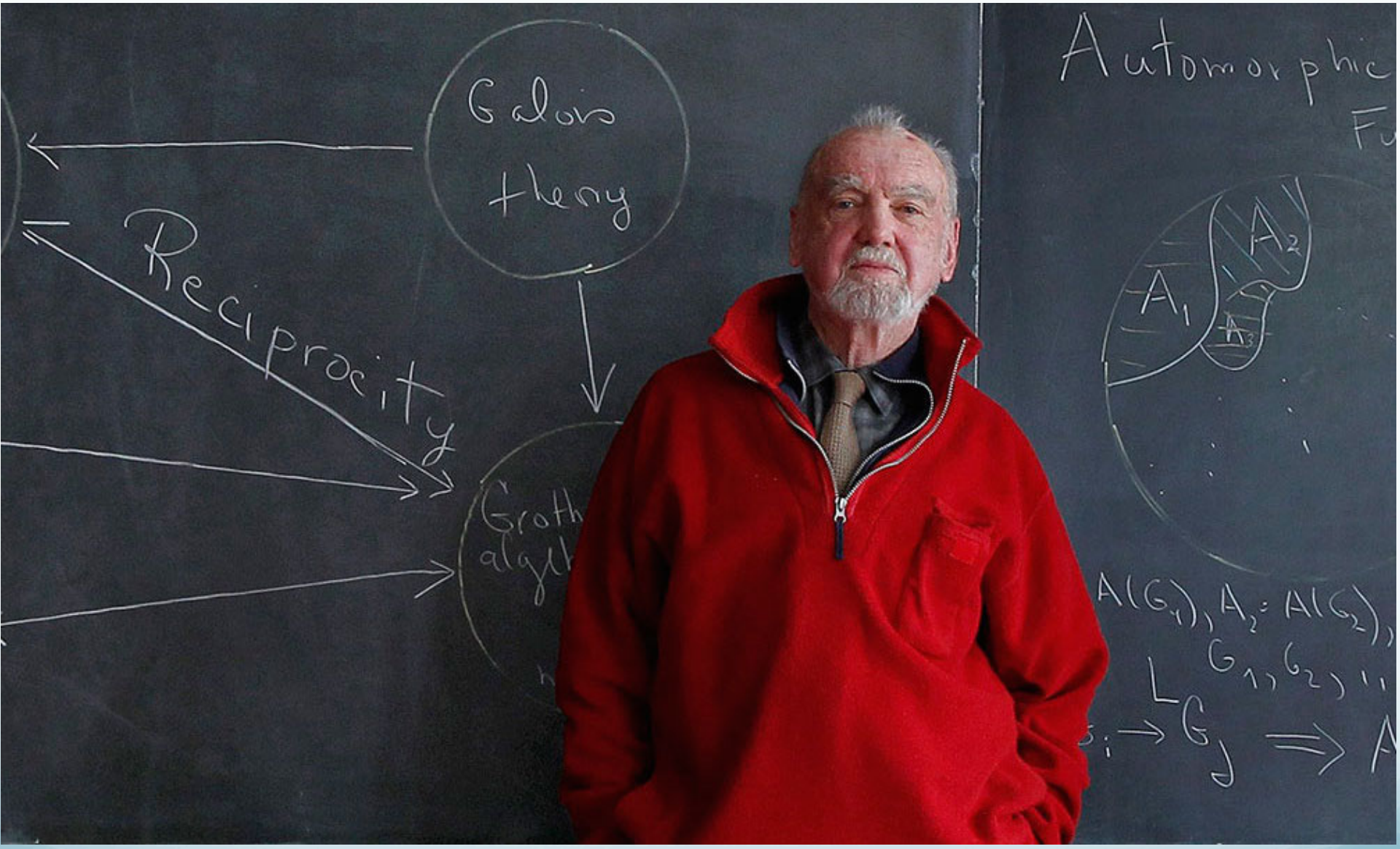
Elementary Introduction to the Langlands Program. III

Edward Frenkel

University of California, Berkeley

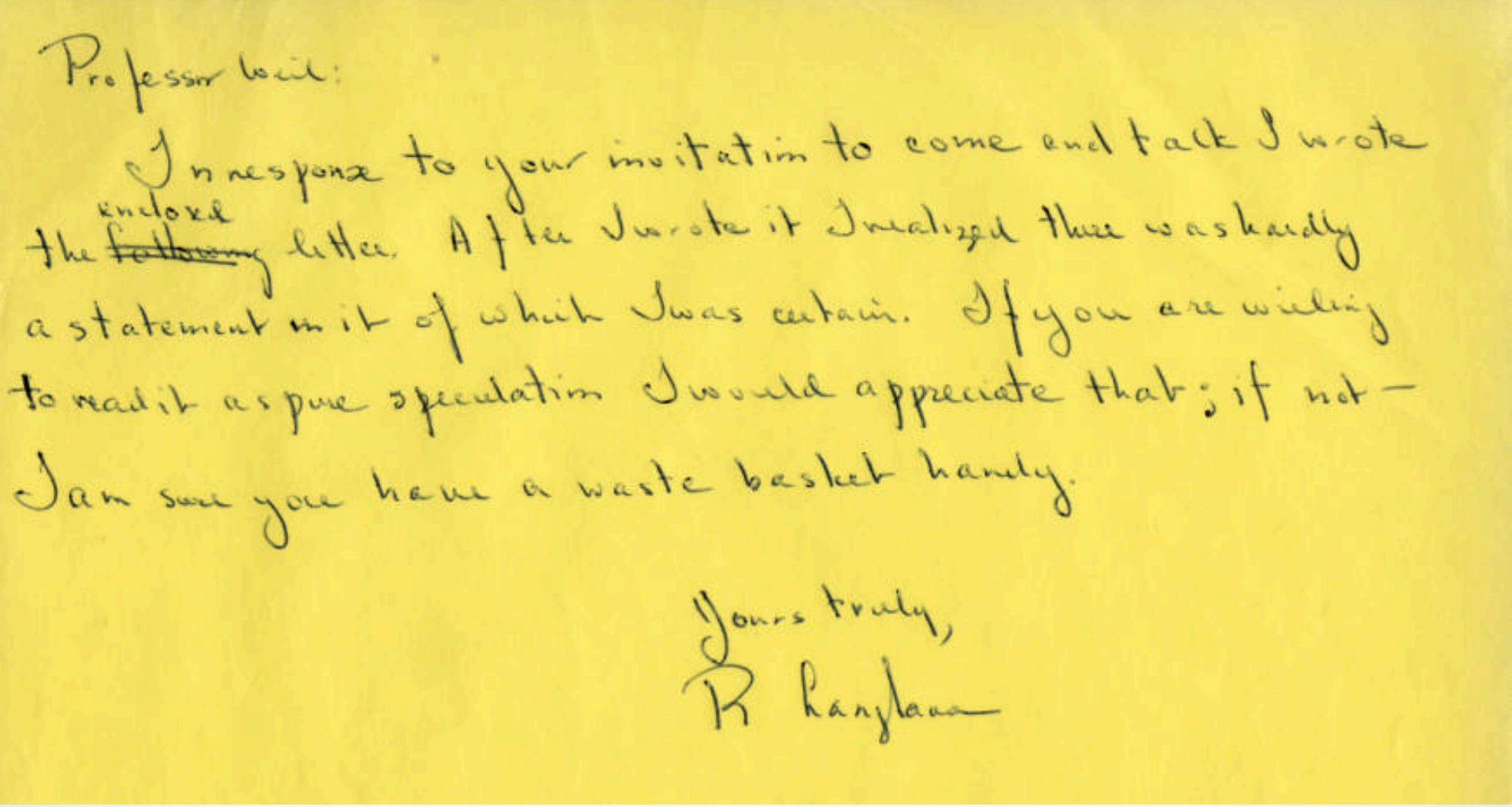


Robert Langlands at his office, 2014 (photo: Toronto Star)

Langlands Program — a bridge between

Number Theory and Harmonic Analysis.

A kind of Grand Unified Theory of Math.



Professor Weil:

In response to your invitation to come and talk I wrote the ~~following~~ enclosed letter. After I wrote it I realized there was hardly a statement in it of which I was certain. If you are willing to read it as pure speculation I would appreciate that; if not — I am sure you have a waste basket handy.

Yours truly,

R Langlands

Cover page of Langlands' letter to Weil, 1967

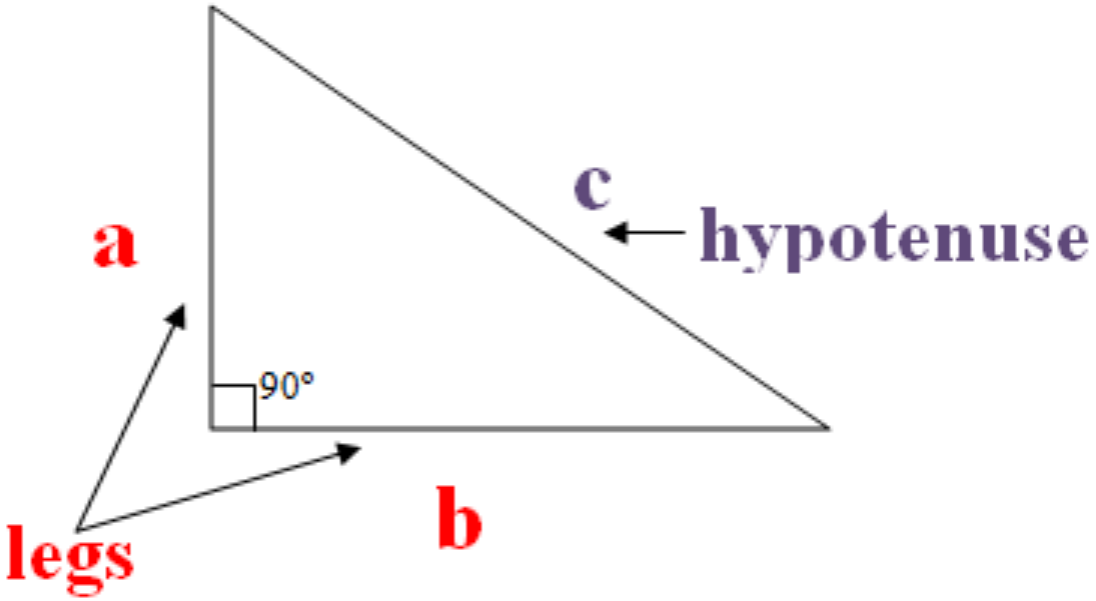
(from the archive of the Institute for Advanced Study)

Fermat's Last Theorem

$$X^n + Y^n = Z^n \qquad n=3,4,5,\ldots$$

has no positive integer solutions X, Y, Z.

Solutions for n=2



$$a^2 + b^2 = c^2$$

Pythagoras triples

- $3^2 + 4^2 = 5^2$
- $5^2 + 12^2 = 13^2$

.....

Pierre de Fermat (1601–1665)

“I have found a truly marvelous proof of this result, which this margin is too narrow to contain”

Edward Frenkel
@edfrenkel

I have found a truly marvelous proof of the Goldbach conjecture but unfortunately I can't fit it in this tweet b/c 140 characters is not eno

RETWEETS 29 FAVORITES 45

Edward Frenkel
@edfrenkel

I have found a truly marvelous proof of the Goldbach conjecture but unfortunately I can't fit it in this tweet b/c 140 characters is not eno

RETWEETS 29 FAVORITES 45

Ignacio Llorente @igll · Sep 19
.@edfrenkel Just send it by SMS!

1

J² @FunkyJdujdu · Sep 19
@edfrenkel Haha just like Fermat ! :D

1

Shimura–Taniyama–Weil Conjecture

- It implies Fermat's Last Theorem (this was proved by the Berkeley mathematician **Ken Ribet** in 1986)

- Shimura–Taniyama–Weil conjecture was proved by **Andrew Wiles** and **Richard Taylor** in 1995

  (in the "stable" case, which is sufficient)

- This completed the proof of Fermat's Last Theorem

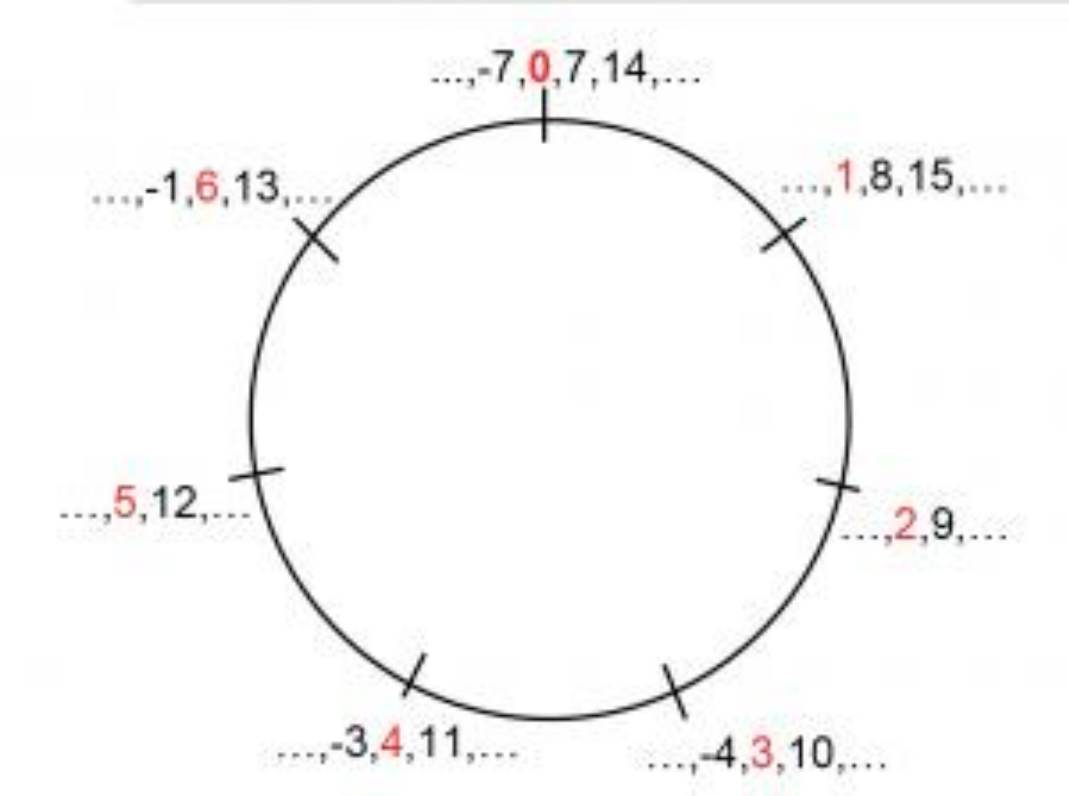
Proof by contradiction

- Suppose that the Fermat's equation has a solution *X*, *Y*, *Z* among positive integers (for some n>2). Then we can construct an "elliptic curve" whose existence is prohibited by the TSW conjecture.

- Therefore, if the T-S-W conjecture is true, such a curve cannot exist, and hence this solution of the Fermat equation cannot exist.

Arithmetic modulo primes

Likewise, we can do arithmetic *modulo* any number; for example, a prime number, such as 2, 3, 5, 7, 11, 13, ...



- Cubic equation, such as

$$y^2 = x^3 - 3x + 5 \quad \text{modulo } p$$

- Look for whole numbers x and y solving this equation

  modulo a prime number p

- Count the number of such solutions (for a given prime p)

Elliptic Curve Cryptography

- A general cubic equation, such as

$$y^2 = x^3 - 3x + 5 \quad \text{modulo } p$$

defines what's called an

Elliptic Curve

- And these are used in **encryption**

theguardian

Series: Glenn Greenwald on security and liberty

Revealed: how US and UK spy agencies defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records
- $250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Security experts say programs 'undermine the fabric of the internet'

RECOMMENDED ELLIPTIC CURVES FOR FEDERAL GOVERNMENT USE

July 1999

This collection of elliptic curves is recommended for Federal government use and contains choices of private key length and underlying fields.

§1. Parameter Choices

1.1 Choice of Key Lengths

The principal parameters for elliptic curve cryptography are the elliptic curve E and a designated point G on E called the *base point*. The base point has order r, a large prime. The number of points on the curve is $n = fr$ for some integer f (the *cofactor*) not divisible by r. For efficiency reasons, it is desirable to take the cofactor to be as small as possible.

NIST Special Publication 800-90A

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Elaine Barker and John Kelsey

Computer Security Division
Information Technology Laboratory

10.3.1 Dual Elliptic Curve Deterministic RBG (Dual_EC_DRBG)

Dual_EC_DRBG is based on the following hard problem, sometimes known as the "elliptic curve discrete logarithm problem" (ECDLP): given points P and Q on an elliptic curve of order n, find a such that $Q = aP$.

Dual_EC_DRBG uses an initial seed that is 2 * *security_strength* bits in length to initiate the generation of *outlen*-bit pseudorandom strings by performing scalar multiplications on two points in an elliptic curve group, where the curve is defined over a field approximately 2^m in size. For all the NIST curves given in this Recommendation, m is at least twice the *security_strength*, and never less than 256. Throughout this DRBG mechanism specification, m will be referred to as *seedlen*; the term "*seedlen*" is appropriate because the internal state of **Dual_EC_DRBG** is used as a "seed" for the random block it produces. Figure 13 depicts the **Dual_EC_DRBG**.

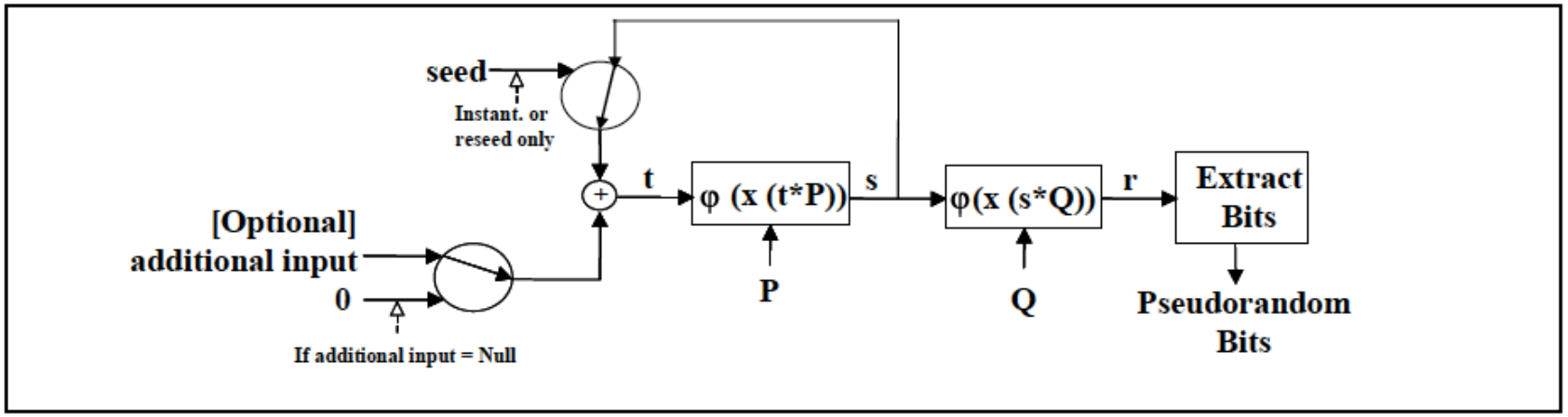


Figure 13: Dual_EC_DRBG

The instantiation of this DRBG mechanism requires the selection of an appropriate elliptic curve and curve points specified in Appendix A.1 for the desired security strength. The

A.1 Constants for the Dual_EC_DRBG

The **Dual_EC_DRBG** requires the specifications of an elliptic curve and two points on the elliptic curve. One of the following NIST **approved** curves with associated points **shall** be used in applications requiring certification under [FIPS 140]. More details about these curves may be found in [FIPS 186]. If alternative points are desired, they **shall** be generated as specified in Appendix A.2.

Each of following curves is given by the equation:

$$y^2 = x^3 - 3x + b \pmod{p}$$

Notation:

- p - Order of the field F_p , given in decimal
- n - Order of the Elliptic Curve Group, in decimal .
- a – (-3) in the above equation
- b - Coefficient above

The x and y coordinates of the base point, i.e., generator G, are the same as for the point P.

A.1.1 Curve P-256

```
p = 115792089210356248762697446949407573530086143\
    415290314195533631308867097853951
```

On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng

Dan Shumow

Niels Ferguson

Microsoft

NIST finally dumps NSA-tainted random number algorithm

TOPICS: Security, Government US

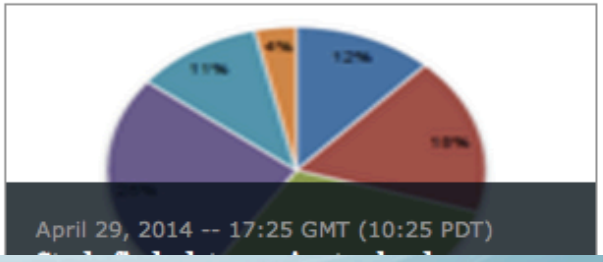
By Larry Seltzer for Zero Day | April 23, 2014 -- 14:04 GMT (07:04 PDT)

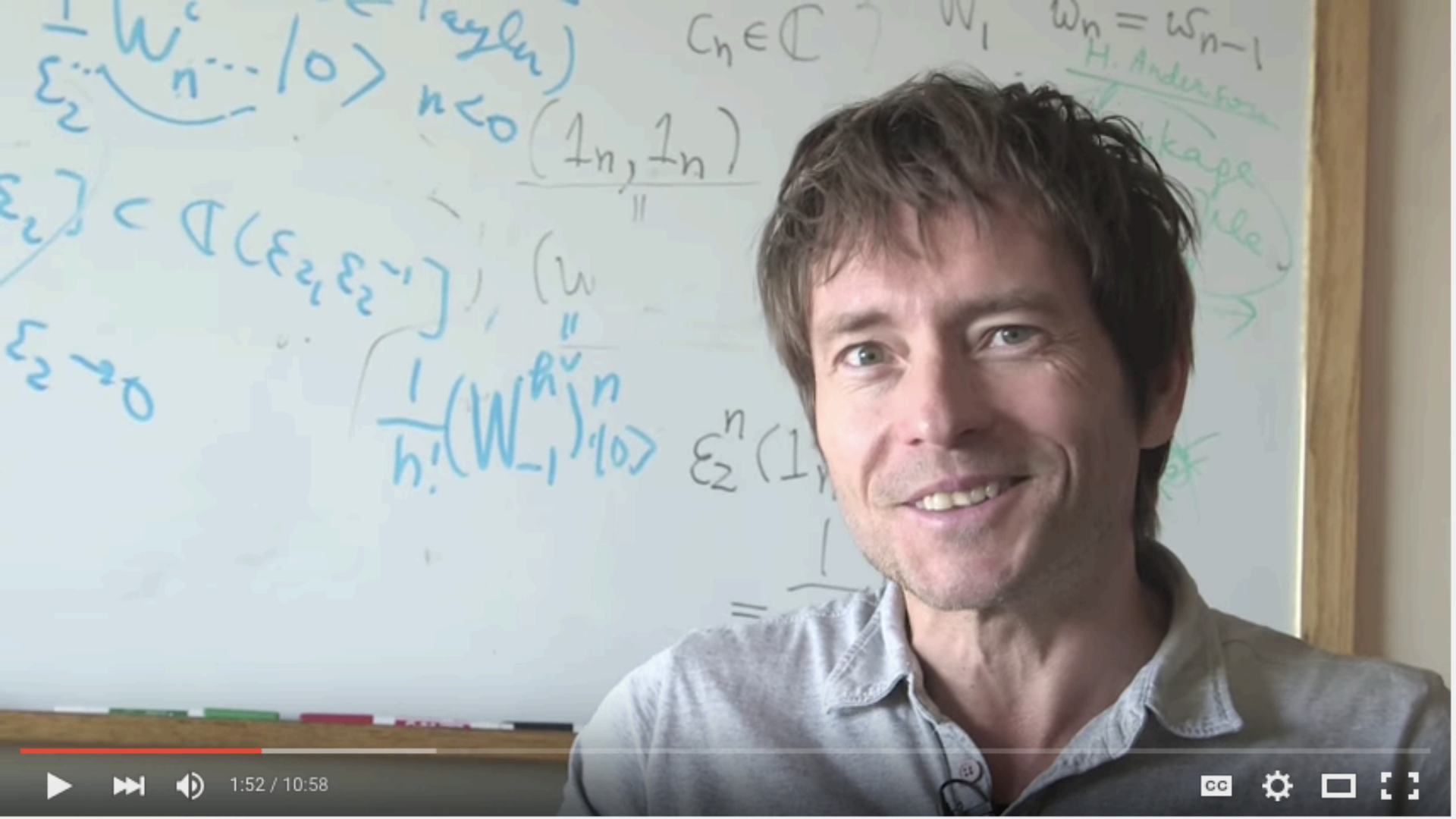
NIST (the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce, has formally removed Dual_EC_DRBG from its draft guidance on random number generators.

This is an odd episode, and the oddness seems to have eluded many observers. The outrage switched on late last year when one of the Snowden leaks indicated that the NSA had intentionally inserted weaknesses into a NIST standard for random number generation, a key component of secure cryptography. Sources told Reuters that RSA Security had entered into $10 million of secret contracts with the NSA, a provision of which was to make the weakened algorithm the default choice in their products. RSA denied the charge.

Why this should have surprised anyone is hard to understand. Problems with Dual_EC_DRBG were first reported almost eight years ago and in 2007 Dan Shumow and Niels Ferguson of Microsoft showed, as Bruce Schneier put it at the time, "...the algorithm contains a weakness that can only be described a backdoor." (Schneier's article in Wired is offline for some reason; click here for the Google cache version.)

Related Articles





How did the NSA hack our emails?

Numberphile

Subscribe 1,376,863

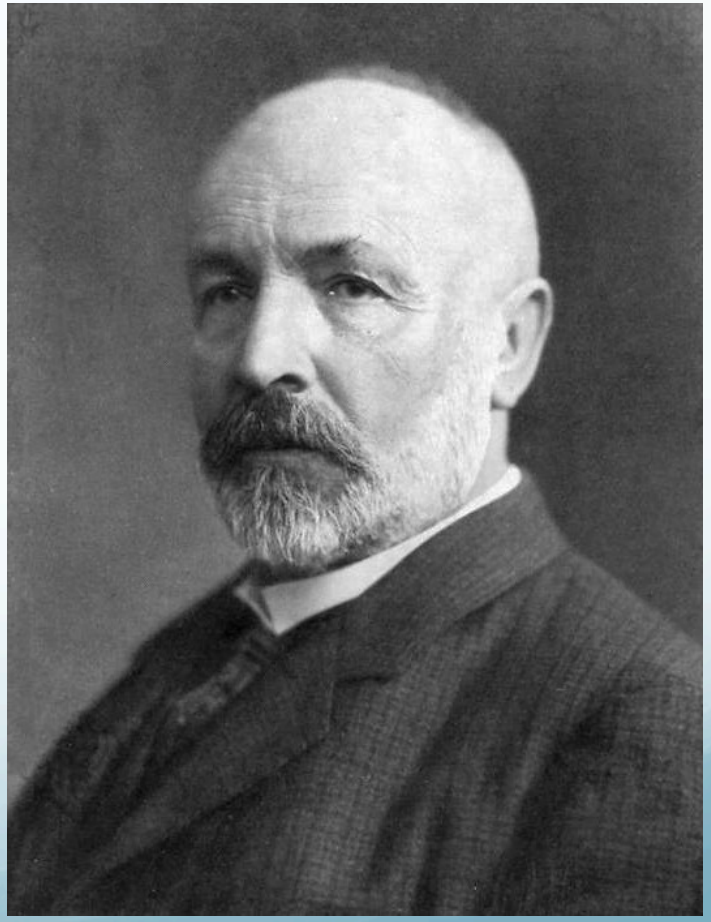
814,972

Add to Share More

11,696 320

“The essence of mathematics lies in its freedom”

—Georg Cantor



Shimura–Taniyama–Weil

- Cubic equation, such as

$$y^2 + y = x^3 - x^2$$

- Look for solutions modulo *every* prime number *p*

- Count the number of solutions for *each* prime *p*

Counting Problem

prime p	number (#) of solutions	$a(p)=p-\#$
2	4	−2
3	4	−1
5	4	1
7	9	−2
11	10	1
13	9	4

Miracle

- These numbers a(p) can be described all at once in the language of **Harmonic Analysis!**
- Namely, they are coefficients in the infinite series

$$q(1-q)^2(1-q^{11})^2(1-q^2)^2(1-q^{22})^2(1-q^3)^2(1-q^{33})^2(1-q^4)^2\ldots$$

$$= q-2q^2-q^3+2q^4+q^5+2q^6-2q^7-2q^9-2q^{10}+q^{11}-2q^{12}+4q^{13}+\ldots$$

Finding order in seeming chaos

- Denote the coefficient in front of the p-th power of q in this series by b(p).

- Then **a(p) = b(p)** for all primes p.

- **Colossal compression of information!** Just one line of code gives us a simple rule generating the "DNA" of the counting problem.

Symmetry in Harmonic Analysis…

- Basic harmonics: sin(nx), cos(nx), n integer
- What do they have in common: they are invariant under shifts

$$x \longrightarrow x + 2\pi$$

- Group of symmetries

$$x \longrightarrow x + 2\pi M, \quad M \text{ arbitrary integer}$$

- Our infinite series actually converges if $|q| < 1$.
- We get a function on the unit disc, which is called a *modular form*; that is, it has special transformation properties under the certain symmetries.

Mathematical Discoveries are the Wonders of the World

Yutaka Taniyama (1927–1958)

Formulated a rough version of the S-T-W conjecture at the International Symposium on Number Theory in Tokyo and Nikko, held in 1955.

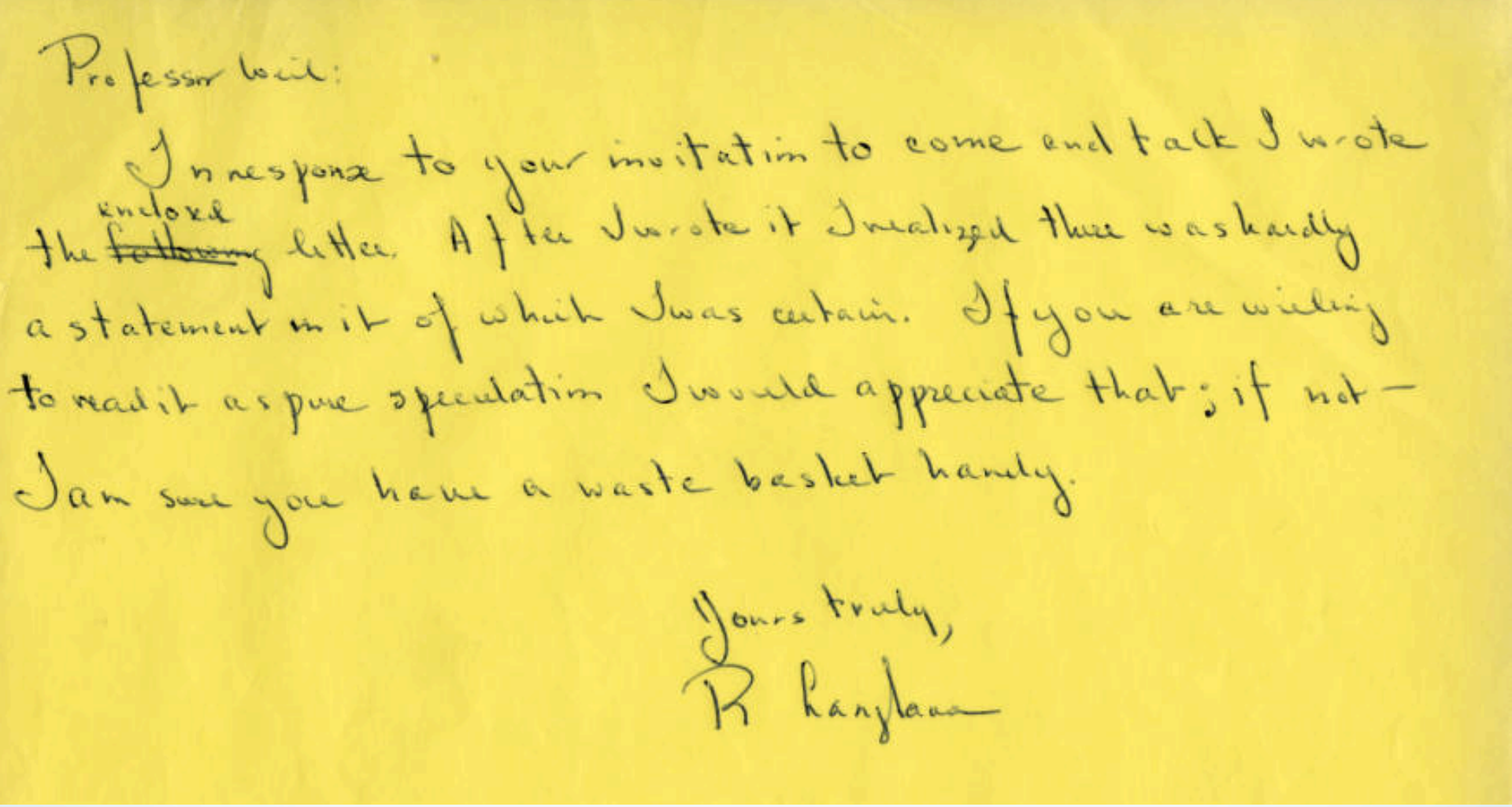
It was further developed by Goro Shimura and André Weil.

Yutaka Taniyama (1927–1958)

"May I say, I am in the frame of mind that I lost confidence in my future... I cannot deny that this is a kind of betrayal, but please excuse it as my last act in my own way, as I have been doing my own way all my life."

Goro Shimura

"I feel his noble generosity ... even more strongly now than when he was alive. And yet nobody was able to give him any support when he desperately needed it. Reflecting on this, I am overwhelmed by the bitterest grief."


Professor Weil:

In response to your invitation to come and talk I wrote the ~~enclosed~~ letter. After I wrote it I realized there was hardly a statement in it of which I was certain. If you are willing to read it as pure speculation I would appreciate that; if not — I am sure you have a waste basket handy.

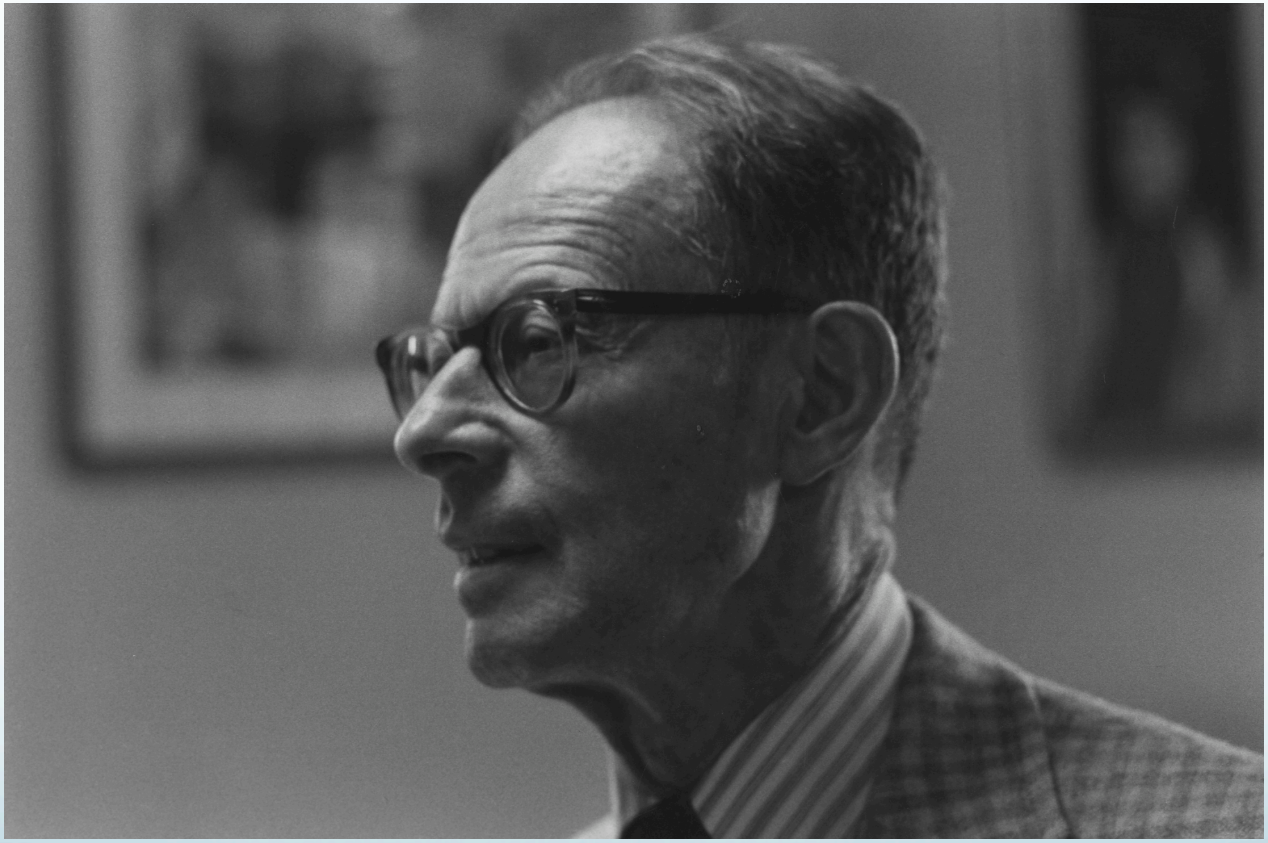
Yours truly,

R Langlands

Cover page of Langlands' letter to **Weil**, 1967

(from the archive of the Institute for Advanced Study)

André Weil (1906–1998)



Tokyo–Nikko symposium, 1955

Next in line...

- Quantum Physics
- Symmetry and the fundamental blocks of nature
- Electromagnetic duality and the Langlands Program