L-FUNCTIONS AND CRYPTOGRPHY

Jerzy Kaczorowski

Adam Mickiewicz University, Poznań, Poland
and
Mathematical Institute of the Polish Academy of Sciences, Warsaw, Poland

June, 2010

Cryptography and Number Theory

Cryptography and Number Theory

Cryptography:

Cryptography and Number Theory

Cryptography:

Algorithms, protocols.

Cryptography and Number Theory

Cryptography:

Algorithms, protocols.

Number Theory:

Cryptography and Number Theory

Cryptography:

Algorithms, protocols.

Number Theory:

Seemingly intractable arithmetic problems.

Cryptography and Number Theory

Cryptography:

Algorithms, protocols.

Number Theory:

Seemingly intractable arithmetic problems:

★ integer factorization

Cryptography and Number Theory

Cryptography:

Algorithms, protocols.

Number Theory:

Seemingly intractable arithmetic problems:

★ integer factorization,

★ discrete logarithms in algebraic groups

Cryptography and Number Theory

Cryptography:

Algorithms, protocols.

Number Theory:

Seemingly intractable arithmetic problems:

★ integer factorization,

★ discrete logarithms in algebraic groups,

★ L-function recognition.

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Definition: Dirichlet charcter $(\mathrm{mod}\, q)$:

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Definition: Dirichlet charcter $(\mathrm{mod}\, q)$:

a function $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Definition: Dirichlet charcter $(\mathrm{mod}\, q)$:

a function $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying

- $\chi(n) = 0$ iff $(n, q) > 1$,

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Definition: Dirichlet charcter $(\mathrm{mod}\, q)$:

a function $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying

- $\chi(n) = 0$ iff $(n, q) > 1$,
- $\chi(n + q) = \chi(n)$,

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Definition: Dirichlet charcter $(\mathrm{mod}\, q)$:

a function $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying

- $\chi(n) = 0$ iff $(n, q) > 1$,
- $\chi(n + q) = \chi(n)$,
- $\chi(nm) = \chi(n)\chi(m)$.

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Autentication's layout:

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Autentication's layout:

Alice: the user,

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Authentication's layout:

Alice: the user,

Bob: the authenticator.

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Authentication's layout:

Alice: the user,

Bob: the authenticator.

Both are in possession of a (secret) Dirichlet character $\chi(\mathrm{mod}\, q)$.

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Authentication's layout:

Alice: the user,

Bob: the authenticator.

Both are in possession of a (secret) Dirichlet character $\chi(\mathrm{mod}\, q)$.

Authentication scheme:

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Authentication's layout:

Alice: the user,

Bob: the authenticator.

Both are in possession of a (secret) Dirichlet character $\chi(\mathrm{mod}\, q)$.

Authentication scheme:

Bob sends to Alice: randomly chosen integers m and $b > 0$,

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Authentication's layout:

Alice: the user,

Bob: the authenticator.

Both are in possession of a (secret) Dirichlet character $\chi(\mathrm{mod}\, q)$.

Authentication scheme:

Bob sends to Alice: randomly chosen integers m and $b > 0$,

Alice sends to Bob: vector $v = (\chi(m), \chi(m+1), \ldots, \chi(m+b))$,

EXAMPLE 1: authentication using Dirichlet characters (cf. [1]).

Authentication's layout:

Alice: the user,

Bob: the authenticator.

Both are in possession of a (secret) Dirichlet character $\chi(\mathrm{mod}\, q)$.

Authentication scheme:

Bob sends to Alice: randomly chosen integers m and $b > 0$,

Alice sends to Bob: vector $v = (\chi(m), \chi(m+1), \ldots, \chi(m+b))$,

Bob: If Alice's list is correct $\rightarrow$ Alice is an authenticated user.

Why does if work?

CONJECTURE (Anshel-Goldfeld [1]) *For* $\chi = \left(\frac{d}{\cdot}\right)$ *(the Kronecker symbol) the associated projection*

$$[X, 2X] \ni d \mapsto \left(\left(\frac{d}{n}\right), \left(\frac{d}{n+1}\right), \ldots, \left(\frac{d}{n+b}\right)\right)$$

where

$$b \geq (\log X)^A \quad , \quad m \leq (\log X)^B$$

is a one-way function.

Why does if work?

CONJECTURE (Anshel-Goldfeld [1]) *For* $\chi = \left(\frac{d}{\cdot}\right)$ *(the Kronecker symbol) the associated projection*

$$[X, 2X] \ni d \mapsto \left(\left(\frac{d}{n}\right), \left(\frac{d}{n+1}\right), \ldots, \left(\frac{d}{n+b}\right)\right)$$

where

$$b \geq (\log X)^A \quad , \quad m \leq (\log X)^B$$

is a one-way function.

IMPORTANT: ranges of the parameters b and m.

GENERALIZATION:

GENERALIZATION:

Both Alice and Bob are in possession of a (secret) L-function ($\Re(s) > 1$):

GENERALIZATION:

Both Alice and Bob are in possession of a (secret) L-function ($\Re(s) > 1$):

$$L(s) = \sum_{n=1}^{\infty} \frac{a_L(n)}{n^s}.$$

GENERALIZATION:

Both Alice and Bob are in possession of a (secret) L-function ($\Re(s) > 1$):

$$L(s) = \sum_{n=1}^{\infty} \frac{a_L(n)}{n^s}.$$

Authentication scheme:

GENERALIZATION:

Both Alice and Bob are in possession of a (secret) L-function ($\Re(s) > 1$):

$$L(s) = \sum_{n=1}^{\infty} \frac{a_L(n)}{n^s}.$$

Authentication scheme:

Bob sends to Alice: randomly chosen positive integers m and b,

GENERALIZATION:

Both Alice and Bob are in possession of a (secret) L-function ($\Re(s) > 1$):

$$L(s) = \sum_{n=1}^{\infty} \frac{a_L(n)}{n^s}.$$

Authentication scheme:

Bob sends to Alice: randomly chosen positive integers m and b,

Alice sends to Bob: vector $v = (a_L(m), a_L(m+1), \ldots, a_L(m+b))$,

GENERALIZATION:

Both Alice and Bob are in possession of a (secret) L-function ($\Re(s) > 1$):

$$L(s) = \sum_{n=1}^{\infty} \frac{a_L(n)}{n^s}.$$

Authentication scheme:

Bob sends to Alice: randomly chosen positive integers m and b,

Alice sends to Bob: vector $v = (a_L(m), a_L(m+1), \ldots, a_L(m+b))$,

Bob: If Alice's list is correct $\rightarrow$ Alice is an authenticated user.

GENERALIZATION:

Both Alice and Bob are in possession of a (secret) L-function ($\Re(s) > 1$):

$$L(s) = \sum_{n=1}^{\infty} \frac{a_L(n)}{n^s}.$$

Authentication scheme:

Bob sends to Alice: randomly chosen positive integers m and b,

Alice sends to Bob: vector $v = (a_L(m), a_L(m+1), \ldots, a_L(m+b))$,

Bob: If Alice's list is correct $\rightarrow$ Alice is an authenticated user.

Previous example: $L(s) = L(s, \chi)$ Dirichlet L-function of χ:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \qquad (\Re(s) > 1).$$

What is an L-function?

What is an L-function?

"We know one when we see one."

What is an L-function?

"We know one when we see one."

Dirichlet series, Euler product, functional equation...

What is an L-function?

"We know one when we see one."

Dirichlet series, Euler product, functional equation...

Do we know all interesting L-functions?

What is an L-function?

"We know one when we see one."

Dirichlet series, Euler product, functional equation...

Do we know all interesting L-functions?

We don't know.

What is an L-function?

"We know one when we see one."

Dirichlet series, Euler product, functional equation...

Do we know all interesting L-functions?

We don't know.

Automorphic L-functions?

Definition of S (Selberg, 1989, (cf. [3]))

$F \in S$ (the Selberg class) if $F(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ where

1. the Dirichlet series converges absolutely for $\sigma > 1$.
2. (*Analytic continuation*) There exists an integer $m \geq 0$ such that $(s-1)^m F(s)$ is entire of finite order.
3. (*Functional equation*)

$$\Phi(s) = \omega \overline{\Phi(1-\overline{s})},$$

where

$\Phi(s) = Q^s \prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) F(s) = \gamma(s) F(s)$, and $r \geq 0$, $Q > 0$, $\lambda_j > 0$, $\Re \mu_j \geq 0$, $|\omega| = 1$.

Definition of S, continuation

4. (*Ramanujan hypothesis*) For every $\varepsilon > 0$ we have $a(n) \ll n^{\varepsilon}$.
5. (*Euler product*) For $\sigma > 1$ we have

$$\log F(s) = \sum_{n} b(n) n^{-s},$$

where $b(n) = 0$ unless $n = p^m$ and $b(n) \ll n^{\theta}$ for some $\theta < 1/2$.

1. Remark: $r = 0$ is possible — the functional equation takes form

$$Q^s F(s) = \omega Q^{1-s} \overline{F}(1-s).$$

2. The *extended Selberg class* $S^{\#}$ consists of $F(s)$ not identically zero satisfying axioms (1), (2) and (3).
3. $\gamma(s) = Q^s \prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j)$ — the *gamma factor* of $F \in S^{\sharp}$.

EXAMPLES

1. The Riemann zeta function $\zeta(s)$

EXAMPLES

1. The Riemann zeta function $\zeta(s)$
2. Shifted Dirichlet L-functions $L(s+i\theta,\chi)$, where χ is a primitive Dirichlet character $(\mathrm{mod}\, q)$, $q>1$, and θ is a real number

EXAMPLES

1. The Riemann zeta function $\zeta(s)$
2. Shifted Dirichlet L-functions $L(s+i\theta,\chi)$, where χ is a primitive Dirichlet character $(\mathrm{mod}\, q)$, $q>1$, and θ is a real number
3. $\zeta_K(s)$, Dedekind zeta function of an algebraic number field K

EXAMPLES

1. The Riemann zeta function $\zeta(s)$
2. Shifted Dirichlet L-functions $L(s+i\theta,\chi)$, where χ is a primitive Dirichlet character $(\mathrm{mod}\, q)$, $q>1$, and θ is a real number
3. $\zeta_K(s)$, Dedekind zeta function of an algebraic number field K
4. $L_K(s,\chi)$, Hecke L-function to a primitive Hecke character $\chi(\mathrm{mod}\mathfrak{f})$, $\mathfrak{f}$ is an ideal of the ring of integers of K

EXAMPLES, continuation

5. L-function associated with a holomorphic newform of a congruence subgroup of $SL_2(\mathbb{Z})$ (after suitable normalization)
6. L-functions of elliptic curves (Wiles)
7. Rankin-Selberg convolution of any two normalized holomorphic newforms.
8. $F, G \in S$ implies $FG \in S$ (the same for $S^{\#}$)
9. If $F \in S$ is entire then the *shift* $F_\theta(s) = F(s + i\theta)$ is in S for every real θ

Conditional examples

1. Artin L-functions for irreducible representations of Galois groups (modulo Artin's conjecture: holomorphy is missing).
2. L-functions associated with nonholomorphic newforms (Ramanujan hypothesis is missing, exceptional eigenvalue problem).

Conditional examples, continuation

3. Symmetric powers (for normalized holomorphic newforms, say):

$$L(s) = \prod_p \left(1 - \frac{a_p}{p^s}\right)^{-1} \left(1 - \frac{b_p}{p^s}\right)^{-1}$$

r-th symmetric power:

$$L_r(s) = \prod_p \prod_{j=0}^{r} (1 - a_p^j b_p^{r-j} p^{-s})^{-1}$$

(modulo Langlands functoriality conjecture).

4. In general: $GL_n(K)$ automorphic L functions (Ramanujan hypothesis is missing).
5. Motivic L-functions (analytic continuation is missing).

Examples, continuation

General examples of L-functions from the extended Selberg class: linear combinations of solutions of the same functional equation as for instance the Davenport-Heilbronn L-function.

$L(s) = \overline{\lambda} L(s, \chi_1) + \lambda L(s, \overline{\chi}_1)$,

$\chi_1 (\mathrm{mod} 5)$ such that $\chi_1(2) = i$,

$\lambda = \frac{1}{2}\left(1 + i\frac{\sqrt{10-2\sqrt{5}}-2}{\sqrt{5}-1}\right)$.

Functional equation

$$\left(\frac{\pi}{5}\right)^{\frac{s}{2}} \Gamma\left(\frac{s+1}{2}\right) L(s) = \left(\frac{\pi}{5}\right)^{\frac{1-s}{2}} \Gamma\left(\frac{2-s}{2}\right) L(1-s).$$

The basic problem of the Selberg class theory

Let $L \in S$ satisfy the following functional equation

$$\Phi(s) = \omega\overline{\Phi(1-\overline{s})},$$

where

$\Phi(s) = Q^s \prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) F(s) = \gamma(s) F(s)$, and
$r \geq 0,\ Q > 0,\ \lambda_j > 0,\ \Re\mu_j \geq 0,\ |\omega| = 1.$

The basic problem of the Selberg class theory

Let $L \in S$ satisfy the following functional equation

$$\Phi(s) = \omega\overline{\Phi(1-\overline{s})},$$

where

$\Phi(s) = Q^s \prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) F(s) = \gamma(s) F(s)$, and
$r \geq 0,\ Q > 0,\ \lambda_j > 0,\ \Re\mu_j \geq 0,\ |\omega| = 1.$

Degree of L: $d_L = 2\sum_{j=1}^{r} \lambda_j$

The basic problem of the Selberg class theory

General Converse Conjecture

The basic problem of the Selberg class theory

General Converse Conjecture

(1) (Degree conjecture) $d_L \in \mathbb{Z}$ for all $L \in S$;

The basic problem of the Selberg class theory

General Converse Conjecture

(1) (Degree conjecture) $d_L \in \mathbb{Z}$ for all $L \in S$;

(2) All L of integer degree are suitably normalized L-functions of automorphic representations.

The basic problem of the Selberg class theory

General Converse Conjecture

(1) (Degree conjecture) $d_L \in \mathbb{Z}$ for all $L \in S$;

(2) All L of integer degree are suitably normalized L-functions of automorphic representations.

THEOREM ([4]) *GCC is true for* $0 \leq d < 2$.

Further cryptographic applications of L-functions

EXAMPLE 2: Elliptic curve PRG, (cf. [1])

DEFINITION: PRG is a deterministic polynomial time algorithm that expands short seeds into longer bit sequences such that the output of the ensemble is polynomial-time indistinguishable from a target probability distribution.

Further cryptographic applications of L-functions

EXAMPLE 2: Elliptic curve PRG (cf. [1])

Elliptic curves over $\mathbb{Q}$

$$a, b \in \mathbb{Z},\ \Delta_E := 4a^3 + 27b^2 \neq 0$$

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} : y^2 = x^3 + ax + b\} \cup \{(\infty, \infty)\}$$

Further cryptographic applications of L-functions

EXAMPLE 2: Elliptic curve PRG (cf. [1])

Elliptic curves over $\mathbb{Q}$

$$a, b \in \mathbb{Z},\ \Delta_E := 4a^3 + 27b^2 \neq 0$$

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} : y^2 = x^3 + ax + b\} \cup \{(\infty, \infty)\}$$

Good reduction: For $p \not| \Delta_E$

$$y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p)$$

defines an elliptic curve over $\mathbb{F}_p$.

For $p \not| \Delta_E$:

$$a_E(p) = p + 1 - \#E(\mathbb{F}_p).$$

THEOREM (A. Wiles et al. + multiplicity one property of automorphic representations) *There exist uniquely determined integers $a_E(p)$, $p|\Delta_E$ such that*

$$L(s,E) = \prod_{p|\Delta_E}\left(1-\frac{a_E(p)}{p^s}\right)^{-1}\prod_{p\nmid\Delta_E}\left(1-\frac{a_E(p)}{p^s}+p^{1-2s}\right)^{-1}$$

defined for $\Re(s) > 3/2$ extends to an entire function satisfying the following functional equation:

$$Q^s\Gamma(s)L(s,E) = \omega Q^{2-s}\Gamma(2-s)L(2-s,E)$$

with $\omega = \pm 1$.

COROLLARY *We have*

1. $$L(s,E)=\sum_{n=1}^{\infty}\frac{a_E(n)}{n^s} \qquad (\Re(s)>3/2),$$
2. $a_E(n)\in\mathbb{Z}$,
3. $|a_E(n)|\leq\sqrt{n}d(n)$ *(Deligne)*,
4. $a_E(p^k)$ *can be computed in a polynomial time (Schoof)*,
5. $L(s+\frac{1}{2},E)\in S$.

THEOREM ([1]) *Let $a, b \in \mathbb{Z}$ be such that $4a^3 + 27b^2 \neq 0$, and let the splitting field of the polynomial*

$$X^3 + aX + b \in \mathbb{Q}[X]$$

has degree 6 over $\mathbb{Q}$. Then the density of primes p for which $a_E(p)$ is even is $2/3$:

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{\substack{p\leq x \\ 2|a_E(p)}} 1 = \frac{2}{3}.$$

THEOREM ([1]) *Let $a, b \in \mathbb{Z}$ be such that $4a^3 + 27b^2 \neq 0$, and let the splitting field of the polynomial*

$$X^3 + aX + b \in \mathbb{Q}[X]$$

has degree 6 over $\mathbb{Q}$. Then the density of primes p for which $a_E(p)$ is even is $2/3$:

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{\substack{p\leq x \\ 2|a_E(p)}} 1 = \frac{2}{3}.$$

PROOF: Artin's conjecture for S_3 and Chebotarev density theorem.

Elliptic Curve Pseudorandom Generator ([1])

Elliptic Curve Pseudorandom Generator ([1])

INPUT: $a, b \in \mathbb{Z}$ such that

1. $4a^3 + 27b^2 \neq 0$,
2. the degree of the splitting field of $X^3 + aX + b$ is of degree 6 over $\mathbb{Q}$.

Elliptic Curve Pseudorandom Generator ([1])

INPUT: $a, b \in \mathbb{Z}$ such that

1. $4a^3 + 27b^2 \neq 0$,
2. the degree of the splitting field of $X^3 + aX + b$ is of degree 6 over $\mathbb{Q}$.

Integer pair (a, b) is the SEED of the PRG.

Elliptic Curve Pseudorandom Generator ([1])

INPUT: $a, b \in \mathbb{Z}$ such that

1. $4a^3 + 27b^2 \neq 0$,
2. the degree of the splitting field of $X^3 + aX + b$ is of degree 6 over $\mathbb{Q}$.

Integer pair (a, b) is the SEED of the PRG.

OUTPUT: The binary string

$$(a_E(p_1)(\mathrm{mod}2), a_E(p_2)(\mathrm{mod}2), \ldots)$$

where $3 = p_1 < p_2 < \ldots$ is the sequence of odd primes.

Elliptic Curve Pseudorandom Generator ([1])

INPUT: $a, b \in \mathbb{Z}$ such that

1. $4a^3 + 27b^2 \neq 0$,
2. the degree of the splitting field of $X^3 + aX + b$ is of degree 6 over $\mathbb{Q}$.

Integer pair (a, b) is the SEED of the PRG.

OUTPUT: The binary string

$$(a_E(p_1)(\mathrm{mod}2), a_E(p_2)(\mathrm{mod}2), \ldots)$$

where $3 = p_1 < p_2 < \ldots$ is the sequence of odd primes.

FACT: ([1]) *This is a pseudorandom sequence with probability distribution* $(1/3, 2/3)$.

GENERALIZATION: Apply the same procedure to any L-function.

EXAMPLE 3: Coin flipping by telephone

Preparations:

EXAMPLE 3: Coin flipping by telephone

Preparations:

Step I: Alice chooses:

EXAMPLE 3: Coin flipping by telephone

Preparations:

Step I: Alice chooses:

(a) an L-function of conductor q,

EXAMPLE 3: Coin flipping by telephone

Preparations:

Step I: Alice chooses:

(a) an L-function of conductor q,

(b) parameters $T, x \in \mathbb{R}$, $N \in \mathbb{N}$ ($N \sim T^{\theta}, \theta > 1/2$),

EXAMPLE 3: Coin flipping by telephone

Preparations:

Step I: Alice chooses:

(a) an L-function of conductor q,

(b) parameters $T, x \in \mathbb{R}$, $N \in \mathbb{N}$ ($N \sim T^{\theta}, \theta > 1/2$),

(c) $E \subset [0,1)$ of Jordan measure $1/2$.

EXAMPLE 3: Coin flipping by telephone

Preparations:

Step I: Alice chooses:

(a) an L-function of conductor q,

(b) parameters $T, x \in \mathbb{R}$, $N \in \mathbb{N}$ ($N \sim T^{\theta}, \theta > 1/2$),

(c) $E \subset [0,1)$ of Jordan measure $1/2$.

Step II: Alice computes consecutive non-trivial zeros $\rho_1, \rho_2, \ldots, \rho_N$ of $L(s)$ on the line $\sigma = 1/2$:

$$\rho_j = \frac{1}{2} + i\gamma_j$$

$$T \leq \gamma_1 \leq \gamma_2 \leq \ldots \leq \gamma_N.$$

EXAMPLE 3: Coin flipping by telephone

Preparations:

Step I: Alice chooses:

(a) an L-function of conductor q,

(b) parameters $T, x \in \mathbb{R}$, $N \in \mathbb{N}$ ($N \sim T^{\theta}, \theta > 1/2$),

(c) $E \subset [0,1)$ of Jordan measure $1/2$.

Step II: Alice computes consecutive non-trivial zeros $\rho_1, \rho_2, \ldots, \rho_N$ of $L(s)$ on the line $\sigma = 1/2$:

$$\rho_j = \frac{1}{2} + i\gamma_j$$

$$T \leq \gamma_1 \leq \gamma_2 \leq \ldots \leq \gamma_N.$$

Step III: Alice sends to Bob N and the vector

$$v = (a_L(2), a_L(3), \ldots, a_L(m))$$

$$m \sim [(\log q)^{\kappa}] \quad , \quad \kappa > 2.$$

EXAMPLE 3: Coin flipping by telephone

The Algorithm

EXAMPLE 3: Coin flipping by telephone

The Algorithm

Bob: sends to Alice a random integer $1 \leq m \leq N$.

EXAMPLE 3: Coin flipping by telephone

The Algorithm

Bob: sends to Alice a random integer $1 \leq m \leq N$.

Alice: Returns $\varepsilon_m \in \{0, 1\}$ computed as follows:

$$\varepsilon_m = \begin{cases} 1 & \text{if} \quad ||x\gamma_m|| \in E, \\ 0 & \text{othervise.} \end{cases}$$

EXAMPLE 3: Coin flipping by telephone

The Algorithm

Bob: sends to Alice a random integer $1 \leq m \leq N$.

Alice: Returns $\varepsilon_m \in \{0, 1\}$ computed as follows:

$$\varepsilon_m = \begin{cases} 1 & \text{if} \quad ||x\gamma_m|| \in E, \\ 0 & \text{othervise.} \end{cases}$$

If $\varepsilon_m = 1$ the coin toss is HEADS,

EXAMPLE 3: Coin flipping by telephone

The Algorithm

Bob: sends to Alice a random integer $1 \leq m \leq N$.

Alice: Returns $\varepsilon_m \in \{0, 1\}$ computed as follows:

$$\varepsilon_m = \begin{cases} 1 & \text{if} \quad ||x\gamma_m|| \in E, \\ 0 & \text{othervise.} \end{cases}$$

If $\varepsilon_m = 1$ the coin toss is HEADS,

If $\varepsilon_m = 0$ the coin toss is TAILS.

EXAMPLE 3: Coin flipping by telephone

Verification: Bob can verify the correctness of the coin flipp when Alice announces L, T, x and E.

Why does it work?

Why does it work?

Let

$$0 < \gamma_1 \leq \gamma_2 \leq \dots$$

be positive imaginary parts of non-trivial zeros of the Riemann zeta function.

Why does it work?

Let

$$0 < \gamma_1 \leq \gamma_2 \leq \dots$$

be positive imaginary parts of non-trivial zeros of the Riemann zeta function.

Theorem (E. Hlawka) *For every real $x \neq 0$ the sequence $(x\gamma_k)$ is uniformly distributed (mod 1) in the sense of H. Weyl:*

$$\forall_{0 \leq a < b < 1} \#\{k \leq N : a \leq ||x\gamma_k|| < b\} \sim (b-a)N$$

as $N \to \infty$.

Why does it work?

Let

$$0 < \gamma_1 \leq \gamma_2 \leq \dots$$

be positive imaginary parts of non-trivial zeros of the Riemann zeta function.

Theorem (E. Hlawka) *For every real $x \neq 0$ the sequence $(x\gamma_k)$ is uniformly distributed (mod 1) in the sense of H. Weyl:*

$$\forall_{0 \leq a < b < 1} \#\{k \leq N : a \leq ||x\gamma_k|| < b\} \sim (b-a)N$$

as $N \to \infty$.

Generalizations: P.D.T.A. Elliott, A. Fuji, H. Rademacher, J.K. ...

A-U.D. (mod 1)

A-U.D. (mod 1)

For simplicity: the case of Dirichlet L-functions.

A-U.D. (mod 1)

For simplicity: the case of Dirichlet L-functions.

- ⋆ Let

$$0 < \gamma_1 \leq \gamma_2 \leq \dots$$

be positive imaginary parts of non-trivial zeros of $L(s, \chi)$.

A-U.D. (mod 1)

For simplicity: the case of Dirichlet L-functions.

- Let

$$0 < \gamma_1 \leq \gamma_2 \leq \dots$$

be positive imaginary parts of non-trivial zeros of $L(s, \chi)$.

- The positive Toeplitz matrix:

A-U.D. (mod 1)

For simplicity: the case of Dirichlet L-functions.

- ⋆ Let

$$0 < \gamma_1 \leq \gamma_2 \leq \dots$$

be positive imaginary parts of non-trivial zeros of $L(s, \chi)$.

- ⋆ The positive Toeplitz matrix:

$$A = [a_{nk}]_{n,k \geq 1}$$

A-U.D. (mod 1)

For simplicity: the case of Dirichlet L-functions.

- Let

$$0 < \gamma_1 \leq \gamma_2 \leq \dots$$

be positive imaginary parts of non-trivial zeros of $L(s, \chi)$.

- The positive Toeplitz matrix:

$$A = [a_{nk}]_{n,k \geq 1}$$

$$a_{nk} = \frac{1}{S_n} e^{-\gamma_k} \gamma_k^n,$$

A-U.D. (mod 1)

For simplicity: the case of Dirichlet L-functions.

- Let

$$0 < \gamma_1 \leq \gamma_2 \leq \dots$$

be positive imaginary parts of non-trivial zeros of $L(s, \chi)$.

- The positive Toeplitz matrix:

$$A = [a_{nk}]_{n,k \geq 1}$$

$$a_{nk} = \frac{1}{S_n} e^{-\gamma_k} \gamma_k^n,$$

$$S_n = \sum_{k=1}^{\infty} e^{-\gamma_k} \gamma_k^n.$$

A-U.D. (mod 1)

THEOREM ([2]) *For every real $x \neq 0$ the sequence $x\gamma_k$ is A-uniformly distributed (mod 1):*

$$\forall_{0\leq a<b<1} \quad \sum_{\substack{k\geq 1 \\ a\leq ||x\gamma_k||<b}} a_{nk} \to (b-a)$$

as $N \to \infty$.

A-U.D. (mod 1)

THEOREM ([2]) *Weyl uniform distribution (mod 1) is of type* 1, *whereas A-uniform distribution (mod 1) is of type* $1/2$.

A-U.D. (mod 1)

THEOREM ([2]) *Weyl uniform distribution (mod 1) is of type* 1, *whereas A-uniform distribution (mod 1) is of type* $1/2$.

COROLLARY *Suppose* (t_k) *is A-u.d. (mod 1). Then every finite subsequence*

$$(t_k)_{k=N}^{N+H} \quad , \quad H \geq N^{1/2+\varepsilon}$$

fills approximately uniformly $[0, 1)$.

A-U.D. (mod 1)

THEOREM ([2]) *Weyl uniform distribution (mod 1) is of type* 1, *whereas A-uniform distribution (mod 1) is of type* $1/2$.

COROLLARY *Suppose* (t_k) *is A-u.d. (mod 1). Then every finite subsequence*

$$(t_k)_{k=N}^{N+H} \quad , \quad H \geq N^{1/2+\varepsilon}$$

fills approximately uniformly $[0,1)$.

HENCE: *For* $N \to \infty$ *the probability that a randomly chosen*

$$t_k \quad N \leq k \leq N + N^{1/2+\varepsilon}$$

lands in $E \subset [0,1)$ *tends to the Jordan measure of* E.

This justifies the choice of parameters of the coin flipping scheme:

This justifies the choice of parameters of the coin flipping scheme:

- $N = T^{\theta}$ with $\theta > 1/2$ since A-u.d. (mod 1) is of type $1/2$;

This justifies the choice of parameters of the coin flipping scheme:

- $N = T^{\theta}$ with $\theta > 1/2$ since A-u.d. (mod 1) is of type $1/2$;
- Jordan measure of $E \subset [0,1)$ being $1/2$ implies

$$Prob(HEADS) = Prob(TAILS) = 1/2.$$

Generalization: Apply the same procedure for an arbitrary L-function.

SOME OPEN PROBLEMS:

SOME OPEN PROBLEMS:

1. Provide algorithms for generating 'large' families of L-functions.

SOME OPEN PROBLEMS:

1. Provide algorithms for generating 'large' families of L-functions.
2. Provide algorithms for calculating Dirichlet coefficients of L-functions (for all n or for prime powers).

SOME OPEN PROBLEMS:

1. Provide algorithms for generating 'large' families of L-functions.
2. Provide algorithms for calculating Dirichlet coefficients of L-functions (for all n or for prime powers).
3. Provide (fast) algorithms for calculating non-trivial zeros of L-functions.

SOME OPEN PROBLEMS:

1. Provide algorithms for generating 'large' families of L-functions.
2. Provide algorithms for calculating Dirichlet coefficients of L-functions (for all n or for prime powers).
3. Provide (fast) algorithms for calculating non-trivial zeros of L-functions.
4. ...

Bibliography

[1] M. Anshel, D. Goldfeld, *Zeta functions, one-way functions, and pseudorandom number generators,* Duke Math. J. **88**(1997), 371–390.

[2] J. Kaczorowski, *The k-functions in multiplicative number theory, II, III,* Acta Arith. **56**(1990), 213–224; ibidem **57**(1990), 199–210.

[3] J. Kaczorowski, *Axiomatic theory of L-functions: the Selberg class,* in *Analytic Number Theory*, C.I.M.E. Summer School,Cetraro (Italy) 2002, ed. by A. Perelli, C. Viola, 133–209, Springer L.N. 1891, 2006.

[4] J. Kaczorowski, A. Perelli, *On the structure of the Selberg class, I, VII,* Acta Math. **182**(1999), 207-241; to appear in Annals of Math.

$$T_h(a,n)^k = y(0,u)!$$