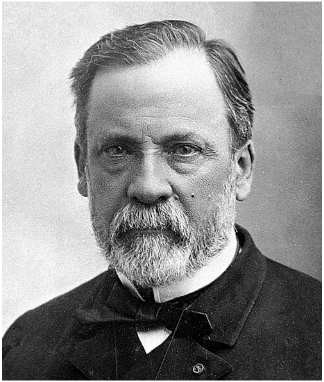
Elliptic Curves and Cryptography: a ~~40~~ 60 year perspective

Victor S. Miller

11 August, 2025

Did I get lucky?



Louis Pasteur

Dans les champs de l'observation le hasard ne favorise que les esprits préparés.

Fortune favors the prepared mind.

Columbia University, 1964-1968

September 1964

- Mathematics IC-IIC-IIC-IVC: "Mathematics for prospective Ph.D's".
- Taught by Serge Lang (who became my advisor) and Lipman Bers.

October 1964

An exercise which pertained to heights on Elliptic Curves (without mentioning them).

It is possible to write endlessly about Elliptic Curves – this is not a threat!

Séminaire BOURBAKI
16e année, 1963/64, n° 274

Mai 1964

Dans les champs de l'observation le hasard ne favorise que les esprits préparés. – Louis Pasteur. Fortune favors the prepared mind.

LES FORMES BILINÉAIRES DE NÉRON ET TATE

par Serge LANG

1. Hauteurs.

2. Formes quasi-linéaires.

Soient G un groupe abélien, et $f : G \to \mathbb{R}$ une fonction réelle. On dit que f est quasi-linéaire si sa "dérivée" $\Delta f(x, y) = f(x+y) - f(x) - f(y)$ est bornée, comme fonction de deux variables x, y. Une fonction de deux variables $\beta(x, y)$ est dite quasi-bilinéaire si la fonction

$$\Delta_1 \beta(x, y, z) = \beta(x+y, z) - \beta(x, z) - \beta(y, z)$$

est bornée sur $G \times G \times G$, ainsi que $\Delta_2 \beta$. Une fonction est dite quasi-quadratique si sa dérivée est quasi-bilinéaire.

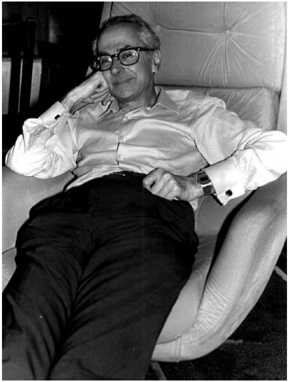
LEMME FONDAMENTAL. – Si f est quasi-linéaire, il existe une seule fonction linéaire équivalente à f. Si f est quasi-quadratique, il existe une fonction quadratique q et une fonction linéaire ℓ (uniquement déterminées) telles que f soit équivalente à $q + \ell$.

Démonstration. – Soit f quasi-quadratique, par exemple. Posons

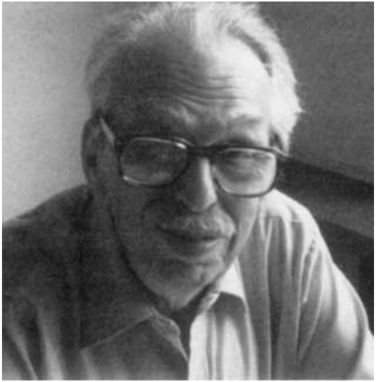
$$\beta(x, y) = f(x+y) - f(x) - f(y) ,$$

et soit

$$B(x, y) = \lim_{m \to \infty} \frac{\beta(2^m x, 2^m y)}{2^{2m}} .$$



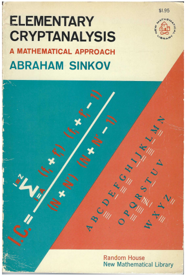
Lipman Bers and Patrick Gallagher

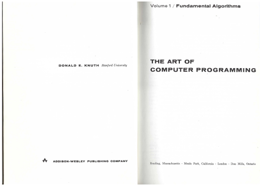


Complex Analysis (and the Weierstrass $\wp$ function).

Analytic Number Theory.

Columbia University Computer Center



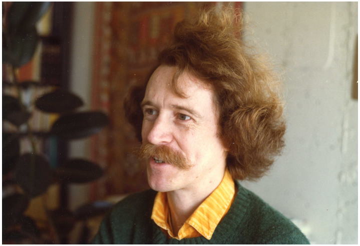


Spent countless hours in the Computer Center teaching myself (there was no Computer Science Department).

Harvard University, 1968-1970

Oscar Zariski: Algebraic Curves

Richard Brauer: Ring Theory.



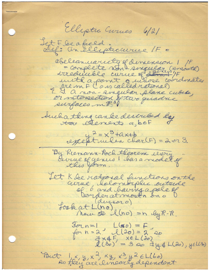
Robin Hartshorne: Schemes.

Lars Ahlfors: Automorphic Forms.

Oxford: Computers in Number Theory 1969

(Sadly, I wasn't there)

Harvard, Summer of 1972



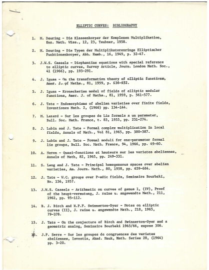
Elliptic Curves 6/21

Let F be a field.
Def: An elliptic curve /F =
abelian variety of dimension 1 /F
= complete non-singular (smooth) irreducible curve of genus 1 /F
with a point o whose coordinates are in F (o is called rational)
E. G. A non-singular plane cubic, or intersection of two quadric surfaces in $\mathbb{P}^3$

Such a thing can be described by two elements $a, b \in F$
$y^2 = x^3 + ax + b$
except when char(F) = 2 or 3.

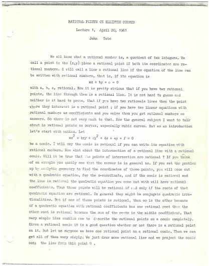
By Riemann-Roch theorem every curve of genus 1 has a model of this form.

Let K be rational functions on the curve, holomorphic outside of o and having a pole of order at most n on o (divisor o)
Look at L(no)
Now $\ell(no) = n$ by R-R.
For n=1 L(o) = F,
for n=2 $\ell(2o) = 2$ so $\exists x \notin F$, $x \in L(2o)$
$\ell(3o) = 3$ so $\exists y \notin L(2o)$, $y \in L(3o)$
But $1, x, y, x^2, xy, x^3, y^2 \in L(6o)$
so they are linearly dependent



ELLIPTIC CURVES: BIBLIOGRAPHY

1. M. Deuring - Die Klassenkorper der Komplexen Multiplikation, Enz. Math. Wiss., 12, 23, Teubner, 1958.
2. M. Deuring - Die Typen der Multiplikatorenringe Elliptischer Funktionenkorper, Abh. Hamb., 16, 1949, p. 32-47.
3. J.W.S. Cassels - Diophantine equations with special reference to elliptic curves, Survey Article, Journ. London Math. Soc., 41 (1966), pp. 193-291.
4. J. Igusa - On the transformation theory of elliptic functions, Amer. J. of Maths., 81, 1959, p. 436-452.
5. J. Igusa - Kroneckerian model of fields of elliptic modular functions, Amer. J. of Maths., 81, 1959, p. 561-577.
6. J. Tate - Endomorphisms of abelian varieties over finite fields, Inventiones Math. 2, (1966) pp. 134-144.
7. M. Lazard - Sur les groupes de Lie formels a un parameter, Bull. Soc. Math. France, t. 83, 1955, pp. 251-274.
8. J. Lubin and J. Tate - Formal complex multiplication in local fields, Annals of Math., Vol 81, 1965, pp. 380-387.
9. J. Lubin and J. Tate - Formal moduli for one-parameter formal lie groups, Bull. Soc. Math. France, 94, 1966, pp. 49-60.
10. A. Neron - Quasi-fonctions et hauteurs sur les varietes abeliennes, Annals of Math, 82, 1965, pp. 249-331.
11. S. Lang and J. Tate - Principal homogeneous spaces over abelian varieties, Am. Journ. Math., 80, 1958, pp. 659-684.
12. J. Tate - W.C. groups over P-adic fields, Seminaire Bourbaki, No. 156, 1957.
13. J.W.S. Cassels - Arithmetic on curves of genus 1, (IV), Proof of the haupt-vermutung, J. reine u. angewandte Math., 211, 1962, pp. 95-112.
14. B. J. Birch and H.P.F. Swinnerton-Dyer - Notes on elliptic curves (II), J. reine u. angewandte Math., 218, 1965, 79-108.
15. J. Tate - On the conjecture of Birch and Swinnerton-Dyer and a geometric analog, Seminaire Bourbaki 1965/66, expose 306.
16. J.P. Serre - Sur les groupes de congruences des varietes abeliennes, Izvestia, Akad. Nauk, Math. Series 28, (1964) pp. 3-20.



RATIONAL POINTS ON ELLIPTIC CURVES

Lecture 1, April 20, 1961

John Tate

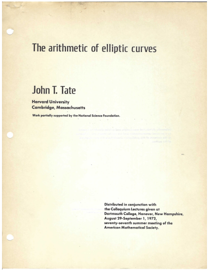
We all know what a rational number is, a quotient of two integers. We call a point in the (x,y) plane a rational point if both its coordinates are rational numbers. I will call a line a rational line if the equation of the line can be written with rational numbers, that is, if its equation is

$$ax + by + c = 0$$

with a, b, c, rational. Now it is pretty obvious that if you have two rational points, the line through them is a rational line. It is not hard to guess and neither is it hard to prove, that if you have two rationals lines then the point where they intersect is a rational point ; if you have two linear equations with rational numbers as coefficients and you solve them you get rational numbers as answers. So there is not very much to that. Now the general subject I want to talk about is rational points on curves, especially cubic curves. But as an introduction let's start with conics. Let

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

be a conic. I will say the conic is rational if you can write its equation with rational numbers. Now what about the intersection of a rational line with a rational conic. Will it be true that the points of intersection are rational ? If you think of an example you easily see that the answer is in general no. If you set the problem up by analytic geometry to find the coordinates of these points, you will come out with a quadratic equation, for the x-coordinate, and if the conic is rational and the line is rational the quadratic equation you come out with will have rational coefficients. Thus these points will be rational if and only if the roots of that quadratic equation are rational. In general they might be conjugate quadratic irrationalities. But if one of these points is rational, then so is the other because if a quadratic equation with rational coefficients has one rational root then the other root is rational because the sum of the roots is the middle coefficient. That very simple idea enables one to describe the rational points on a conic completely. Given a rational conic it is a good question whether or not there is a rational point on it. But let us suppose we have one rational point on a rational conic. Then we can get all of them very simply. We just draw some rational line and we project the conic onto the line from this point 0 .



The arithmetic of elliptic curves

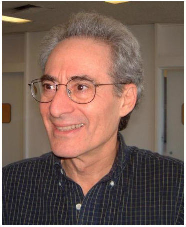
John T. Tate

Harvard University
Cambridge, Massachusetts

Work partially supported by the National Science Foundation.

Distributed in conjunction with the Colloquium Lectures given at Dartmouth College, Hanover, New Hampshire, August 29-September 1, 1972, seventy-seventh summer meeting of the American Mathematical Society.

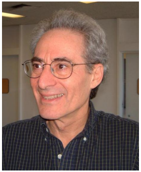
John Tate



Barry Mazur

John Coates

Harvard, 1972-1973



Barry Mazur

John Tate

Bryan Birch

Peter Swinnerton-Dyer

Jean-Pierre Serre

Martin Hellman and Whit Diffie, 1976

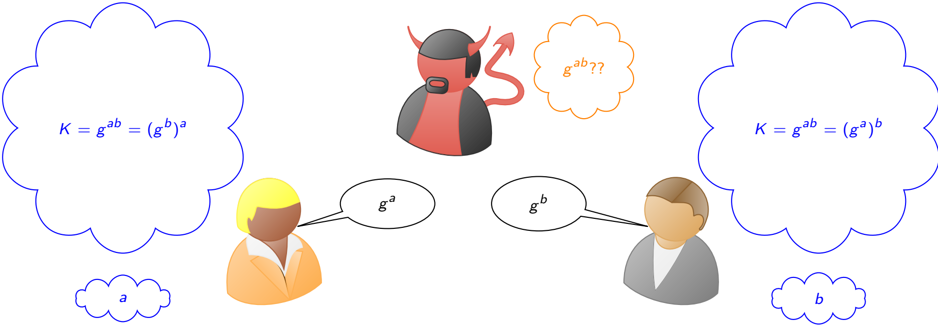
IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Diffie-Hellman key exchange



Fielding Diffie-Hellman

Ron Mullin

Scott Vanstone

Gordon Agnew

Cryptech$\Rightarrow$*Möbius*: Chip for arithemetic in $\mathbb{F}_{2^{127}}$ for use in Diffie-Hellman.

$\Rightarrow$ certicom™ securing innovation

The Inspiration

SIAM J. ALG. DISC. METH.
Vol. 5, No. 2, June 1984

COMPUTING LOGARITHMS IN FINITE FIELDS OF CHARACTERISTIC TWO*

I. F. BLAKE†, R. Fuji-Hara §, R. C. MULLIN‡ AND S. A. VANSTONE‡

Don Coppersmith

EVALUATING LOGARITHMS IN GF(2^n)

Don Coppersmith
IBM Thomas J. Watson Research Center
Yorktown Heights, New York 10598

Computer Algebra, 1983-1984

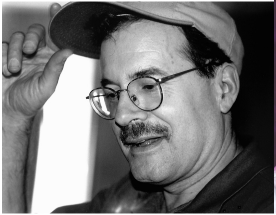
Counting Primes, 1983

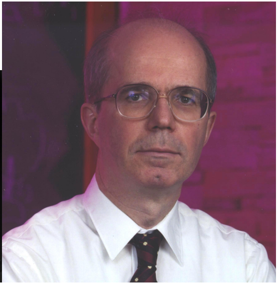
MATHEMATICS OF COMPUTATION
VOLUME 44, NUMBER 170
APRIL 1985, PAGES 537–560

Computing $\pi(x)$: The Meissel-Lehmer Method

By J. C. Lagarias, V. S. Miller and A. M. Odlyzko

Abstract. E. D. F. Meissel, a German astronomer, found in the 1870's a method for computing individual values of $\pi(x)$, the counting function for the number of primes $\leqslant x$. His method was based on recurrences for partial sieving functions, and he used it to compute $\pi(10^9)$. D. H. Lehmer simplified and extended Meissel's method. We present further refinements of the Meissel-Lehmer method which incorporate some new sieving techniques. We give an asymptotic running time analysis of the resulting algorithm, showing that for every $\varepsilon > 0$ it computes $\pi(x)$ using at most $O(x^{2/3+\varepsilon})$ arithmetic operations and using at most $O(x^{1/3+\varepsilon})$ storage locations on a Random Access Machine (RAM) using words of length $[\log_2 x] + 1$ bits. The algorithm can be further speeded up using parallel processors. We show that there is an algorithm which, when given M RAM parallel processors, computes $\pi(x)$ in time at most $O(M^{-1}x^{2/3+\varepsilon})$ using at most $O(x^{1/3+\varepsilon})$ storage locations on each parallel processor, provided $M \leqslant x^{1/3}$. A variant of the algorithm was implemented and used to compute $\pi(4 \times 10^{16})$.





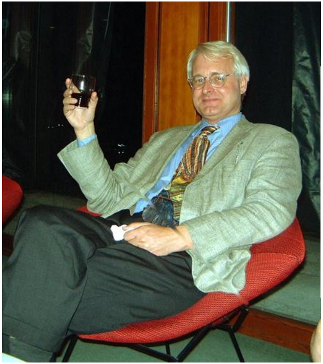
MATHEMATICS OF COMPUTATION
VOLUME 44, NUMBER 170
APRIL 1985, PAGES 483–494

Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p

By René Schoof

Abstract. In this paper we present a deterministic algorithm to compute the number of $\mathbf{F}_q$-points of an elliptic curve that is defined over a finite field $\mathbf{F}_q$ and which is given by a Weierstrass equation. The algorithm takes $O(\log^9 q)$ elementary operations. As an application we give an algorithm to compute square roots mod p. For fixed $x \in \mathbf{Z}$, it takes $O(\log^9 p)$ elementary operations to compute $\sqrt{x}$ mod p.

Hendrik W. Lenstra, Jr.

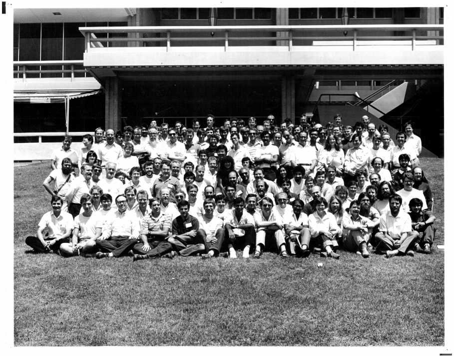


Annals of Mathematics, **126** (1987), 649–673

Factoring integers with elliptic curves

By H. W. Lenstra, Jr.

Crypto 1985



Use of Elliptic Curves in Cryptography

Victor S. Miller

Exploratory Computer Science, IBM Research, P.O. Box 218, Yorktown Heights, NY 10598

ABSTRACT

We discuss the use of elliptic curves in cryptography. In particular, we propose an analogue of the Diffie-Hellmann key exchange protocol which appears to be immune from attacks of the style of Western, Miller, and Adleman. With the current bounds for infeasible attack, it appears to be about 20% faster than the Diffie-Hellmann scheme over GF(p). As computational power grows, this disparity should get rapidly bigger.

If you have chips to do fast arithmetic in a field of characteristic 2, don't throw them away. I have another use for them.

Adleman

McCurley

Vanstone

Short Programs 1986

Manuel Blum

Erich Kaltofen

Short Programs for functions on Curves

Victor S. Miller
Exploratory Computer Science
IBM, Thomas J. Watson Research Center
Yorktown Heights, NY 10598

May 6, 1986

The Weil Pairing, and Its Efficient Calculation

Victor S. Miller
Center for Communications Research,
Princeton, NJ 08540, U.S.A.
victor.miller@idaccr.org

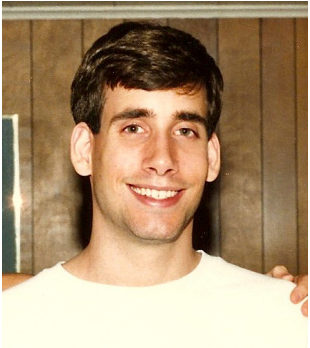
Communicated by Arjen K. Lenstra

Received 4 January 2003 and revised 27 May 2004
Online publication 12 August 2004

Burt Kaliski

Elliptic curves and Cryptography: A Pseudorandom Bit Generator and Other Tools

Burton S. Kaliski, Jr.[1]

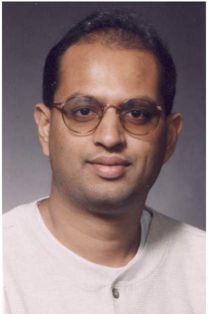


Menezes, Okamoto and Vanstone

Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field

Alfred Menezes & Scott Vanstone
Dept. of Combinatorics and Optimization, University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1.

Tatsuaki Okamoto
NTT Laboratories
Take, Yokosuka-Shi, 238-03 Japan.



Gerhard Frey, Hans-Georg Rück

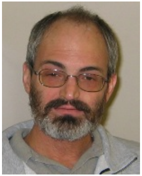
A REMARK CONCERNING m-DIVISIBILITY AND THE DISCRETE LOGARITHM IN THE DIVISOR CLASS GROUP OF CURVES

GERHARD FREY AND HANS-GEORG RÜCK

Pairing Based Cryptography

Antoine Joux

Dan Boneh



Matt Franklin

A One Round Protocol for Tripartite Diffie–Hellman

Antoine Joux

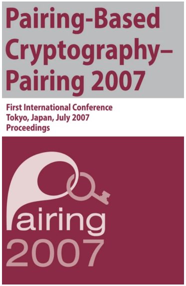
SCSSI, 18, rue du Dr. Zamenhoff
F-92131 Issy-les-Mx Cedex, France
`Antoine.Joux@ens.fr`

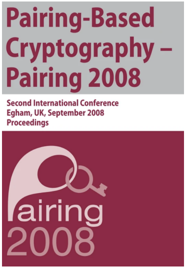
Identity-Based Encryption from the Weil Pairing

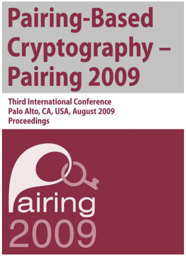
Dan Boneh[1*] and Matt Franklin[2**]

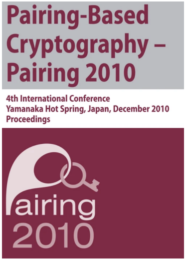
Gödel Prize 2013

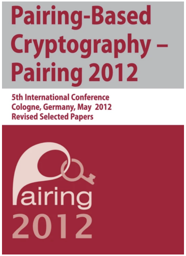
Influence – The Conferences

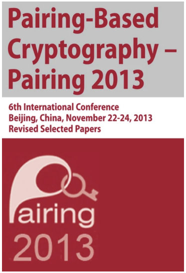












CFAIL

Our Distinguished Failure Awards

At CFAIL 2019, we awarded **Victor Miller** the distinguished **Failure to Publish** award for his foundational work in pairings. This work was initially rejected for publication and long cited by cryptographers as an "unpublished manuscript." It presented the first polynomial-time algorithm for computing pairings on elliptic curves, hence spawning the subfield of "bilinear map" cryptography, an incredibly active and fruitful research area.

Victor Miller (right) graciously accepting his award at CFAIL 2019. Presumably he had just said something very funny.

Will it last?

WIRED

JESSE FREUND CULTURE MAY 5, 1998 6:02 PM

Hype List

Deflating this month's overblown memes.

2. Elliptic Curve Cryptography

Meme on the Rise

Life Expectancy: 12 Months

Watching the wranglings of the cryptography industry has become computing's latest spectator sport. Take elliptic curve cryptography (ECC), a slim public key encryption algorithm designed for low-power devices such as smartcards and cell phones. For years, RSA Data Security discounted ECC developers such as Certicom. But now that RSA is rolling the technology into its line of products, the company bills itself as "ECC Central." Internecine competition aside, ECC may be great for small devices, but few people use encryption for anything other than Web-based transactions.

2005


National Security Agency
Central Security Service
Meet Slate!
Home
About NSA
Research
Business
Careers
Public Info
History
Information Assurance
For Academia
For Industry
For Government
Business Affairs
Education & Training
Programs
Glossary
Links
>>The Case for Elliptic Curve Cryptography
Search
Go
What's new?

Today

TLS 1.3

Only allows *ECDHE* for key establishment

Blockchain

Almost all use some sort of Elliptic Curve based security.
Most ZK proof systems use Elliptic Curves.

Post Quantum

- Isogenies.
- Non-abelian endomorphism rings.

Conclusion

- The study of Elliptic Curves has gone from a beautiful, but arcane, piece of Mathematics to an idea of major impact in Cryptography.
- A good reason to learn hard Number Theory. [1]

[1] Photograph of the Oxford Conference on Computation used by permission of Gillman and Soames. Photograph of Robin Hartshorne used by permission of Archives of the Mathematisches Forschungsinstitut Oberwolfach.


VICTOR