ZASTOSOWANIE FUNKCJI L W KRYPTOLOGII

Jerzy Kaczorowski

Wydział Matematyki i Informatyki UAM, Poznań,
Instytut Matematyczny PAN, Warszawa

Streszczenie. Bezpieczeństwo asymetrycznych systemów kryptologicznych opiera się na założeniu, że istnieją funkcje jednokierunkowe. Fakt ten nie został do tej pory ściśle udowodniony. Nie mniej jednak pewne trudne obliczeniowo problemy teorii liczb, takie jak na przykład problem faktoryzacji, czy też problem obliczania logarytmu dyskretnego w skończonych grupach abelowych, mogą być podstawą konstrukcji funkcji uważanych za jednkierunkowe. Idea wykorzystania w tym konstekście funkcji typu L (elementów klasy Selberga) pojawiła się po raz pierwszy w pracy M. Anshela i D. Goldfelda z 1997 roku. Ich przydatność ilustrujemy na przykładzie protokołu uwierzytelnienia przy użyciu współczynników Dirichleta funkcji L oraz eliptycznego generatora pseudolosowego. Na zakończenie przedstawiamy propozycję innego typu, a mianowicie opis protokołu rzutu monetą przez telefon opartego na wykorzystaniu nietrywialnych zer funkcji L.

Słowa kluczowe: funkcje jednokierunkowe, funkcje L, klasa Selberga.

1.

Znaczenie teorii liczb dla kryptologii stało się ważne z chwilą pojawienia się systemów asymetrycznych. Ich bezpieczeństwo opiera się na założeniu, że istnieją funkcje jednokierunkowe, których wartości mogą być efektywnie obliczane, natomiast przeciwobrazy – nie. Istnienie takich funkcji nie zostało jeszcze ściśle udowodnione, nie mniej jednak znane są przykłady, które najprawdopodobniej prowadzą do funkcji jednokierunkowych. Jednym z nich jest zwyczajne mnożenie liczb naturalnych. Może być ono szybko i efektywnie (w czasie wielomianowym) wykonane, natomiast operacja odwrotna, to znaczy rozkład liczby naturalnej na czynniki, jest znacznie trudniejsza i w chwili obecnej nie wiadomo, czy istnieje działający wielomianowo algorytm rozwiązujący to zagadnienie. Innym standardowym przykładem trudnego obliczeniowo problemu, na którym oparte są niektóre asymetryczne systemy kryptologiczne jest zagadnienie logarytmu dyskretnego w grupach. Z tego punktu widzenia szczególnie ciekawa jest teoria krzywych eliptycznych nad ciałami skończonymi, głównie ze względu na

Praca częściowo sfinansowana ze środków projektu badawczego nr 2013/11/B/ST1/02799 Narodowego Centrum Nauki

łatwość generowania grup abelowych o dobrych własnościach kryptologicznych.

Zasadnicze ograniczenia w konstrukcji nowych asymetrycznych systemów szyfrowania wynikają z faktu, że znanych jest stosunkowo niewiele funkcji, które są prawdopodobnie jednokierunkowe. Najpopularniejsze to wspomiane wyżej operacje związane z problemem faktoryzacji oraz logarytmu dyskretnego. Niniejsza praca ma na celu zareklamowanie innej rodziny o potencjalnie dużym znaczeniu kryptologicznym związanej z wykorzystaniem dobrze znanych w teorii liczb funkcji typu L. Idea ta pojawiła się po raz pierwszy w pracy M. Anshela i D. Goldfelda z 1997 roku ([1]), do której będziemy się wielokrotnie odwoływać.

Przykład 1. (*Uwierzytelnianie przy pomocy charakterów Dirichleta,* por. [1]). Zakładamy, że Alicja jest użytkownikiem pewnego systemu, a Bob jest osobą mającą stwierdzić, czy jest ona użytkownikiem uprawnionym. Zakładamy, że każdy uprawniony użytkownik zna (tajny) charakter Dirichleta $\chi(\bmod q)$. Schemat uwierzytelniania jest wtedy następujący: Bob do Alicji wysyła dwie losowo wybrane liczby całkowite m oraz $b > 0$, a w odpowiedzi Alicja do wysyła Boba wektor $v = (\chi(m), \chi(m+1), \dots, \chi(m+b))$. Bob weryfikuje otrzymaną listę i jeżeli jest poprawna, to potwierdza tożsamość Alicji. Procedurę może iterować dla większego bezpieczeństwa. Nietrywialnym przykładem charakteru Dirichleta jest symbol Kroneckera $\chi = \left(\frac{d}{\cdot}\right)$. Podstawowe wiadomości o charakterach Dirichleta, a w szczególności o symbolu Kroneckra czytelnik znajdzie na przykład w [4]. Wiara w to, że przedstawiony prosty schemat uwierzytelniania jest bezpieczny opiera się na następującej hipotezie, którą dla prostoty przedstawiamy w szczególnym przypadku, gdy rozważany charakter jest symbolem Kroneckera.

Hipoteza. (Anshel-Goldfeld [1]) *Dla dostatecznie dużej liczby rzeczywistej X oraz ustalonych A i B (niezależnych od X) projekcja*

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

gdzie

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

jest funkcją jednokierunkową.

Podobną hipotezę można wypowiedzieć w odniesieniu do dowolnego pierwotnego charakteru Dirichleta o dostatecznie dużym przewodniku. Istota sprawy w rozważanym przykładzie jest taka, że wartości symbolu

Kroneckera, lub ogólniej ustalonego charakteru Dirichleta, mogą być obliczane szybko, natomiast rozpoznanie, o który charakter chodzi znając tylko pewną liczbę jego wartości (dość dużą, ale znaczaco mniejszą od przewodnika) jest zagadnieniem trudnym obliczeniowo. W każdym razie nie znamy żadnego efektywnego algorytmy rozwiązującego to zagadnienie. Krótko mówiąc do naszej dotychczasowej listy problemów obliczeniowo trudnych (faktoryzacjia, logarytm dyskretny) dołączamy następny, a mianowicie identyfikację charakteru Dirichleta przy znajomości pewnej liczby jego wartości przyjmowanych na kolejnych liczbach całkowitych.

Zauważmy, że charakter Dirichleta $\chi(\mathrm{mod} q)$ jednoznacznie wyznacza funkcję L Dirichleta, zdefiniowaną dla liczb zespolonych $s = \sigma + it$, $\sigma > 1$ wzorem

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

a dla pozostałych s poprzez przedłużenie analityczne. Odwrotnie, każda funkcja L Dirichleta jednoznacznie wyznacza pewien charakter. W związku z tym poprzedni przykład można uogólnić następująco. Alicja i Bob ustalają (tajną) L-funkcję ($\mathrm{Re}\,(s) > 1$):

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

a następnie postępują w sposób analogiczny do wcześniej omówionego. Bob przesyła Alicji losowo wybrane liczby naturalne m i b, a w odpowiedzi otrzymuje wektor współczynników $v = (a_L(m), a_L(m+1), \ldots, a_L(m+b))$. Jeżeli lista Alicji jest poprawna, to jest ona uprawnionym użytkownikiem systemu.

Jest jasne, że funkcja L użyta w tym uogólnieniu musi spełniać następujące dwa warunki. Po pierwsze, jej współczynniki Dirichleta powinny być łatwe do wyznaczania i po drugie, problem identyfikacji samej funkcji L powinien być obliczeniowo trudny. Niewątpliwą korzyścią z dopuszczenia do rozważań ogólnych funkcji L jest uzyskanie znacznej swobody w konstrukcjach kryptologicznych. Związane jest to z obszernością klasy znanych funkcji L.

Należy zacząć od sprecyzowania tego pojęcia i odpowiedzieć na z pozoru proste pytanie: co to jest funkcja L? Paradoksalnie udzielenie zadawalającej odpowiedzi nie jest proste. W tym artykule przez funkcję L będzieny rozumieć nietrywialny elemant klasy Selberga.

Definicja. (Selberg, 1989, (por. [22])). Funkcja F należy do klasy Selberga wtedy i tylko wtedy, gdy $F(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$, gdzie:

1. szereg Dirichleta jest bezwzględnie zbieżny dla $\sigma := \mathrm{Re}\,(s) > 1$.
2. (*Przedłużenie analityczne*) Istnieje liczba całkowita $m \geq 0$ taka, że $(s-1)^m F(s)$ jest funkcją całkowitą skończonego rzędu.
3. (*Równanie funkcyjne*)

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

gdzie

$$\Phi(s) = Q^s \prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) F(s) = \gamma(s) F(s),$$

dla pewnych $r \geq 0$, $Q > 0$, $\lambda_j > 0$, $\mathrm{Re}\,\mu_j \geq 0$, $|\omega| = 1$.

4. (*Postulat Ramanujana*) Dla każdego $\varepsilon > 0$ mamy $a(n) \ll n^{\varepsilon}$, to znaczy istnieje stała $A(\varepsilon)$ taka, że dla $n \geq 1$ mamy $|a(n)| \leq A(\varepsilon) n^{\varepsilon}$.
5. (*Iloczyn Eulera*) Dla $\sigma > 1$ mamy

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

gdzie $b(n) = 0$ dla $n \neq p^m$ oraz $b(n) \ll n^{\theta}$ dla pewnego $\theta < 1/2$.

Klasę Selberga oznaczamy symbolem S. Funkcja tożsamościowo równa 1 jest w sposób oczywisty elementem klasy Selberga. Jest to jednak przykład nieciekawy z punktu widzenia kryptologii. Przez nietrywialne elementy S rozumiemy funkcje $F \not\equiv 1$. Przegląd podstawowych własności klasy Selberga czytelnik znajdzie w [14]. Czasami wygodnie jest rozważać większy zbiór szeregów Dirichleta, a mianowicie tak zwaną *rozszerzoną klasę Selberga* $S^{\#}$. Jest to zbiór funkcji $F \not\equiv 0$ spełniających aksjomaty (1), (2) i (3).

Przykład 2. (*Elementy klasy Selberga*).

1. Funkcja dzeta Riemanna $\zeta(s)$, por. [24], [11];
2. przesunięta funkcja L Dirichleta $L(s+i\theta, \chi)$, gdzie χ jest pierwotnym charakterem Dirichleta (mod$q$), $q > 1$, a θ jest liczbą rzeczywistą, por. [4], [19];
3. $\zeta_K(s)$, funkcja dzeta Dedekinda ciała liczb algebraicznych K, por. [18];
4. $L_K(s, \chi)$, funkcja L Hecke'go z pierwotnym charakterem Hecke'go $\chi(\mathrm{mod}\mathfrak{f})$, $\mathfrak{f}$ jest ideałem pierścienia liczb algebraicznych całkowitych ciała K, por. [18];
5. funkcje L holomorficznych nowych form podgrup kongruencyjnych grupy$SL_2(\mathbb{Z})$ (po odpowiednim znormalizowaniu). Jest to wniosek

z klasycznej teorii Hecke'go (por. [12], [17]) oraz słynnego twierdzenia P. Deligne'a [5];
6. funkcje L wymiernych krzywych eliptycznych. Jest to wniosek poprzedniego przykładu w połączeniu z twierdzeniem A. Wilesa ([26], [25], [2]);
7. sploty Rankina-Selberga znormalizowanych holomorficznych nowych form, por. [12], [17];
8. $F, G \in S \Rightarrow FG \in S$ (podobnie dla $S^{\#}$)
9. Jeżeli $F \in S$ jest całkowita to jej przesunięcie $F_\theta(s) = F(s + i\theta)$ jest elementem S dla każdej liczby rzeczywistej θ.

W pewnych przypadkach nie potrafimy stwierdzić, czy klasyczna funkcja L jest elementem klasy Selberga. Najczęściej prawdopodobnie tak jest, ale odpowiedź zależy od przyjęcia pewnych (klasycznych) hipotez.

Przykład 3. (*Warunkowe elementy klasy Selberga*).
1. Funkcje L Artina nieprzywiedlnych reprezentacji grup Galois (modulo hipoteza Artina: brakuje dowodu istnienia przedłużenia do funkcji holomorficznej na $\mathbb{C}$), por. [16];
2. funkcje L nieholomorficznych nowych form modularnych (problemy z postulatem Ramanujana), por. [3];
3. potęgi symetryczne, np. dla znormalizowanych holomorficznych nowych form:
$$L(s) = \prod_p \left(1 - \frac{a_p}{p^s}\right)^{-1} \left(1 - \frac{b_p}{p^s}\right)^{-1}$$
r-ta potęga symetryczna:
$$L_r(s) = \prod_p \prod_{j=0}^{r} (1 - a_p^j b_p^{r-j} p^{-s})^{-1}$$
(modulo hipoteza Langlandsa o funktorialności);
4. ogólniej: funkcje L reprezentacji automorficznych $GL_n(K)$ (problemy z postulatem Ramanujana), por. [3].

Standardowymi przykładami funkcji L z rozszerzonej klasy Selberga są kombinacje liniowe elementów klasy Selberga spełniające to samo równanie funkcyjne. Klasycznym przykładem jest funkcja Davenporta-Heilbronna
$$L(s) = \overline{\lambda} L(s, \chi_1) + \lambda L(s, \overline{\chi}_1),$$

gdzie χ_1 charakterem Dirichleta $\bmod 5$ takim, że $\chi_1(2) = i$, a stała λ dana jest wzorem

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

Równanie funkcyjne tej funkcji jest postaci

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

Nie wszystkie funkcje L z klasy Selberga jednakowo dobrze nadają się do zastosowań kryptologicznych. W niektórych przypadkach przeszkodą może być na przykład brak algorytmów szybkiego obliczania ich współczynników Dirichleta. Tak jest na przykład dla pewnych rozmaitości abelowych nad ciałami skończonymi (por. [8]).

2. Eliptyczne generatory pseudolosowe

Niech E oznacza krzywą eliptyczną nad $\mathbb{Q}$ daną równaniem Weierstrassa

$$E: \quad y^2 = x^3 + ax + b$$
$$a, b \in \mathbb{Z} \quad , \quad \Delta_E := 4a^3 + 27b^2 \neq 0.$$

Dla liczb pierwszych $p \not| \Delta_E$ równanie

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

definiuje krzywą eliptyczną nad p-elementowym ciałem skończonym $\mathbb{F}_p$. Dla $p \not| \Delta_E$ kładziemy

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

Z cytowanego już wcześniej twierdzenia A. Wilesa otrzymujemy jako wniosek następujący wynik o podstawowym znaczeniu.

Twierdzenie 1. *Istnieją jednoznacznie wyznaczone liczby całkowite* $a_E(p)$, $p|\Delta_E$ *takie, że*

$$L(s,E) = \prod_{p|\Delta_E}\left(1 - \frac{a_E(p)}{p^s}\right)^{-1} \prod_{p \not| \Delta_E}\left(1 - \frac{a_E(p)}{p^s} + p^{1-2s}\right)^{-1}$$

(iloczyn zbieżny dla $\mathrm{Re}\,(s) > 3/2$*) ma przedłużenie do funkcji holomorficznej na całej płaszczyźnie zespolonej i spełnia następujące równanie funkcyjne:*

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

gdzie, $\omega = \pm 1$.

Twierdzenie 2.

1. *Dla* $\mathrm{Re}\,(s) > 3/2$ *funkcja* $L(s, E)$ *jest określona przez bezwzględnie zbieżny szereg Dirichleta*

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

2. *Współczynniki* $a_E(n)$ *są liczbami całkowitymi.*
3. *Dla* $n \geq 1$ *mamy* $|a_E(n)| \leq \sqrt{n}d(n)$ *(jest to znane twierdzenie Hasse'go, por. np. [10]).*
4. *Współczynniki* $a_E(p^k)$ *mogą być obliczone w czasie wielomianowym (por. Schoof [21]).*
5. $L(s + \frac{1}{2}, E) \in S$.

Twierdzenie 3. *Niech* $a, b \in \mathbb{Z}$ *będą takie, że* $4a^3 + 27b^2 \neq 0$, *oraz ciało rozkładu wielomianu*

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

ma nad $\mathbb{Q}$ *stopień równy* 6. *Wtedy gęstość liczb pierwszych* p, *dla których* $2|a_E(p)$ *wynosi* $2/3$*:*

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

Dowód tego twierdzenia można znaleźć w [1]. Z założenia o stopniu ciała rozkładu wynika łatwo, że grupa Galois wielomianu $X^3 + aX + b$ jest grupą $\mathbf{S}_3$ symetryczną trzech elementów. Pierwszym fundamentalnym faktem użytym w dowodzie Twierdzenia jest twierdzenie Serre'a o obrazie reprezentacji tej grupy indukowanej przez jej działanie na zbiorze punktów krzywej eliptycznej ustalonego rzędu ([23]). Drugim faktem używanym w dowodzie jest słynne twierdzenie Czebotarewa o gęstości, por. [15].

Pokażemy teraz jak funkcje L krzywych eliptycznych mogą być wykorzystane do konstrukcji generatorów pseudolosowych. W pierwszym kroku procedury ustalamy liczby $a, b \in \mathbb{Z}$ takie, że

1. $4a^3 + 27b^2 \neq 0$,
2. ciało rozkładu wielomianu $X^3 + aX + b$ ma stopień 6 nad $\mathbb{Q}$.

Para (a, b) jest zalążkiem ciągu pseudolosowego. Następnie rozważamy krzywą eliptyczną E daną równaniem Weierstrassa

$$y^2 = x^3 + ax + b$$

oraz odpowiadającą jej funkcję $L(s, E)$. Redukując modulo 2 współczynniki szeregu Dirichleta tej funkcji odpowiadające liczbom pierwszym otrzymujemy ciąg binarny

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

Z ostatniego twierdzenia wnioskujemy, że jest to ciąg pseudolosowy z rozkładem prawdopodobieństwa $(1/3, 2/3)$, to znaczy ciąg, w którym prawdopodobieństwo wystąpienia cyfry 0 jest równe $2/3$, a cyfry 1 równe $1/3$.

Problem: zastosować podobną procedurę do innych funkcji typu L.

3. Rzut monetą przez telefon

Dotychczas opisane w literaturze zastosowania kryptologiczne funkcji L oparte są głównie na użyciu ich współczynników Dirichleta. Wydaje się jednak, że jest to jedynie fragment potencjalnych możliwości. Na zakończenie tej krótkiej notki przedstawimy propozycję innego typu, a mianowicie opis protokołu rzutu monetą przez telefon opartego na wykorzystaniu nietrywialnych zer funkcji L.

Czynności przygotowawcze
Krok I: Alicja wybiera:
(a) funkcję L,
(b) parametry $T, x \in \mathbb{R}$, $N \in \mathbb{N}$ ($N \sim T^\theta, \theta > 1/2$),
(c) zbiór $E \subset [0, 1)$ o mierze Jordana $1/2$.
Krok II: Alicja oblicza kolejne nietrywialne zera $\rho_1, \rho_2, \ldots, \rho_N$ funkcji $L(s)$ na prostej $\sigma = 1/2$:

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

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

Algorytm

Bob: wysyła do Alicji losowo wybraną liczbę całkowią $1 \leq m \leq N$.
Alicja: zwraca $\varepsilon_m \in \{0, 1\}$ obliczone następująco:

$$\varepsilon_m = \begin{cases} 1 & \text{g}dy \quad \|x\gamma_m\| \in E, \\ 0 & \text{w } przeciwnym\ wypadku, \end{cases}$$

gdzie dla liczby rzeczywistej α, symbol $||\alpha||$ oznacza jej część ułamkową. Jeżeli $\varepsilon_m = 1$, wynikiem rzutu monetą jest ORZEŁ,

Jeżeli $\varepsilon_m = 0$, wynikiem rzutu monetą jest RESZKA.

Weryfikacja

Bob może zweryfikować poprawność rzutów, gdy Alicja ujawni L, T, x oraz E.

Zasadniczym faktem leżącym u podstaw powyższego protokołu jest ekwipartycja części urojonych nietrywialnych zer funkcji L. Pierwszy bezwarunkowy wynik w tym kierunku uzyskał E. Hlawka w przypadku funkcji dzeta Riemanna. Niech $0 < \gamma_1 \leq \gamma_2 \leq \ldots$ będą dodatnimi częściami urojonymi nietrywialnych zer tej funkcji.

Twierdzenie 4. ([9]) *Dla każdej liczby rzeczywistej $x \neq 0$ ciąg $(x\gamma_k)$ ma ekwipartycję* (mod 1) *w sensie H. Weyla:*

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

przy $N \to \infty$.

Twierdzenie to było następnie wielokrotnie uogólniane i wzmacniane, por. np. P.D.T.A. Elliott [6], A. Fujii [7], H. Rademacher [20]. Dla potrzeb omawianego zastosowania kryptologicznego najodpowiedniejsze będzie posłużenie się tak zwaną A-ekwipartycją (mod 1), pojęcem wprowadzonym w [13]. Dla ustalenia uwagi ograniczymy się do przypadku funkcji L Dirichleta, chociaż nie ma zasadniczych trudności, aby potrzebne twierdzenia uzyskać dla znacznie ogólniejszej klasy funkcji L. Ustalmy charakter Dirichleta χ oraz uszeregujmy części urojone nietrywialnych zer $L(s,\chi)$ w porządku niemalejącym (z uwzględnieniem krotności): $0 < \gamma_1 \leq \gamma_2 \leq \ldots$, a następnie rozważmy następującą dodatnią macierz Toeplitza:

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

$$a_{nk} = \frac{1}{S_n} e^{-\gamma_k} \gamma_k^n, \quad S_n = \sum_{k=1}^{\infty} e^{-\gamma_k} \gamma_k^n.$$

Twierdzenie 5. ([13]) *Dla każdej liczby rzeczywistej $x \neq 0$ ciąg $(x\gamma_k)$ jest A-jednostajnie rozłożony* (mod 1)*, to znaczy*

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

przy $N \to \infty$.

Twierdzenie 6. ([13]) *Ekwipartycja* (mod 1) *w sensie Weyla jest typu* 1, *natomiast A-ekwipartycja jest typu* 1/2.

Dokładne wyjaśnienie znaczenia tego twierdzenia, a w szczególności definicję typu ekwipartycji można znaleźć w [13]. Z grubsza rzecz ujmując fakt, iż A-ekwipartycja ma typ 1/2 oznacza, że jeżeli ciąg (t_k), jest A-jednostajnie rozłożony (mod 1), to każdy skończony ciąg

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

mniej więcej równomiernie wypełnia przedział $[0,1)$. W szczególności przy $N \to \infty$, prawdopodobieństwo tego, że część ułamkowa losowo wybranego wyrazu

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

będzie należała do ustalonego zbioru $E \subset [0,1)$ dąży do miary Jordana zbioru E.

To uzasadnia wybór parametrów w schemacie rzutu monetą przez telefon. Założenie $N = T^\theta$ z $\theta > 1/2$ wystarcza na mocy ostatniego Twierdzenia. Fakt, że miara Jordana zbioru $E \subset [0,1)$ wynosi 1/2 gwarantuje równość prawdopodobieństw wylosownia orła i reszki

$$Prob(\text{RESZKA}) = Prob(\text{ORZEŁ}) = 1/2.$$

Zmieniając miarę zbioru E otrzymujemy protokół rzutu monetą niesymetryczną.

Literatura

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

[2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises,* J. Amer. Math. Soc. 14 (2001), no. 4, 843–939.

[3] D. Bump, *Authomorphic forms and representations*, Cambridge University Press, Cambridge 1997.

[4] H. Davenport, *Multiplicative number theory*, 2nd ed. Springer, Berlin-Heidelberg 1980.

[5] P. Deligne, *Formes modulaires et reprsentations l-adiques*, Séminaire Bourbaki vol. 1968/69 Exposés 347-363, Lecture Notes in Mathematics 179, Berlin, New York: Springer-Verlag, 1971.

[6] P. D. T. A. Elliott, *The Riemann zeta function and coin tossing,* J. Reine Angew. Math. 254 (1972), 100–109.

[7] A. Fujii, *On the zeros of Dirichlet L-functions, III, IV* Trans. Amer. Math. Soc. 219 (1976), 347–349; J. Reine Angew. Math. 286(287) (1976), 139–143.

[8] J. von zur Gathen, M. Karpinski, I, Shparlinski, *Counting courves and their projections* , in Proceedings of the 25th Annual Symposium on Theory of Computing, Association for Computing Machinery, New York, 1993, 805–812.

[9] E. Hlawka, *Über die Gleichverteilung gewisser Folgen, welche mit den Nullstellen der Zetafunktion zusammenhängen*, Österreich. Akad. Wiss. Math.-Naturwiss. Kl. S.-B. II 184 (1975), no. 8-10, 459–471

[10] D. Husemoller, *Elliptic Curves,* Grad. Texts in Math. 111, Springer-Verlag, New York 1987.

[11] A. Ivić, *The Riemann Zeta-function*, Wiley, New York, 1985.

[12] H. Iwaniec, *Topics in Classical Automorphic forms*, Graduate Studies in Mathematics, 17, American Mathematical Sociaty, Providence, Rhode Island, 1997.

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

[14] 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.

[15] J. C. Lagarias, A. M. Odlyzko, *Effective versions of the Chebotarev density theorem. Algebraic number fields: L-functions and Galois properties* (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464. Academic Press, London, 1977.

[16] J. Martinet, *Character theory and Artin L-functions*, in A. Fröhlich (ed.) *Algebraic Number Theory*, Academic Press London-New York-San Francisco 1977.

[17] T. Miyake, *Modular forms*, Springer-Verlag 1989.

[18] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN, Springer-Verlag, 1990.

[19] K. Prachar, *Primzahlverteilung*, Springer-Verlag, 1978.

[20] H. Rademacher, *Collected papers of Hans Rademacher. Vol. II,* Mathematicians of Our Time, 4. MIT Press, Cambridge, Mass.-London, 1974. xxi+638 pp.

[21] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. 44 (1985), no. 170, 483–494.

[22] A. Selberg, *Old and new conjecture and results about a class of Dirichlet series*, Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989) (ed. by E. Bombieri et. al.), 367-385, Università di Salerno, Salerno 1992; Collected papers vol II, 47-63, Springer, Berlin 1991.

[23] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Invent. Math. 15 (1972), no. 4, 259–331.

[24] E.C. Titchmarsh, *The theory of the Riemann zeta function*, 2nd ed., Clarendon Press, Oxford, 1988.

[25] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras,* Ann. of Math. (2) 141 (1995), no. 3, 553–572.

[26] A. Wiles, *Modular elliptic curves and Fermat's last theorem,* Ann. of Math. (2) 141 (1995), no. 3, 443–551.

APPLICATIONS OF L-FUNCTIONS IN CRYPTOLOGY

Abstract. Security of asymmetric cryptological systems is based on the unproved hypothesis that one-way functions do exist. Some difficult computational problems in number theory, such as factorization or a discrete logarithm problem in finite Abelian groups may serve as a basis for constructing presumably one-way functions. The idea of using L-functions (elements of the Selberg class) in this context goes back to M. Anshel and D. Goldfeld (1997). Following them we describe an authentication protocol and an elliptic pseudo-random generator. The former uses Dirichlet L-functions, and the latter Hasse-Weil L-functions of elliptic curves over $\mathbb{Q}$. We conclude by proposing a protocol of coin toss by phone based on the use of non-trivial zeros of L-functions.

Keywords: one-way functions, L-functions, Selberg class.