. Without public key cryptography the Internet as we currently know it could not exist; as it would be impossible to securely transmit data without having pre-agreed some shared secret key.

In a second development Rene Schoof was asked a relatively random question by Henri Cohen (who was visiting Hendrik Lenstra in Amsterdam at the time). Rene was a student at the time, and the question was whether there was a fast algorithm to compute the number of points on an elliptic curve over a finite field. Rene answered the question in the affirmative that evening, but decided to do nothing with the algorithm as this seemed to be a problem completely lying within the realm of pure mathematics. Submitting the algorithm to a journal Rene tagged on a relatively dull application to finding square roots in a finite field so as to show some "application". The paper was finally published in 1985 [**14**].

The resulting algorithm, now called Schoof's algorithm, used much of the beautiful pure mathematics developed over the previous 150 years. For example, in an extension by Atkin and Elkies (which is the variant now implemented) modular forms are used in a vital way.

At around the same time Victor Miller was looking at an algorithm to compute the Weil pairing, a mathematical object which had been invented so as to solve the problem of finding the number of rational solutions to an elliptic curve equation. Which itself links to the prior work of Mordell and Cassels on the Selmer group. Miller found that a prior statement of Davenport that the function would be hard to compute was false. Indeed Miller found a very efficient algorithm, now called Miller's algorithm, but just like Schoof the algorithm was not seen to be interesting as it had no obvious compelling application. It was not until 2004 that Miller's paper was finally published [**10**]; although a manuscript had been circulating for many years previously.

So we now find ourselves in the mid 1980's. We have public key cryptography and a bunch of apparently useless mathematics lying around which are related to elliptic curves. At this point Victor Miller [**9**] and Neil Koblitz [**4**] independently come up with the concept that elliptic curves could be used to construct new public key cryptosystems. Not only that but the resulting cryptographic systems would be more secure and more efficient than the ones based on integer factoring. The invention of this Elliptic Curve Cryptography was announced in 1985 at two separate events.

However, a key obstacle remained. To produce elliptic curves for use in cryptography one needed a method to compute the number of points on an elliptic curve over a finite field. Luckily we already knew how to do this efficiently, due to Schoof's algorithm published in the

same year. Note, this is the same algorithm which had a few months previously been rejected due to lack of application!

Before continuing with our narrative, it is worthwhile stopping to say that since the mid 1980's even more advanced techniques have been applied to the computation of the number of points on an elliptic curve, bringing in various areas of hitherto "theoretical" mathematics. One algorithm is specially tailored to curves whose endormorphism ring is an order in a quadratic number field with low class number; this algorithm uses class field theory to solve the problem. Another method, Satoh's algorithm, (now used for small finite fields) makes use of p-adic numbers, isogeny cycles, the arithmetic-geometric mean amongst other things. The generalisation to higher degree curves brings in the areas such as cohomology theory and algebraic geometry.

However, despite Schoof's algorithm being available, in the late 1980's the existing implementation of Schoof's algorithm were too slow. Therefore to implement early Elliptic Curve based systems implementers turned to using curves for which the number of points was easy to compute. The main class they settled on were the so-called supersingular curves. These are curves whose endomorphism ring (the ring of maps from the curve to itself) is isomorphic to an order (essentially a sub-ring) in a quaternion algebra. These are very special curves, since most elliptic curves over finite fields have endomorphism ring isomorphic to an order in a quadratic number field.

However in the early 1990's an attack was found on supersingular curves which meant they were not as secure as had at first been thought [**8**]. And what was the main trick needed to implement this attack? None other than that other algorithm with no application, the one used to compute the Weil and Tate pairing, i.e. Miller's algorithm. Indeed, Miller's work had pointed at the fact that such an attack would exist. Luckily however by this time various mathematical improvements and increases in computing power enabled the implementation of Schoof's algorithm. This enabled the easy switch to general curves (or "ordinary" elliptic curves), and the increasing uses of elliptic curves in systems. As remarked at the beginning of the piece, one can now find elliptic curves in almost all of the high-tech equipment we currently use in our day to day lives. Indeed they are planned to be incorporated in the next generation of chip-and-pin payment technology.

Returning to an early aspect of the story, we find in the mid 1990s the most celebrated result of twentieth century mathematics; namely the proof by Wiles of Fermat's Last Theorem [**15**]. This is the highpoint of pure mathematical achievement, but it to is related to our story. The proof of Fermat's Last Theorem is intertwined with the theory of elliptic curves, indeed the result follows from showing that a certain class of elliptic curves are "modular". Here the term modular means that they can be parametrized by complex functions which possess remarkable symmetries. These complex functions are called modular forms; and the modular forms are themselves related to the modular curves. The self same modular curves which arise in Schoof's algorithm.

But our story does not end there. For around eight years, until 2001, it was thought that Miller's algorithm provided a negative result in cryptography; namely that supersingular elliptic curves were not as secure as ordinary elliptic curves. But the reduction in security is only compared to the gold standard of ordinary curves. In 2001 a series of papers arose [**3**, **7**, **13**] which showed how curves which possess efficiently computable pairings on them could be used to solve a number of long standing problems in cryptography. Thus was born a whole new field called "Pairing Based Cryptography". At the heart of this new field was research to compute the Weil and Tate pairings (and other pairings) highly efficiently; and all of this research follows from Miller's unpublished algorithm. Indeed this is why in 2004 Miller's paper was eventually published. At the time of writing, pairing based cryptography can be found in a number of products.

So finally we see that it is very hard to predict where pure mathematical research will lead us. Even mathematicians themselves are unable to predict this, and often (as in the case of Miller and Schoof) reject work due to its "inapplicability" despite major commercial impact being just around the corner. Without the work of pure mathematicians over thousands of years, and in particular the work on the number theory of elliptic curves performed since the Second World War, we would today not have this important foundational technology for our information age.

References

1. B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, **212**, 7–25, 1963.

2. B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, **218**, 79–108, 1965.

3. D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In *Advances in Cryptology – CRYPTO 2001*, Springer-Verlag LNCS 2139, 213–229, 2001.

4. N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, **48**, 203–209, 1987.

5. J.W.S. Cassels. Arithmetic on curves of genus 1. III The Tate-Safarevic and Selmer groups. *Proc. London Math. Soc.*, **12**, 259–296, 1962.

6. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. on Info. Th.*, **22**, 644–654, 1976.

7. A. Joux. A one round protocol for tripartite Diffie–Hellman. In *Algorithmic Number Theory Symposium – ANTS IV*, Springer-Verlag LNCS 1838, 385–394, 2000.

8. A.J. Menezes, T. Okamoto and S.A. Vanstone. Reducing elliptic curve logarithms to a finite field. *IEEE Trans. Info. Theory*, **39**, 1639–1646, 1993.

9. V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO 85*. Springer-Verlag, LNCS 218, 417–426, 1986.

10. V. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, **174**, 235–261, 2004.

11. L.J. Mordell. On the rational solutions of the indeterminante equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, **21**, 179–192, 1922.

12. R.L. Rivest, Shamir A. and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, **21**, 120–126, 1978.

13. R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. In *2000 Symposium on Cryptography and Information Security (SCIS2 000)*, 2000.

14. R. Schoof. Elliptic curves over finite fields and the computation of square roots mod *p*. *Math. Comp.*, **44**, 483–494, 1985.

15. A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. Math.*, **142**, 443–551, 1995.

Nigel P. Smart,
Department of Computer Science,
University of Bristol, Bristol,
BS8 1UB
UK

nigel@cs.bris.ac.uk