Pseudorandom Binary Sequences from Elliptic Curves

László Mérai

Rényi Institute
Budapest, Hungary

June 12, 2010

Pseudorandomness

Definition

A sequence can be considered as a pseudorandom sequence, if it cannot be distinguish from random sequences.

Pseudorandomness

Definition

A sequence can be considered as a pseudorandom sequence, if it cannot be distinguish from random sequences.

- If the sequence is *infinite*, then we can test it by complexity theory, etc.
- If the sequence is *finite*, we can only study its statistical properties

Pseudorandomness

Definition

A sequence can be considered as a pseudorandom sequence, if it cannot be distinguish from random sequences.

- If the sequence is *infinite*, then we can test it by complexity theory, etc.
- If the sequence is *finite*, we can only study its statistical properties
  - well-distribution relative to arithmetic progression

Pseudorandomness

Definition

A sequence can be considered as a pseudorandom sequence, if it cannot be distinguish from random sequences.

- If the sequence is *infinite*, then we can test it by complexity theory, etc.
- If the sequence is *finite*, we can only study its statistical properties
  - well-distribution relative to arithmetic progression
  - normality
  - auto-correlation

Pseudorandomness

Definition

A sequence can be considered as a pseudorandom sequence, if it cannot be distinguish from random sequences.

- If the sequence is *infinite*, then we can test it by complexity theory, etc.
- If the sequence is *finite*, we can only study its statistical properties
  - well-distribution relative to arithmetic progression
  - normality
  - auto-correlation

Maudit and Sárközy introduced several measures of pseudorandomness focusing on this properties.

If we want to consider a sequence as pseudorandom, then it must be indistinguishable from random sequences with respect to these measures.

Measures of pseudorandomness

Let $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ be a finite binary sequence. Then

Definition (Mauduit, Sárközy)

The well-distribution measure of E_N:

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=1}^{t-1} e_{a+jb} \right|,$$

where $a, b, t \in \mathbb{N}$, $a + (t-1)b \leq N$.

The correlation measure of order ℓ of E_N:

$$C_\ell(E_N) = \max_{M,D} \left| \sum_{j=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right|,$$

$D = (d_1, d_2, \dots, d_\ell)$, $M \in \mathbb{N}$, $M + d_\ell \leq N$.

Measures of pseudorandomness

Theorem (Alon, Kohayakava, Mauduit, Moreira, Rödl)

If E_N is a truly random sequence, then we have

$$\frac{1}{\delta}\sqrt{N} < W(E_N) < \delta\sqrt{N}$$

and

$$\frac{2}{5}\sqrt{N\log\binom{N}{\ell}} < C_\ell(E_N) < \frac{7}{4}\sqrt{N\log\binom{N}{\ell}}.$$

with probability at least $1-\varepsilon$.

Measures of pseudorandomness

Theorem (Alon, Kohayakava, Mauduit, Moreira, Rödl)

If E_N is a truly random sequence, then we have

$$\frac{1}{\delta}\sqrt{N} < W(E_N) < \delta\sqrt{N}$$

and

$$\frac{2}{5}\sqrt{N\log\binom{N}{\ell}} < C_\ell(E_N) < \frac{7}{4}\sqrt{N\log\binom{N}{\ell}}.$$

with probability at least $1-\varepsilon$.

Definition

The E_N sequence is considered as a pseudorandom sequence if

$$W(E_N) \ll N^{1/2}\log N^{c} \quad \text{ill.} \quad C_\ell(E_N) \ll \ell N^{1/2}\log N^{c'}.$$

Earlier construction over $\mathbb{F}_p$

Several construction have been tested in terms of these measures earlier:

- *Goubin, Mauduit, Sárközy*: Legendre symbol sequence:

$$e_n = \left(\frac{f(n)}{p} \right)$$

Earlier construction over $\mathbb{F}_p$

Several construction have been tested in terms of these measures earlier:

- *Goubin, Mauduit, Sárközy*: Legendre symbol sequence:

$$e_n = \left(\frac{f(n)}{p} \right)$$

- *Rivat, Mauduit, Sárközy*: Residue of a polynomial:

$$e_n = +1 \quad \Leftrightarrow \quad f(n) \in \{0, 1, 2, \dots, \frac{p-1}{2}\}$$

Earlier construction over $\mathbb{F}_p$

Several construction have been tested in terms of these measures earlier:

- *Goubin, Mauduit, Sárközy*: Legendre symbol sequence:

$$e_n = \left(\frac{f(n)}{p}\right)$$

- *Rivat, Mauduit, Sárközy*: Residue of a polynomial:

$$e_n = +1 \quad \Leftrightarrow \quad f(n) \in \{0, 1, 2, \ldots, \frac{p-1}{2}\}$$

- *Gyarmati*: Construction based on the discrete logarithm:

$$e_n = +1 \quad \Leftrightarrow \quad \log f(n) \in \{0, 1, 2, \ldots, \frac{p-1}{2}\}$$

Earlier construction over $\mathbb{F}_p$

Several construction have been tested in terms of these measures earlier:

- *Goubin, Mauduit, Sárközy*: Legendre symbol sequence:

$$e_n = \left(\frac{f(n)}{p}\right)$$

- *Rivat, Mauduit, Sárközy*: Residue of a polynomial:

$$e_n = +1 \quad \Leftrightarrow \quad f(n) \in \{0, 1, 2, \dots, \frac{p-1}{2}\}$$

- *Gyarmati*: Construction based on the discrete logarithm:

$$e_n = +1 \quad \Leftrightarrow \quad \log f(n) \in \{0, 1, 2, \dots, \frac{p-1}{2}\}$$

- *Gyarmati, Pethő, Sárközy*: A transform of sequences generating by linear recursion:

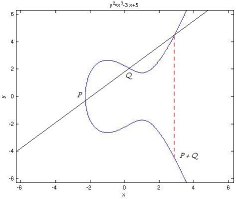
$$x_n \equiv c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_h x_{n-h} \pmod p$$

$$e_n = \left(\frac{x_n}{p}\right)$$

Here $f \in \mathbb{F}_p[x]$, $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo p.

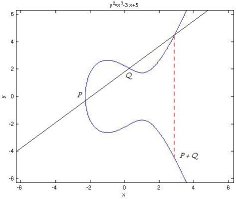
Elliptic curves

$$\mathcal{E}(\mathbb{F}_p) = \{(x, y) : y^2 = x^3 + Ax + B\}, \quad A, B \in \mathbb{F}_p.$$



Elliptic curves

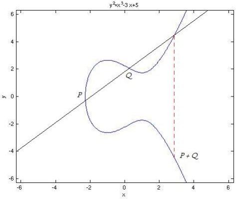
$$\mathcal{E}(\mathbb{F}_p) = \{(x, y) : y^2 = x^3 + Ax + B\}, \quad A, B \in \mathbb{F}_p.$$



- $(\mathcal{E}(\mathbb{F}_p), +)$ is an Abelian group.

Elliptic curves

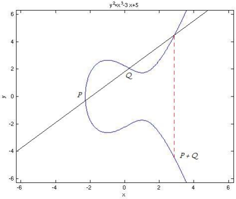
$$\mathcal{E}(\mathbb{F}_p) = \{(x, y) : y^2 = x^3 + Ax + B\}, \quad A, B \in \mathbb{F}_p.$$



- $(\mathcal{E}(\mathbb{F}_p), +)$ is an Abelian group.
- The neutral element of $\mathcal{E}$ is $\mathcal{O}$.

Elliptic curves

$$\mathcal{E}(\mathbb{F}_p) = \{(x, y) : y^2 = x^3 + Ax + B\}, \quad A, B \in \mathbb{F}_p.$$

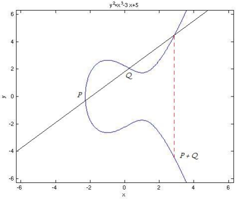


- $(\mathcal{E}(\mathbb{F}_p), +)$ is an Abelian group.
- The neutral element of $\mathcal{E}$ is $\mathcal{O}$.
- The number of points in $\mathcal{E}(\mathbb{F}_p)$ satisfies:

$$|p + 1 - |\mathcal{E}(\mathbb{F}_p)|| \leq 2\sqrt{q}.$$

Elliptic curves

$$\mathcal{E}(\mathbb{F}_p) = \{(x, y) : y^2 = x^3 + Ax + B\}, \quad A, B \in \mathbb{F}_p.$$



- $(\mathcal{E}(\mathbb{F}_p), +)$ is an Abelian group.
- The neutral element of $\mathcal{E}$ is $\mathcal{O}$.
- The number of points in $\mathcal{E}(\mathbb{F}_p)$ satisfies:

$$|p + 1 - |\mathcal{E}(\mathbb{F}_p)|| \leq 2\sqrt{q}.$$

- The set of rational function $f(P)(= f(x, y))$ on $\mathcal{E}$ is

$$\mathbb{F}_p(\mathcal{E}) = \mathbb{F}_p(x, y)/(y^2 = x^3 + Ax + B).$$

- We will use the notation: $P = (x(P), y(P))$.

Sequences generated from Elliptic Curves

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$ (or at least an element with large order). Then

$$n \longmapsto x(nG) \in \mathbb{F}_p,$$

Sequences generated from Elliptic Curves

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$ (or at least an element with large order). Then

$$n \longmapsto x(nG) \in \mathbb{F}_p,$$

or in general

$$n \longmapsto f(nG) \in \mathbb{F}_p,$$

where $f \in \mathbb{F}_p(\mathcal{E})$.

Sequences generated from Elliptic Curves

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$ (or at least an element with large order). Then

$$n \longmapsto x(nG) \in \mathbb{F}_p,$$

or in general

$$n \longmapsto f(nG) \in \mathbb{F}_p,$$

where $f \in \mathbb{F}_p(\mathcal{E})$.
In order to generate *binary* sequences we have to choose one of the bits of $f(nG)$:

Chen: $$n \quad \mapsto \quad \left(\frac{f(nG)}{p}\right)$$

Sequences generated from Elliptic Curves

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$ (or at least an element with large order). Then

$$n \longmapsto x(nG) \in \mathbb{F}_p,$$

or in general

$$n \longmapsto f(nG) \in \mathbb{F}_p,$$

where $f \in \mathbb{F}_p(\mathcal{E})$.
In order to generate *binary* sequences we have to choose one of the bits of $f(nG)$:

$$\text{Chen:} \quad n \mapsto \left(\frac{f(nG)}{p}\right)$$

$$\text{Liu, Zhan, Wang:} \quad n \mapsto \begin{cases} +1 & \text{if } f(nG) \in \{0, 1, 2 \ldots, \frac{p-1}{2}\} \\ -1 & \text{otherwise} \end{cases}$$

Here $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo p.

Sequences generated from Elliptic Curves

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$ (or at least an element with large order). Then

$$n \longmapsto x(nG) \in \mathbb{F}_p,$$

or in general

$$n \longmapsto f(nG) \in \mathbb{F}_p,$$

where $f \in \mathbb{F}_p(\mathcal{E})$.
In order to generate *binary* sequences we have to choose one of the bits of $f(nG)$:

Chen: $\quad n \mapsto \left(\frac{f(nG)}{p}\right)$

Liu, Zhan, Wang: $\quad n \mapsto \begin{cases} +1 & \text{if } f(nG) \in \{0, 1, 2 \ldots, \frac{p-1}{2}\} \\ -1 & \text{otherwise} \end{cases}$

Here $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo p.

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = x$.

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = x$.

$$e_n = \left(\frac{x(nG)}{19}\right)$$

n	nG	e_n	n	nG	e_n
1	(2,2)	-1	11	(18 ,1)	
2	(7,14)		12	(16 ,6)	
3	(15,1)		13	(10,12)	
4	(11,6)		14	(5,18)	
5	(13,10)		15	(13,9)	
6	(5 ,1)		16	(11,13)	
7	(10 ,7)		17	(15,18)	
8	(16 ,13)		18	(7,5)	
9	(18 ,18)		19	(2,17)	
10	(0 ,0)		20	$\mathcal{O}$	

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2,2)$ is a generator.

Let $f(x,y) = x$.

$$e_n = \left(\frac{x(nG)}{19}\right)$$

n	nG	e_n
1	(2,2)	-1
2	(7,14)	+1
3	(15,1)	
4	(11,6)	
5	(13,10)	
6	(5 ,1)	
7	(10 ,7)	
8	(16 ,13)	
9	(18 ,18)	
10	(0 ,0)	

n	nG	e_n
11	(18 ,1)	
12	(16 ,6)	
13	(10,12)	
14	(5,18)	
15	(13,9)	
16	(11,13)	
17	(15,18)	
18	(7,5)	
19	(2,17)	
20	$\mathcal{O}$	

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = x$.

$$e_n = \left(\frac{x(nG)}{19} \right)$$

n	nG	e_n	n	nG	e_n
1	(2,2)	-1	11	(18 ,1)	
2	(7,14)	+1	12	(16 ,6)	
3	(15,1)	-1	13	(10,12)	
4	(11,6)		14	(5,18)	
5	(13,10)		15	(13,9)	
6	(5 ,1)		16	(11,13)	
7	(10 ,7)		17	(15,18)	
8	(16 ,13)		18	(7,5)	
9	(18 ,18)		19	(2,17)	
10	(0 ,0)		20	$\mathcal{O}$	

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = x$.

$$e_n = \left(\frac{x(nG)}{19} \right)$$

n	nG	e_n	n	nG	e_n
1	(2,2)	-1	11	(18 ,1)	-1
2	(7,14)	+1	12	(16 ,6)	+1
3	(15,1)	-1	13	(10,12)	-1
4	(11,6)	+1	14	(5,18)	+1
5	(13,10)	-1	15	(13,9)	-1
6	(5 ,1)	+1	16	(11,13)	+1
7	(10 ,7)	-1	17	(15,18)	-1
8	(16 ,13)	+1	18	(7,5)	+1
9	(18 ,18)	-1	19	(2,17)	-1
10	(0 ,0)	+1	20	$\mathcal{O}$	+1

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = x$.

$$e_n = \left(\frac{x(nG)}{19} \right)$$

Why E_{20} is *not* pseudorandom?

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2,2)$ is a generator.

Let $f(x,y) = x$.

$$e_n = \left(\frac{x(nG)}{19}\right)$$

Why E_{20} is *not* pseudorandom?
Let $nG = (x,y)$, then

$$e_n \cdot e_{n+10} = \left(\frac{f(nG)}{19}\right) \cdot \left(\frac{f((n+10)G)}{19}\right) = \left(\frac{f(nG) \cdot f(nG + 10G)}{19}\right)$$

$$= \left(\frac{f(nG) \cdot f(nG + (0,0))}{19}\right) = \left(\frac{x \cdot \left(\left(\frac{y}{x}\right)^2 - x\right)}{19}\right) = 1,$$

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = x$.

$$e_n = \left(\frac{x(nG)}{19} \right)$$

Why E_{20} is *not* pseudorandom?
Let $nG = (x, y)$, then

$$e_n \cdot e_{n+10} = \left(\frac{f(nG)}{19} \right) \cdot \left(\frac{f((n+10)G)}{19} \right) = \left(\frac{f(nG) \cdot f(nG + 10G)}{19} \right)$$

$$= \left(\frac{f(nG) \cdot f(nG + (0,0))}{19} \right) = \left(\frac{x \cdot \left(\left(\frac{y}{x} \right)^2 - x \right)}{19} \right) = 1,$$

since

$$x \cdot \left(\left(\frac{y}{x} \right)^2 - x \right) \equiv -2 \mod y^2 = x^3 - 2x \text{ over } \mathbb{F}_{19}$$

is a constant function!

Sequences generated from Elliptic Curves, example

Let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2,2)$ is a generator.

Let $f(x,y) = x$.

$$e_n = \left(\frac{x(nG)}{19}\right)$$

Why E_{20} is *not* pseudorandom?
Let $nG = (x,y)$, then

$$e_n \cdot e_{n+10} = \left(\frac{f(nG)}{19}\right) \cdot \left(\frac{f((n+10)G)}{19}\right) = \left(\frac{f(nG) \cdot f(nG+10G)}{19}\right)$$

$$= \left(\frac{f(nG) \cdot f(nG+(0,0))}{19}\right) = \left(\frac{x \cdot \left(\left(\frac{y}{x}\right)^2 - x\right)}{19}\right) = 1,$$

since

$$x \cdot \left(\left(\frac{y}{x}\right)^2 - x\right) \equiv -2 \mod y^2 = x^3 - 2x \text{ over } \mathbb{F}_{19}$$

is a constant function!
Thus the original sequence

$$n \longmapsto x(nG) \in \mathbb{F}_p,$$

is also not pseudorandom.

Sequences generated from Elliptic Curves, admissibility

In general: the $C_\ell(E_T)$ is small, if the function

$$F(P) = f(P + d_1 G) \dots f(P + d_\ell G) \in \mathbb{F}_p(\mathcal{E})$$

is *not* a square.

Sequences generated from Elliptic Curves, admissibility

In general: the $C_\ell(E_T)$ is small, if the function

$$F(P) = f(P + d_1 G) \dots f(P + d_\ell G) \in \mathbb{F}_p(\mathcal{E})$$

is *not* a square.

Definition

(k, ℓ, m) is a d-admissible triple, if there are no multisets $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ such that

- $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$
- *the number of solution of $a + b = c$, $a \in \mathcal{A}$, $b \in \mathcal{B}$ is divisible by d.*

Sequences generated from Elliptic Curves, admissibility

In general: the $C_\ell(E_T)$ is small, if the function

$$F(P) = f(P + d_1 G) \dots f(P + d_\ell G) \in \mathbb{F}_p(\mathcal{E})$$

is *not* a square.

Definition

(k, ℓ, m) is a d-admissible triple, if there are no multisets $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ such that

- $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$
- *the number of solution of $a + b = c$, $a \in \mathcal{A}$, $b \in \mathcal{B}$ is divisible by d.*

Let $k = |\operatorname{Supp}(f)|$, $m = p$, $d = 2$. If the triple $(\operatorname{Supp}(f), \ell, p)$ is 2-admissible, then the function F is *not* a square.
If

- $\mathcal{A}$: the multiset of the zeros and poles of f;
- $\mathcal{B} = \{d_1 G, \dots, d_\ell G\}$;
- F is a square,

then $a + b = c$ has even number of solution for each c.

Sequences generated from Elliptic Curves, general construction

Construction (Chen)

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$*, and* $f \in \mathbb{F}_p(\mathcal{E})$*, and let us define* $E_T = (e_1, \ldots, e_T)$ *by*

$$e_n = \begin{cases} \left(\frac{f(nG)}{p}\right) & \text{ha } f(nG) \neq 0, \mathcal{O}, \\ +1 & \text{ha } f(nG) = 0, \mathcal{O}. \end{cases}$$

Sequences generated from Elliptic Curves, general construction

Construction (Chen)

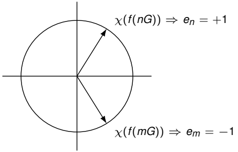
Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$, and $f \in \mathbb{F}_p(\mathcal{E})$, and let us define $E_T = (e_1, \ldots, e_T)$ by

$$e_n = \begin{cases} \left(\frac{f(nG)}{p}\right) & \text{ha } f(nG) \neq 0, \mathcal{O}, \\ +1 & \text{ha } f(nG) = 0, \mathcal{O}. \end{cases}$$

Construction (Mérai)

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$, and $f \in \mathbb{F}_p(\mathcal{E})$, χ is a multiplicative character of $\mathbb{F}_p$, and let us define $E_T = (e_1, \ldots, e_T)$ by

$$e_n = \begin{cases} +1 & \text{if } \arg\left(\chi(f(nG))\right) \in [0, \pi) \\ -1 & \text{otherwise.} \end{cases}$$



Sequences generated from Elliptic Curves, general construction

Theorem

If the order of G is T, and the order of χ *is d then*

$$W(E_T) \ll |\operatorname{Supp}(f)|p^{1/2}(1+\log T)\log d.$$

If the triple $(|\operatorname{Supp}(f)|, \ell, T)$ *is d-admissible, then*

$$C_\ell(E_T) \ll \ell 10^\ell |\operatorname{Supp}(f)|p^{1/2}(1+\log T)(\log d)^\ell.$$

Sequences generated from Elliptic Curves, general construction

Theorem

If the order of G is T, and the order of χ is d then

$$W(E_T) \ll |\operatorname{Supp}(f)| p^{1/2}(1 + \log T) \log d.$$

If the triple $(|\operatorname{Supp}(f)|, \ell, T)$ is d-admissible, then

$$C_\ell(E_T) \ll \ell 10^\ell |\operatorname{Supp}(f)| p^{1/2}(1 + \log T)(\log d)^\ell.$$

The proof is based on the notion of admissibility and an elliptic curve analogue of the Weil bound.

Sequences generated from Elliptic Curves, general construction

Theorem

If the order of G is T, and the order of χ is d then

$$W(E_T) \ll |\operatorname{Supp}(f)| p^{1/2}(1 + \log T) \log d.$$

If the triple $(|\operatorname{Supp}(f)|, \ell, T)$ is d-admissible, then

$$C_\ell(E_T) \ll \ell 10^\ell |\operatorname{Supp}(f)| p^{1/2}(1 + \log T)(\log d)^\ell.$$

The proof is based on the notion of admissibility and an elliptic curve analogue of the Weil bound.

Special cases:

- $d = 2$: Legendre symbol sequence over elliptic curves.

Sequences generated from Elliptic Curves, general construction

Theorem

If the order of G is T, and the order of χ is d then

$$W(E_T) \ll |\operatorname{Supp}(f)| p^{1/2}(1+\log T)\log d.$$

If the triple $(|\operatorname{Supp}(f)|, \ell, T)$ is d-admissible, then

$$C_\ell(E_T) \ll \ell 10^\ell |\operatorname{Supp}(f)| p^{1/2}(1+\log T)(\log d)^\ell.$$

The proof is based on the notion of admissibility and an elliptic curve analogue of the Weil bound.

Special cases:

- $d = 2$: Legendre symbol sequence over elliptic curves.
- $d = p - 1$: Chen, Xiao: Elliptic curve analogue of a construction of Gyarmati based on the discrete logarithm.

Admissibility

Theorem

Let $p(m)$ be the smallest prime factor of m. Then

- *If $k < p(m)$, then the triple $(k, 2, m)$ is d-admissible.*
- *If*

  $$(4\ell)^k < p(m),$$

  then (k, ℓ, m) is d-admissible.
- *If m is a prime, and each prime factor of d is primitive root modulo m, then (k, ℓ, m) is d-admissible.*

Note: It is enough to prove the theorem in the case when d is a prime number.

Proof of the admissibility I.

If there exist multisets $\mathcal{A}, \mathcal{B}$, such that

- $|\mathcal{A}| = k$, $|\mathcal{B}| = 2$;
- for each c if the equation $a + b = c$ has solution, then there are at least two.

Let $\mathcal{B} = \{r, r + s\}$ ($s \neq 0$).
Then each elements of $\mathcal{A} + r$ has at least two representations

So

$$|\mathcal{A}| = |\{a + r \mid a \in \mathcal{A}\}| = |\{a + r + s \mid a \in \mathcal{A}\}| = \\ = |\{a + r + st \mid a \in \mathcal{A}\}| \geq p(m),$$

since $\{a + r + st \mid a \in \mathcal{A}\}$ is a not-trivial co-set of $\mathbb{Z}_m$, which contradicts to the condition $k < p(m)$.

Proof of the admissibility III.

Let $p = m$, d be prime numbers.
For a given multiset $\mathcal{C} \subseteq \mathbb{Z}_p$ let

$$P_{\mathcal{C}}(x) = \sum_{c \in \mathcal{C}} x^{r_p(c)}.$$

(where $r_m(c)$ is the least non-negative residue of c modulo p.)

For a given $u \in \mathbb{Z}_p$ we have

$$P_{u+\mathcal{C}}(x) \equiv x^u \cdot P_{\mathcal{C}}(x) \mod x^p - 1 \text{ over } \mathbb{Z}_d.$$

In $\mathcal{A} + \mathcal{B}$ each element is represented in d ways if and only if

$$P_{\mathcal{A}}(x) \cdot P_{\mathcal{B}}(x) \equiv P_{\mathcal{A}+\mathcal{B}}(x) = 0 \mod x^p - 1 \text{ over } \mathbb{Z}_d.$$

So there are *no* multisets $\mathcal{A}, \mathcal{B}$ if the polinomial

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + 1$$

is irreducible over $\mathbb{Z}_d$, i.e. d is primitive root modulo p.

Sequences generated from Elliptic Curves

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$ (or at least an element with large order). Then

$$n \longmapsto x(nG) \in \mathbb{F}_p,$$

or in general

$$n \longmapsto f(nG) \in \mathbb{F}_p,$$

where $f \in \mathbb{F}_p(\mathcal{E})$.
In order to generate *binary* sequences we have to choose one of the bits of $f(nG)$:

Chen: $\quad n \mapsto \left(\frac{f(nG)}{p}\right)$

Liu, Zhan, Wang: $\quad n \mapsto \begin{cases} +1 & \text{if } f(nG) \in \{0, 1, 2 \ldots, \frac{p-1}{2}\} \\ -1 & \text{otherwise} \end{cases}$

Here $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo p.

An other construction

Construction

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$, and $f \in \mathbb{F}_p(\mathcal{E})$, and let us define $E_T = (e_1, \ldots, e_T)$ by

$$e_n = \begin{cases} +1 & f(nG) \in \{0, 1, 2, \ldots, \frac{p-1}{2}\} \\ -1 & \text{otherwise.} \end{cases}$$

An other construction

Construction

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$, and $f \in \mathbb{F}_p(\mathcal{E})$, and let us define $E_T = (e_1, \ldots, e_T)$ by

$$e_n = \begin{cases} +1 & f(nG) \in \{0, 1, 2, \ldots, \frac{p-1}{2}\} \\ -1 & \text{otherwise.} \end{cases}$$

Liu, Zhan, Wang:

- f is a "polynomial", i.e. the $\mathcal{O}$ is the only pole of f;
- $1/f$ is a "polynomial", i.e. the $\mathcal{O}$ is the only zero of f;

What can we say, when f is a general function?

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \ldots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \dots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

n	nG	$f(nG)$	e_n
1	(2,2)	9	
2	(7,14)	17	
3	(15,1)	16	
4	(11,6)	11	
5	(13,10)	6	
6	(5 ,1)	11	
7	(10 ,7)	16	
8	(16 ,13)	17	
9	(18 ,18)	9	
10	(0 ,0)	∞	

n	nG	$f(nG)$	e_n
11	(18 ,1)	9	
12	(16 ,6)	17	
13	(10,12)	16	
14	(5,18)	11	
15	(13,9)	6	
16	(11,13)	11	
17	(15,18)	16	
18	(7,5)	17	
19	(2,17)	9	
20	$\mathcal{O}$	∞	

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \dots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

n	nG	$f(nG)$	e_n
1	(2,2)	9	+1
2	(7,14)	17	
3	(15,1)	16	
4	(11,6)	11	
5	(13,10)	6	
6	(5 ,1)	11	
7	(10 ,7)	16	
8	(16 ,13)	17	
9	(18 ,18)	9	
10	(0 ,0)	∞	

n	nG	$f(nG)$	e_n
11	(18 ,1)	9	
12	(16 ,6)	17	
13	(10,12)	16	
14	(5,18)	11	
15	(13,9)	6	
16	(11,13)	11	
17	(15,18)	16	
18	(7,5)	17	
19	(2,17)	9	
20	$\mathcal{O}$	∞	

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \ldots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

n	nG	$f(nG)$	e_n
1	(2,2)	9	+1
2	(7,14)	17	-1
3	(15,1)	16	
4	(11,6)	11	
5	(13,10)	6	
6	(5 ,1)	11	
7	(10 ,7)	16	
8	(16 ,13)	17	
9	(18 ,18)	9	
10	(0 ,0)	∞	

n	nG	$f(nG)$	e_n
11	(18 ,1)	9	
12	(16 ,6)	17	
13	(10,12)	16	
14	(5,18)	11	
15	(13,9)	6	
16	(11,13)	11	
17	(15,18)	16	
18	(7,5)	17	
19	(2,17)	9	
20	$\mathcal{O}$	∞	

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \ldots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

n	nG	$f(nG)$	e_n
1	(2,2)	9	+1
2	(7,14)	17	-1
3	(15,1)	16	-1
4	(11,6)	11	
5	(13,10)	6	
6	(5 ,1)	11	
7	(10 ,7)	16	
8	(16 ,13)	17	
9	(18 ,18)	9	
10	(0 ,0)	∞	

n	nG	$f(nG)$	e_n
11	(18 ,1)	9	
12	(16 ,6)	17	
13	(10,12)	16	
14	(5,18)	11	
15	(13,9)	6	
16	(11,13)	11	
17	(15,18)	16	
18	(7,5)	17	
19	(2,17)	9	
20	$\mathcal{O}$	∞	

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \dots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

n	nG	$f(nG)$	e_n	n	nG	$f(nG)$	e_n
1	(2,2)	9	+1	11	(18 ,1)	9	+1
2	(7,14)	17	-1	12	(16 ,6)	17	-1
3	(15,1)	16	-1	13	(10,12)	16	-1
4	(11,6)	11	-1	14	(5,18)	11	-1
5	(13,10)	6	+1	15	(13,9)	6	+1
6	(5 ,1)	11	-1	16	(11,13)	11	-1
7	(10 ,7)	16	-1	17	(15,18)	16	-1
8	(16 ,13)	17	-1	18	(7,5)	17	-1
9	(18 ,18)	9	+1	19	(2,17)	9	+1
10	(0 ,0)	∞	-1	20	$\mathcal{O}$	∞	-1

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$
$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.
Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \ldots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

Why this sequence is *not* random?

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$

$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.

Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \ldots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

Why this sequence is *not* random?
The correlation measure $C_2(E_{20})$ is large:

$$e_n \cdot e_{n+10} = +1 \quad \text{for } n = 1, 2, \ldots, 10.$$

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$
$|\mathcal{E}| = 20$, $G = (2, 2)$ is a generator.
Let $f(x, y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0, 1, 2, \dots, 9\} \\ -1 & \text{otherwise.} \end{cases}$$

Why this sequence is *not* random?
The correlation measure $C_2(E_{20})$ is large:

$$e_n \cdot e_{n+10} = +1 \quad \text{for } n = 1, 2, \dots, 10.$$

By using additive character sums, it can be shown that the correlation measure of order ℓ is small, if none of the functions

$$F(P) = h_1 \cdot f(P + d_1 G) + \cdots + h_\ell \cdot f(P + d_\ell G) \quad (h_1, \dots, h_\ell) \in \mathbb{F}_p^\ell \setminus (0, \dots, 0)$$

are constant.

An other construction, an example

Again let $\mathcal{E} : y^2 = x^3 - 2x$ over $\mathbb{F}_{19}$
$|\mathcal{E}| = 20$, $G = (2,2)$ is a generator.
Let $f(x,y) = 9x + \frac{1}{x}$.

$$e_n = \begin{cases} +1 & 9x(nG) + \frac{1}{x(nG)} \in \{0,1,2,\dots,9\} \\ -1 & \text{otherwise.} \end{cases}$$

Why this sequence is *not* random?
The correlation measure $C_2(E_{20})$ is large:

$$e_n \cdot e_{n+10} = +1 \quad \text{for } n = 1,2,\dots,10.$$

By using additive character sums, it can be shown that the correlation measure of order ℓ is small, if none of the functions

$$F(P) = h_1 \cdot f(P + d_1 G) + \cdots + h_\ell \cdot f(P + d_\ell G) \quad (h_1,\dots,h_\ell) \in \mathbb{F}_p^\ell \setminus (0,\dots,0)$$

are constant.
But

$$f(P) - f(P+10G) = \left(9x + \frac{1}{x}\right) - \left(9\left(\left(\frac{y}{x}\right)^2 - x\right) + \frac{1}{\left(\frac{y}{x}\right)^2 - x}\right)$$
$$= \left(9x + \frac{1}{x}\right) - \left(9 \cdot \frac{-2}{x} + \frac{-1}{2}x\right) = 0$$

An other construction

Construction (Mérai)

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$, and $f \in \mathbb{F}_p(\mathcal{E})$, and let us define $E_T = (e_1, \ldots, e_T)$ by

$$e_n = \begin{cases} +1 & f(nG) \in \{0, 1, 2, \ldots, \frac{p-1}{2}\} \\ -1 & \text{otherwise.} \end{cases}$$

An other construction

Construction (Mérai)

Let G be a generator of $\mathcal{E}(\mathbb{F}_p)$, and $f \in \mathbb{F}_p(\mathcal{E})$, and let us define $E_T = (e_1, \dots, e_T)$ by

$$e_n = \begin{cases} +1 & f(nG) \in \{0, 1, 2, \dots, \frac{p-1}{2}\} \\ -1 & \text{otherwise.} \end{cases}$$

For general rational functions:

Theorem

If the order of G is T then

$$W(E_T) \ll |\operatorname{Supp}(f)| p^{1/2} \log p \log T.$$

If $p(T)$ is the least prime divisor of p and

- $|\operatorname{Supp}(f)| < p(T)$ *and* $\ell = 2$, *or*
- $(4|\operatorname{Supp}(f)|)^{\ell} < p(T)$,

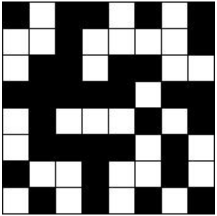
then

$$C_\ell(E_T) \ll \ell |\operatorname{Supp}(f)| p^{1/2} (\log p)^{\ell+1} \log T.$$

Extension of constructions to several dimensions

The extension of binary sequences in *several dimensions*, called *binary lattice*:

$$\eta : \{1, 2, \ldots, N\}^n \to \{+1, -1\}$$



We can define the analogue of the measures of pseudorandomness in several dimensions: $Q_\ell(\eta)$.

Application:

- encryption of several dimensions map or picture via the analogue of the Vernam cipher.

Constructions of binary lattices

Let $q = p^n$ be a prime power, $u_1, \ldots, u_n \in \mathbb{F}_q$ is a basis over $\mathbb{F}_p$. Let $f \in \mathbb{F}_q[x]$

Constructions of binary lattices

Let $q = p^n$ be a prime power, $u_1, \dots, u_n \in \mathbb{F}_q$ is a basis over $\mathbb{F}_p$. Let $f \in \mathbb{F}_q[x]$

- Huber, Mauduit, Sárközy:

$$\eta(x_1, \dots, x_n) = \chi_2\left(f(x_1 u_1 + \dots + x_n u_n)\right),$$

where χ_2 is the quadratic character over $\mathbb{F}_q$.

Constructions of binary lattices

Let $q = p^n$ be a prime power, $u_1, \dots, u_n \in \mathbb{F}_q$ is a basis over $\mathbb{F}_p$. Let $f \in \mathbb{F}_q[x]$

- Huber, Mauduit, Sárközy:

$$\eta(x_1, \dots, x_n) = \chi_2\left(f(x_1 u_1 + \dots + x_n u_n)\right),$$

  where χ_2 is the quadratic character over $\mathbb{F}_q$.

- Mérai:

$$\eta(x_1, \dots, x_n) = +1, \text{ if } \arg\Big(\chi\big(f(x_1 u_1 + \dots + x_n u_n)\big)\Big) \in [0, \pi),$$

  where χ is a general multiplicative character.

Constructions of binary lattices

Let $q = p^n$ be a prime power, $u_1, \dots, u_n \in \mathbb{F}_q$ is a basis over $\mathbb{F}_p$. Let $f \in \mathbb{F}_q[x]$

- Huber, Mauduit, Sárközy:

$$\eta(x_1, \dots, x_n) = \chi_2 \left(f(x_1 u_1 + \dots + x_n u_n) \right),$$

  where χ_2 is the quadratic character over $\mathbb{F}_q$.

- Mérai:

$$\eta(x_1, \dots, x_n) = +1, \text{ if } \arg \Big(\chi\big(f(x_1 u_1 + \dots + x_n u_n) \big) \Big) \in [0, \pi),$$

  where χ is a general multiplicative character.

- Mauduit, Sárközy:

$$\eta(x_1, \dots, x_n) = f^{-1}(x_1 u_1 + \dots + x_n u_n) \in B,$$

  where x^{-1} is the multiplicative inverse of x, $B \subset \mathbb{F}_q$.

Construction of binary lattice from elliptic curves

Definition

The points $P_1, \ldots, P_n \in \mathcal{E}$ are weakly independents if

$$\lambda_1 P_1 + \cdots + \lambda_n P_n = \mathcal{O} \Rightarrow \lambda_i P_i = \mathcal{O} \text{ for each } i = 1, \ldots, n.$$

Construction of binary lattice from elliptic curves

Definition

The points $P_1, \ldots, P_n \in \mathcal{E}$ are weakly independents if

$$\lambda_1 P_1 + \cdots + \lambda_n P_n = \mathcal{O} \Rightarrow \lambda_i P_i = \mathcal{O} \text{ for each } i = 1, \ldots, n.$$

Construction (Mérai)

Let $P_1, \ldots, P_n \in \mathcal{E}$ are weakly independent element, let us define η by

$$\eta(x_1, \ldots, x_n) = \begin{cases} \left(\frac{f(x_1 P_1 + \cdots + x_n P_n)}{p}\right) & \text{if } x_1 P_1 + \cdots + x_n P_n \neq \mathcal{O} \\ -1 & \text{otherwise.} \end{cases}$$

Construction of binary lattice from elliptic curves

Definition

The points $P_1, \ldots, P_n \in \mathcal{E}$ are weakly independents if

$$\lambda_1 P_1 + \cdots + \lambda_n P_n = \mathcal{O} \Rightarrow \lambda_i P_i = \mathcal{O} \text{ for each } i = 1, \ldots, n.$$

Construction (Mérai)

Let $P_1, \ldots, P_n \in \mathcal{E}$ are weakly independent element, let us define η by

$$\eta(x_1, \ldots, x_n) = \begin{cases} \left(\frac{f(x_1 P_1 + \cdots + x_n P_n)}{p} \right) & \text{if } x_1 P_1 + \cdots + x_n P_n \neq \mathcal{O} \\ -1 & \text{otherwise}. \end{cases}$$

Example

- If $\mathcal{E}$ is *not* cyclic, and $P, Q \in \mathcal{E}$ are the echelonized generators, then they are weakly independents.

Construction of binary lattice from elliptic curves

Definition

The points $P_1, \ldots, P_n \in \mathcal{E}$ are weakly independents if

$$\lambda_1 P_1 + \cdots + \lambda_n P_n = \mathcal{O} \Rightarrow \lambda_i P_i = \mathcal{O} \text{ for each } i = 1, \ldots, n.$$

Construction (Mérai)

Let $P_1, \ldots, P_n \in \mathcal{E}$ are weakly independent element, let us define η by

$$\eta(x_1, \ldots, x_n) = \begin{cases} \left(\frac{f(x_1 P_1 + \cdots + x_n P_n)}{p} \right) & \text{if } x_1 P_1 + \cdots + x_n P_n \neq \mathcal{O} \\ -1 & \text{otherwise.} \end{cases}$$

Example

- If $\mathcal{E}$ is *not* cyclic, and $P, Q \in \mathcal{E}$ are the echelonized generators, then they are weakly independents.
- If $P \in \mathcal{E}$, $|P| = \alpha_1 \ldots \alpha_n$ such that the numbers $\alpha_1 \ldots \alpha_n$ are pairwise co-prime, then the elements

  $$P_1 = \frac{|P|}{\alpha_1} P, \ldots, P_n = \frac{|P|}{\alpha_n} P$$

  are weakly independents.

Construction of binary lattice from elliptic curves

$$\eta(x_1, \dots, x_n) = \begin{cases} \left(\frac{f(x_1P_1+\cdots+x_nP_n)}{p}\right) & \text{if } x_1P_1 + \cdots + x_nP_n \neq \mathcal{O} \\ -1 & \text{otherwise.} \end{cases}$$

Theorem

Let $\mathcal{H}$ be the subgroup generated by $P_1, \dots, P_n$, $p(\mathcal{H})$ is the least prime divisor of $|\mathcal{H}|$. If

- $|\operatorname{Supp}(f)| < P(\mathcal{H})$ *and* $\ell = 2$*; or*
- $4^{n(|\operatorname{Supp}(f)|+\ell)} < p(\mathcal{H})$,

then

$$Q_\ell \ll_{n,\ell,f} p^{1/2+\varepsilon}.$$

Construction of binary lattice from elliptic curves

$$\eta(x_1,\ldots,x_n) = \begin{cases} \left(\frac{f(x_1P_1+\cdots+x_nP_n)}{p}\right) & \text{if } x_1P_1+\cdots+x_nP_n \neq \mathcal{O} \\ -1 & \text{otherwise.} \end{cases}$$

Theorem

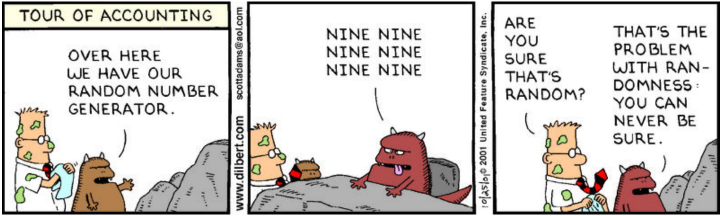
Let $\mathcal{H}$ be the subgroup generated by $P_1,\ldots,P_n$, $p(\mathcal{H})$ is the least prime divisor of $|\mathcal{H}|$. If

- $|\operatorname{Supp}(f)| < P(\mathcal{H})$ *and* $\ell = 2$; *or*
- $4^{n(|\operatorname{Supp}(f)|+\ell)} < p(\mathcal{H})$,

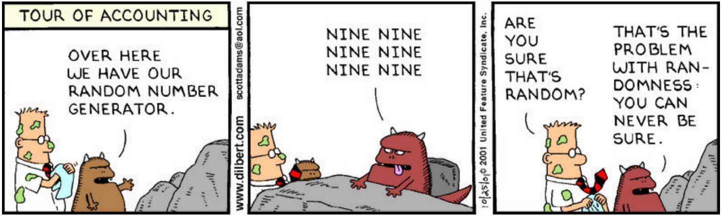
then

$$Q_\ell \ll_{n,\ell,f} p^{1/2+\varepsilon}.$$

- Good constructions can be defined with general multiplicative characters.
- The proof based on the notion of admissibility over general (not cyclic) Abelian group and character sum estimates over elliptic curves.


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
scottadams@aol.com
www.dilbert.com
10/25/01 © 2001 United Feature Syndicate, Inc.

Thank You!



TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RAN-DOMNESS: YOU CAN NEVER BE SURE.