Last time:

How random is $a \mapsto \bar{a}$ mod p

for $p \to \infty$. $\nu_p = \frac{1}{p-1} \sum_{a(p)}' \delta_{(\frac{a}{p}, \frac{\bar{a}}{p})}$ $\xrightarrow{\text{Ch.a.; weak-*}}$ μ = Haar. = Lebesgue on $\mathbb{T}^2$.

$C_c(\mathbb{T}^2)$

$\nu_p(f) = \int f d\nu_p = \langle \nu_p, f \rangle = \frac{1}{p-1} \sum_{a(p)}' f(\frac{a}{p}, \frac{\bar{a}}{p})$.

$\mathbb{T}^2 = (\mathbb{R}/\mathbb{Z})^2$

$(\mathbb{Z}/p)^2$

$\langle \nu_p, f \rangle = \frac{1}{p^2} \cdot \sum_{m,n(p)} \hat{\nu}_p(m,n) \cdot \overline{\hat{f}^p(m,n)}$,

$\hat{f}^p(m,n) = \sum_{a,b(p)} f(\frac{a}{p}, \frac{b}{p}) \overline{e(\frac{am+bn}{p})}$

$\hat{\nu}_p(m,n) = \frac{1}{p-1} \sum_{a(p)}' \overline{e_p(an+\bar{a}n)}$.

$\frac{1}{p^2} \hat{\nu}_p(0,0) \hat{f}^p(0,0) \to \mu(f)$.

$+ \frac{1}{p^2} \sum_{(m,n) \neq (0,0)} \cdots$ need $\to 0$.

$S(-m,-n;p)$ = Kloosterman sum

$(m,n) \neq (0,0)$, $\hat{\nu}_p(m,n) \ll p^{-1/4}$.

(modular analogue to K-Bessel). $\int e^{-y(u+1/u)} \cdots$

Need bounds for Kloosterman sum. Trivial bound:

$|S(m,n;p)| \le \sum_{a(p)}' 1 \le p-1$. Need capture cancellation in exponential sum.

Idea: embed in a family, take 2nd moment:

$|S(m,n;p)|^2 \le \sum_{k,l(p)} |S(k,l;p)|^2 = \sum_{k,l(p)} \left| \sum_{a(p)}' e_p(ak+\bar{a}l) \right|^2$.

open square:

$|\sum_a 1|^2 = \sum_a \sum_b 1 \cdot \bar{1}$.

$= \sum_{a,b(p)}' \sum_{k,l(p)} e_p(ak+\bar{a}l) e_p(-bk-\bar{b}l)$.

$= p^2 \cdot (p-1)$.

$p \cdot \mathbb{1}_{a \equiv b} \cdot p \cdot \mathbb{1}_{\bar{a} \equiv \bar{b}}$.

$\Rightarrow |S(m,n;p)| \ll p^{3/2}$. Worse than trivial.

Try 4th moment.

$$\sum_{f\in\mathcal{F}} |\hat{f}|^4 = \sum_{f\in\mathcal{F}} \left(|\hat{f}|^2\right)^2 = \sum_{g} |\hat{g}*\hat{g}|^2$$

$$|S(m,n;p)|^4 \le \sum_{k,l(p)} |S(k,l;p)|^4 = \sum_{a,b,c,d(p)} \sum_{k,l(p)} e_p(\underline{a}k+\bar{a}l)\, e_p(\underline{b}k+\bar{b}l)\, e_p(-\underline{c}k-\bar{c}l)\, e_p(-\underline{d}k-\bar{d}l).$$

Count # solutions to $\begin{cases} a+b=c+d \\ \bar{a}+\bar{b}=\bar{c}+\bar{d} \end{cases} \pmod p$.

$$p\cdot \mathbb{1}_{a+b\equiv c+d}\cdot p\cdot \mathbb{1}_{\bar{a}+\bar{b}=\bar{c}+\bar{d}}.$$

Fix a,b (p^2 choices) — need to count # $\begin{cases} c+d=f \text{ fixed} \\ \bar{c}+\bar{d}=g\bar{c} \end{cases}$ $\Leftrightarrow f=d+c=gcd$ $\Leftrightarrow \begin{cases} c+d=f \\ cd\equiv fg\bar{} := h \text{ fixed} \end{cases}$

- $a\neq -b$ ($\ll p^2$ choices)
  - $g\neq 0$, $p\neq 2$.
  - $g=0$, $c+d=0$. (choose c (p choices), d det'd.
- $a=-b$ (p choices).

$\to c(f-c)\equiv h \Rightarrow c^2-cf+h\equiv 0$.

$(c-f\cdot\bar{2})^2 - f^2\bar{4}+h \equiv c^2-cf+\cancel{f^2}\bar{\cancel{4}}+h\equiv 0$. $\Big\}$ ≤ 2 vals for c. $\Rightarrow d$ det'd.

$\to \#\text{Solns} \ll p\cdot p\cdot + p^2\cdot 1\cdot 1 \ll p^2$.

$$\Rightarrow |S(m,n;p)|^4 \le \sum_{k,l(p)} |S(k,l;p)|^4 \ll p^2\cdot p^2 = p^4$$

(sum all k,l once.)

$\Rightarrow |S(m,n;p)| \ll p$.

trivial!

Need to "adj" that $(m,n)\neq(0,0)$.

Say $m\neq 0$. Then

$$S(m,n;p) = \sum_{a(p)}{}' e_p(am+\bar{a}n) = \sum_{a(p)} e_p(ak+\bar{a}mk).$$

$a\mapsto a\cdot\bar{m}\cdot k$ $(k\neq 0)$. $= S(k,mk;p)$.

→ So $|S(m,n;p)|^4$ occurs with multiplicity $p-1$ in 4th moment! (Only true if at least one $\neq 0$).

$\frac{1}{p}\cdot|S(m,n;p)|^4 \ll p^4 \Rightarrow |S(m,n;p)| \ll p^{3/4} = p\cdot p^{-1/4}$

(Kloosterman 1927). (Weil 1948. $\ll p^{1/2}$).

Equidistribution: (4_4-sums). $\Rightarrow U_p \to M$ weak *.

Question: How random is modular multiplication, i.e. $a \mapsto a\cdot b \pmod p$. Graph $\left(\frac{a}{p}, \frac{ba}{p}\right)$ mod 1. If b generator. More generally, map $a \mapsto a\cdot b + c \bmod p$.

Linear congruential pseudorandom number generator.

If $c=0$, to get long as possible cycle, need $b=$ primitive root.

$1, b, b^2, b^3, \ldots, b^{p-1} \equiv 1$. ← randomness of this sequence is the discrete log problem (cryptosystems!).

Most naive test of a sequence is "serial correlation of pairs" $(b^k, b^{k+1}) \bmod p$.

Look at graph of $\left(\frac{a}{p}, \frac{ba}{p}\right) \in \pi^2$.

Took $p = 7919$ (1000th prime).

$b_1 = 5125$ root

$b_2 = 5128$ root

Why is this happening??? Look at slopes:

"partial quotients"

$$\frac{11}{17} \approx \frac{5125}{7919} = [0, 1, 1, 1, 5, \underbrace{28}_{\infty}, 1, 15, \cancel{\infty}] = 0 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}$$

$$\frac{5128}{7919} = [0, 1, 1, 1, 5, 6, 1, 3, 2, 7]$$

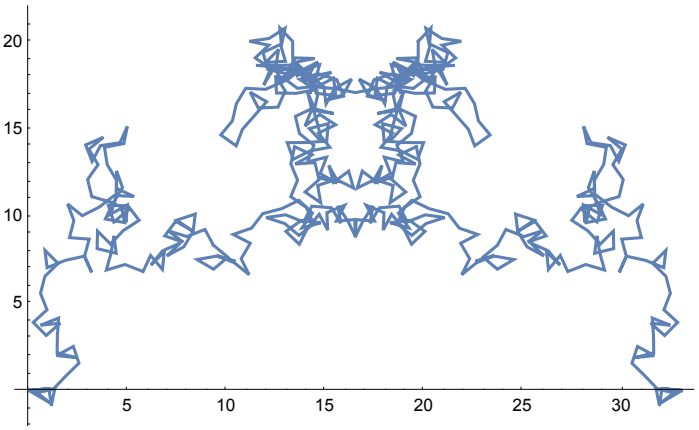
$$\text{flip}, \left\lfloor \frac{7919}{5125} \right\rfloor = 1, \left\lfloor \frac{7919 - 5125}{5125} \right\rfloor, \left\lfloor \frac{1}{0} \right\rfloor = \infty.$$

Looked at $\dfrac{f_n}{f_{n+1}} = [0, 1, \ldots, 1]$.

In[1]:=
```
m = 2 ; n = 9; p = Prime[100]
ListLinePlot[ReIm /@ Table[
   Sum[Exp[2 Pi I ( a m + PowerMod[a, -1, p] n) / p], {a, 1, b}]
   ,
   {b, 0, p - 1}]]
Sum[Exp[2 Pi I ( a m + PowerMod[a, -1, p] n) / p], {a, 1, p - 1}] // N
Sqrt[p] // N
```

Out[1]= 541

Out[2]=



Out[3]= 32.9874 + 0. i

Out[4]= 23.2594

In[5]:=
```
p = Prime[1000]
```

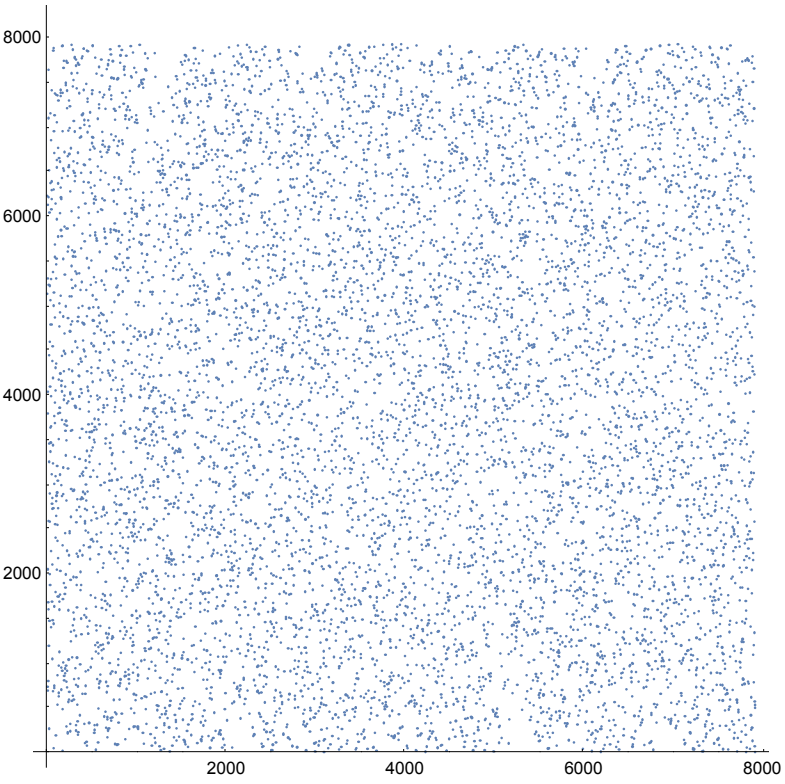
Out[5]= 7919

In[6]:=
```
PowerMod[root = 5125, (p - 1) / 2, p]
```

Out[6]= 7918

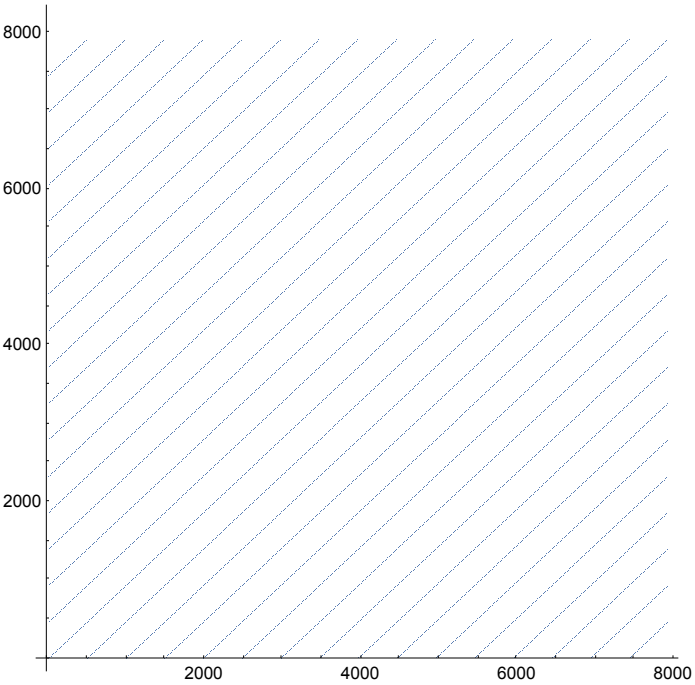
In[7]:=
```
ListPlot[Table[{k, PowerMod[root, k, p]}, {k, 1, p - 1}], AspectRatio → Automatic]
```

Out[7]=



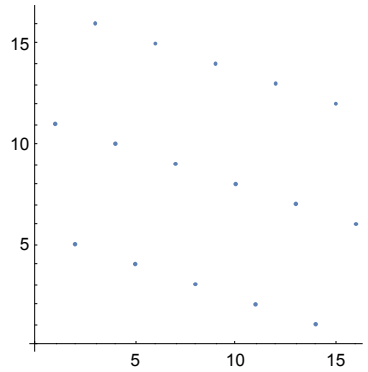
In[8]:=
```
ListPlot[Table[{k, Mod[k root, p]}, {k, 1, p - 1}], AspectRatio → Automatic]
```

Out[8]=



In[9]:=
```
ListPlot[Table[{k, Mod[k 11, 17]}, {k, 1, 17 - 1}], AspectRatio → Automatic]
```

Out[9]=

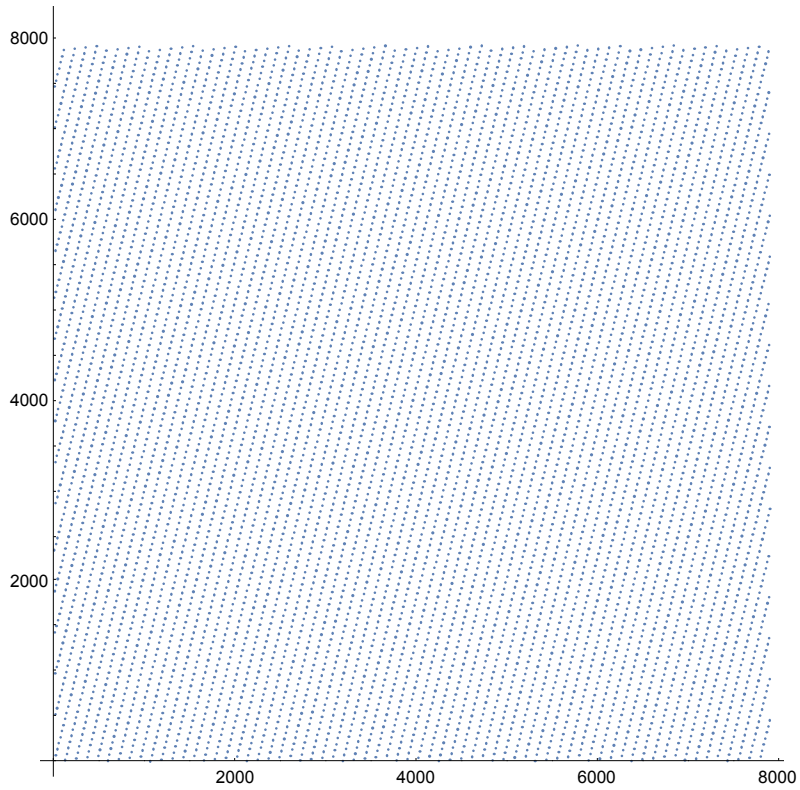


In[10]:=
```
PowerMod[root = 5128, (p - 1) / 2, p]
```

Out[10]= 7918

In[11]:=
```
ListPlot[Table[{k, Mod[k root, p]}, {k, 1, p - 1}], AspectRatio → Automatic]
```

Out[11]=



In[12]:=
```
ContinuedFraction[5125 / 7919]
```

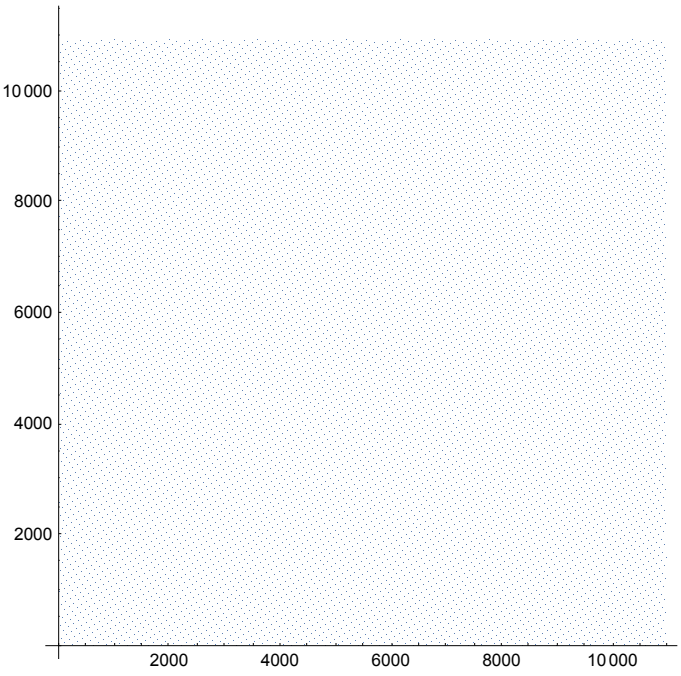
Out[12]= {0, 1, 1, 1, 5, 28, 1, 15}

In[13]:=
```
ContinuedFraction[5128 / 7919]
```

Out[13]= {0, 1, 1, 1, 5, 6, 1, 3, 2, 7}

In[14]:=
```
ListPlot[Table[{k, Mod[k Fibonacci[20], Fibonacci[21]]}, {k, 1, Fibonacci[21] - 1}],
 AspectRatio → Automatic]
```

Out[14]=



In[15]:=
```
ContinuedFraction[Fibonacci[20] / Fibonacci[21]]
```

Out[15]=
```
{0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2}
```

In[16]:=
```
FromContinuedFraction[{0, 1, 1, 1, 5}]
```

Out[16]=
$$\frac{11}{17}$$