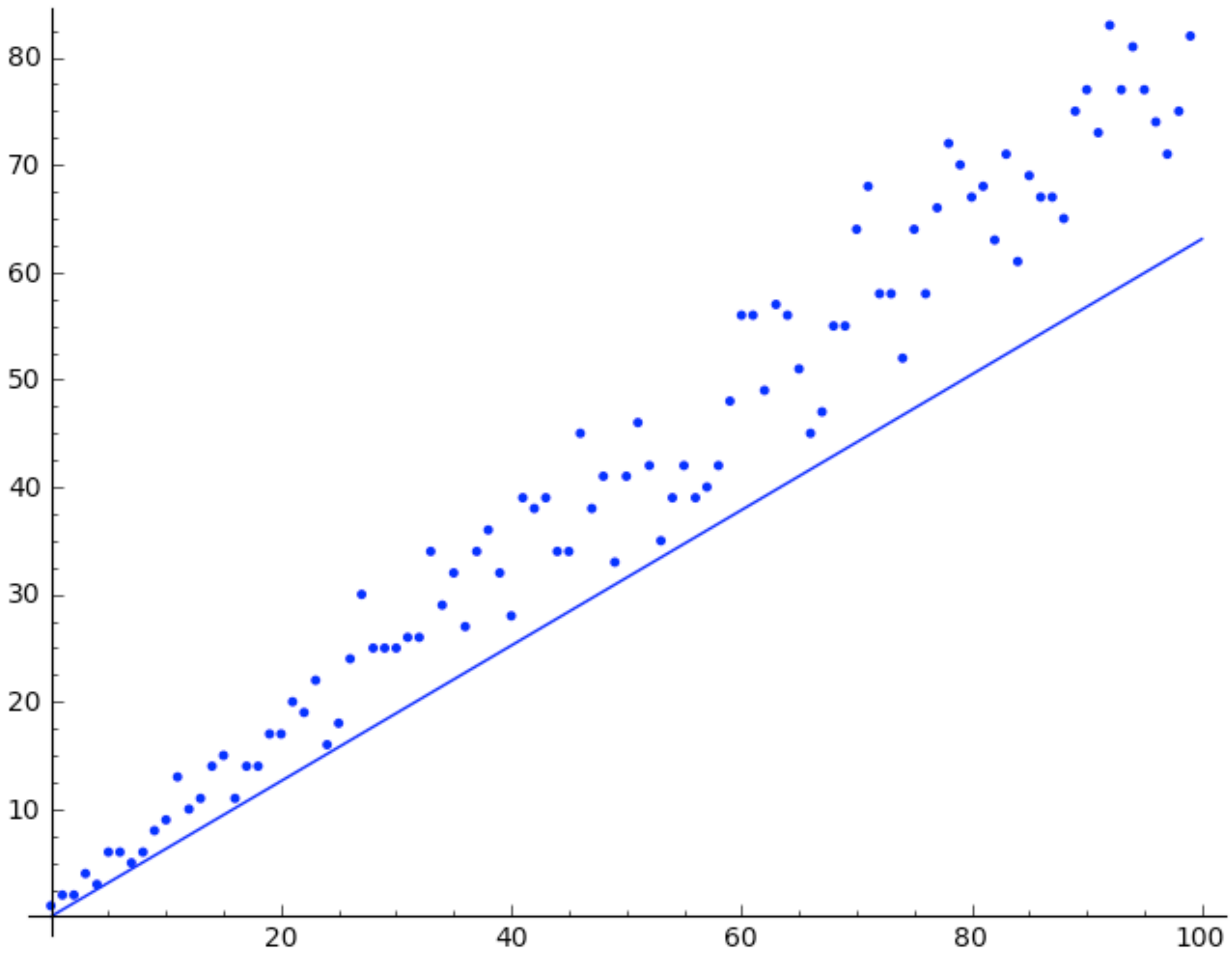
# Bits of powers of three in binary

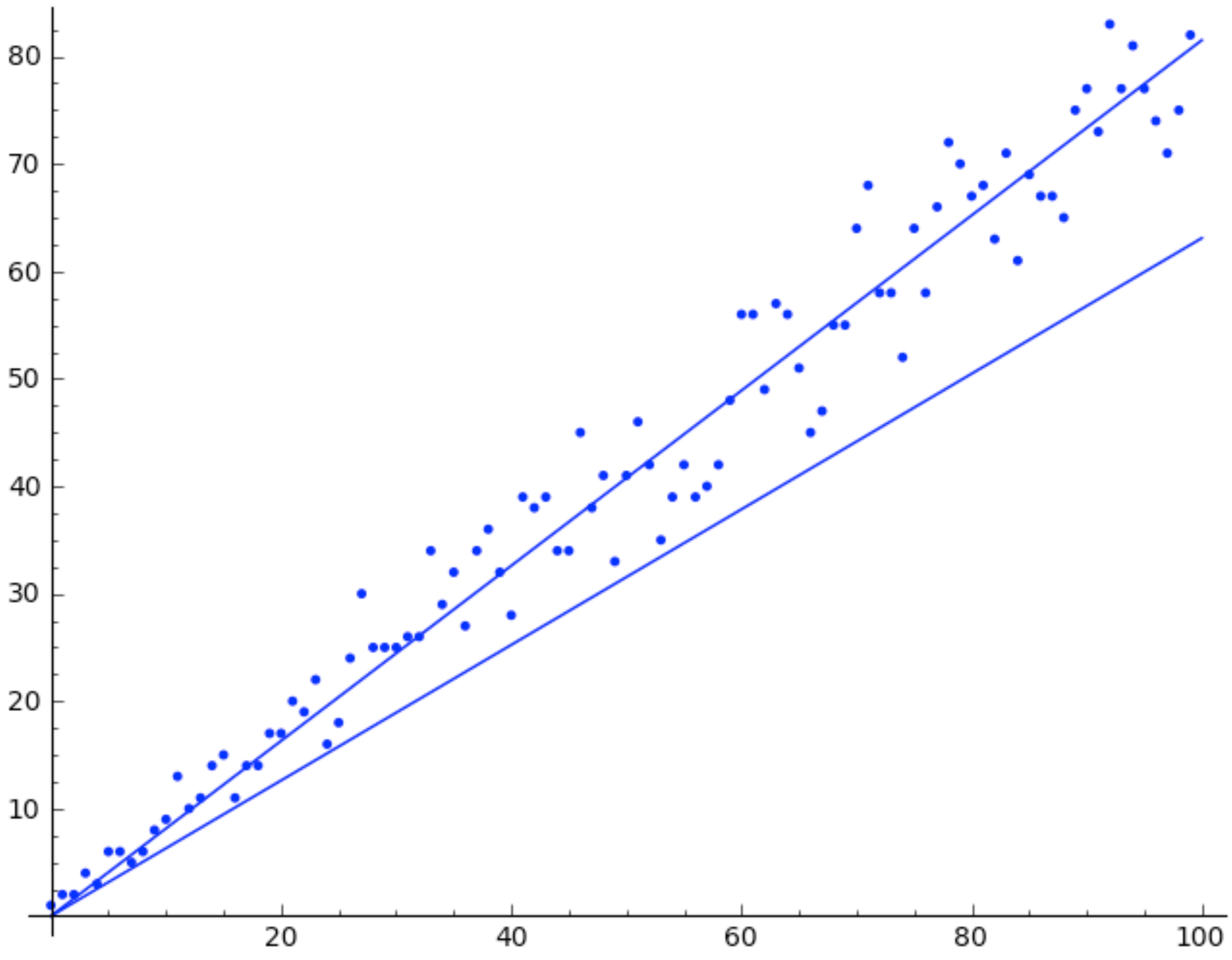
Taylor Dupuy (w/ D. Weirich)
West Coast Number Theory Seminar

- Cris Moore: Can one find a “formula” for the number of ones of $3^n$ in binary?

# Some Computations:



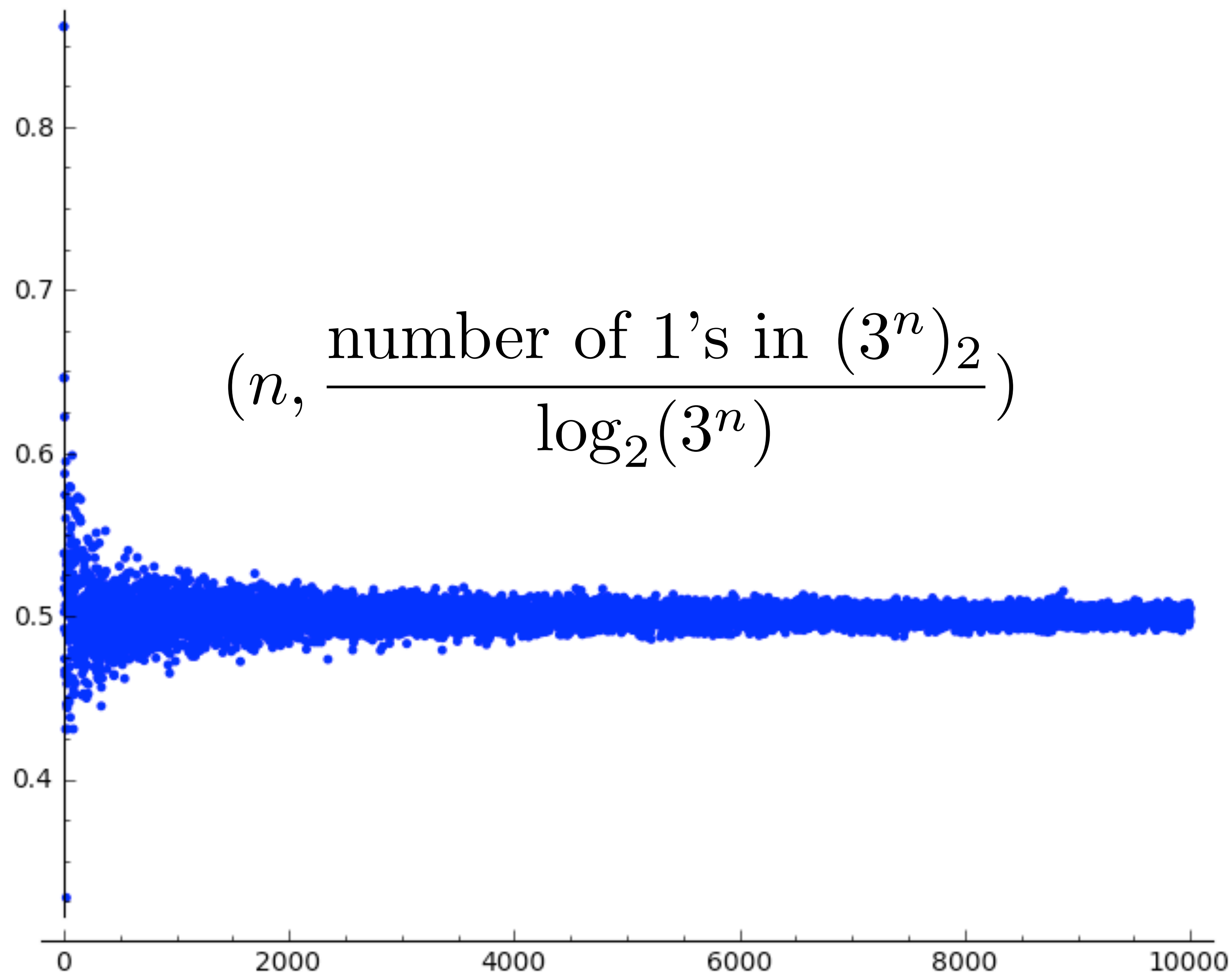

$$(n, \text{number of 1's in } (3^n)_2)$$

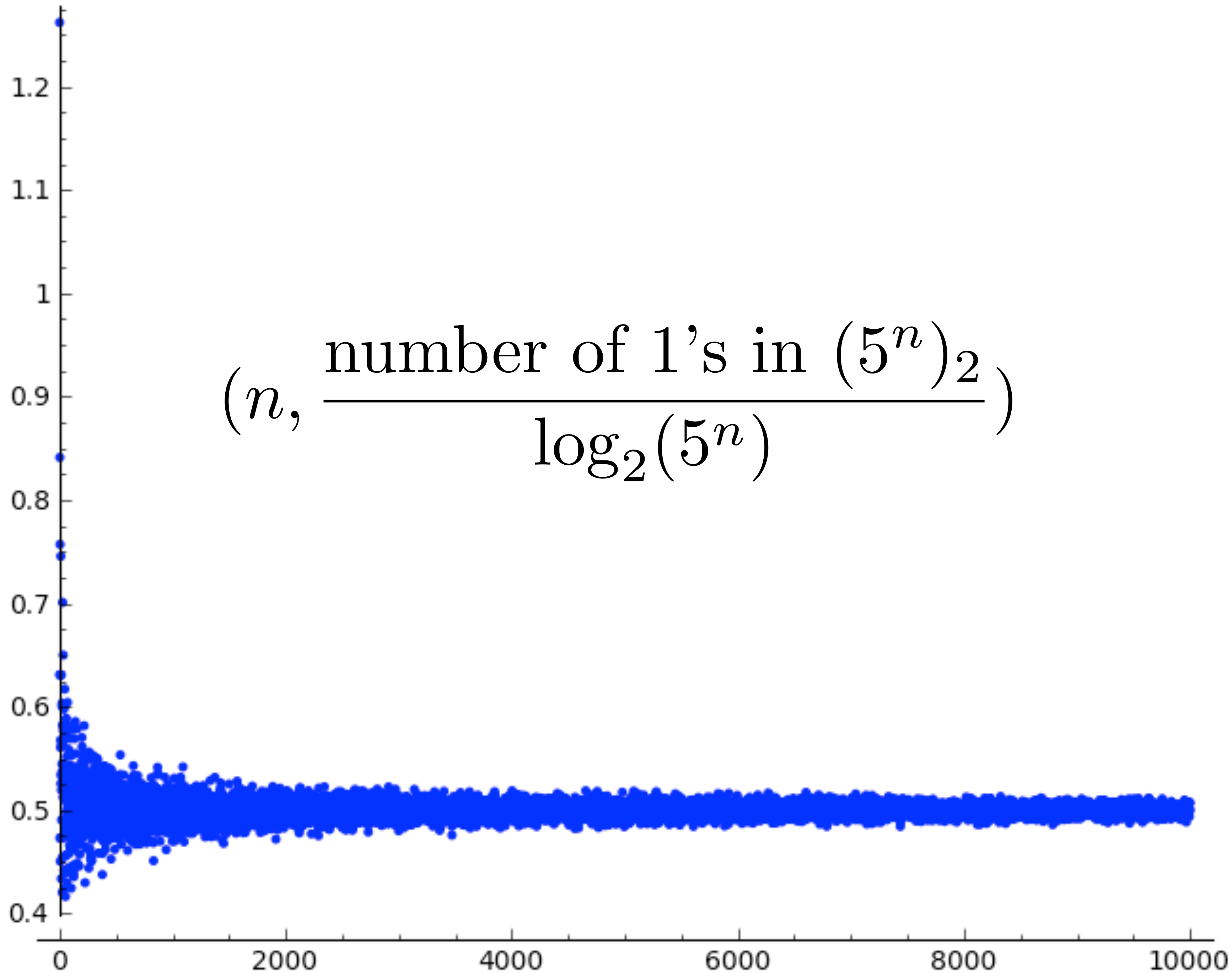



$$y = mx$$

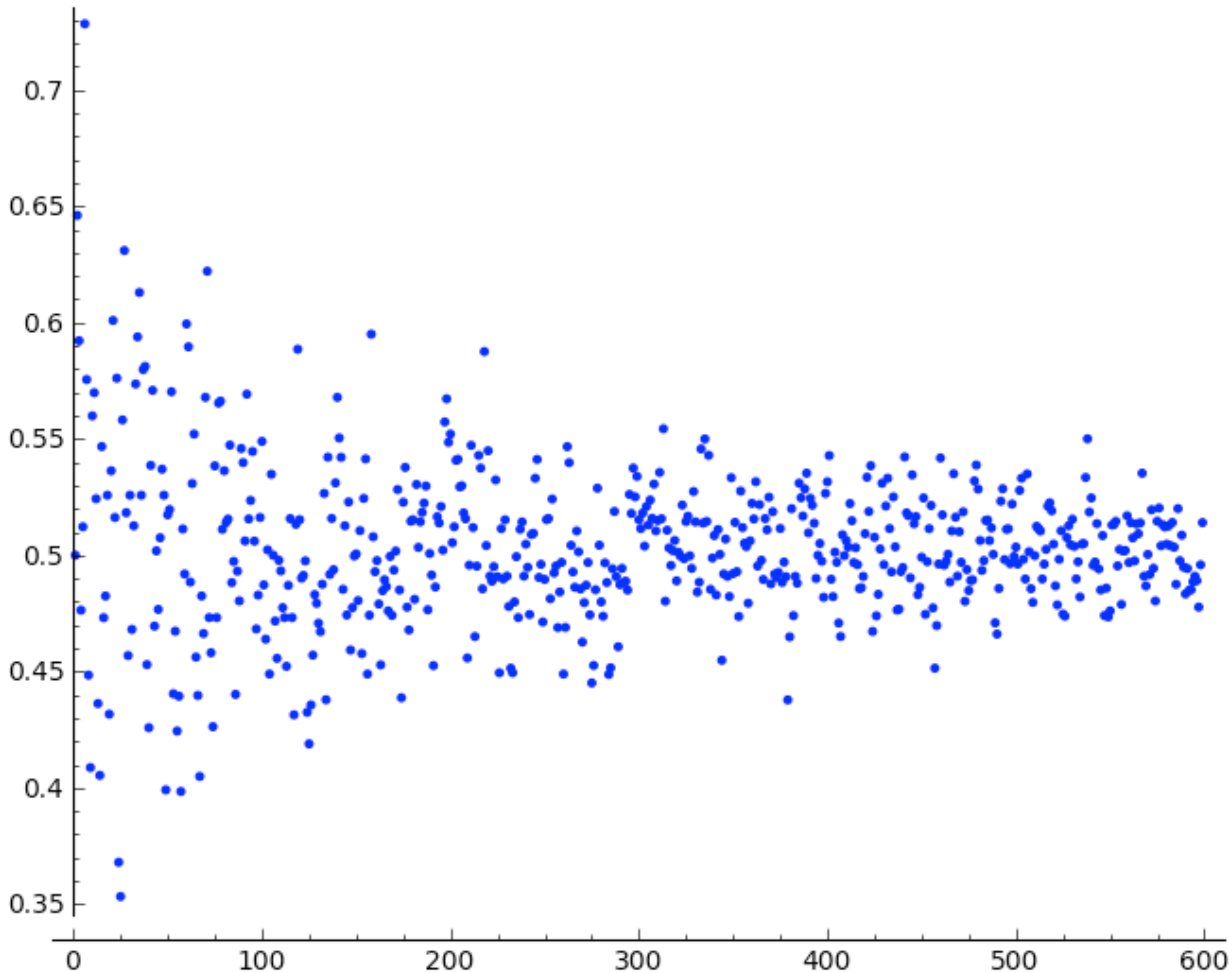
$$m = 0.3151\ldots$$

# proportion of 1's in the binary expansion

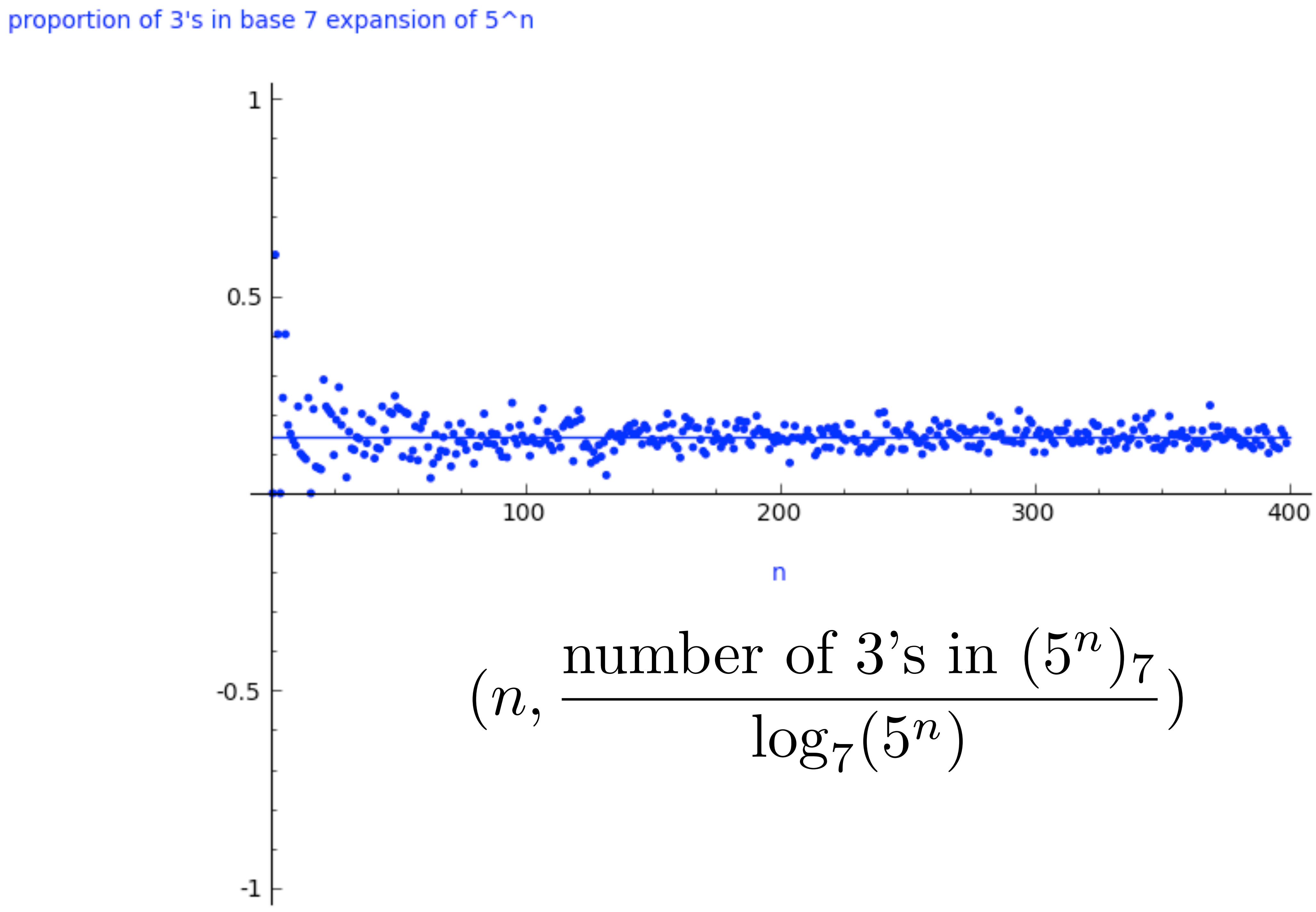




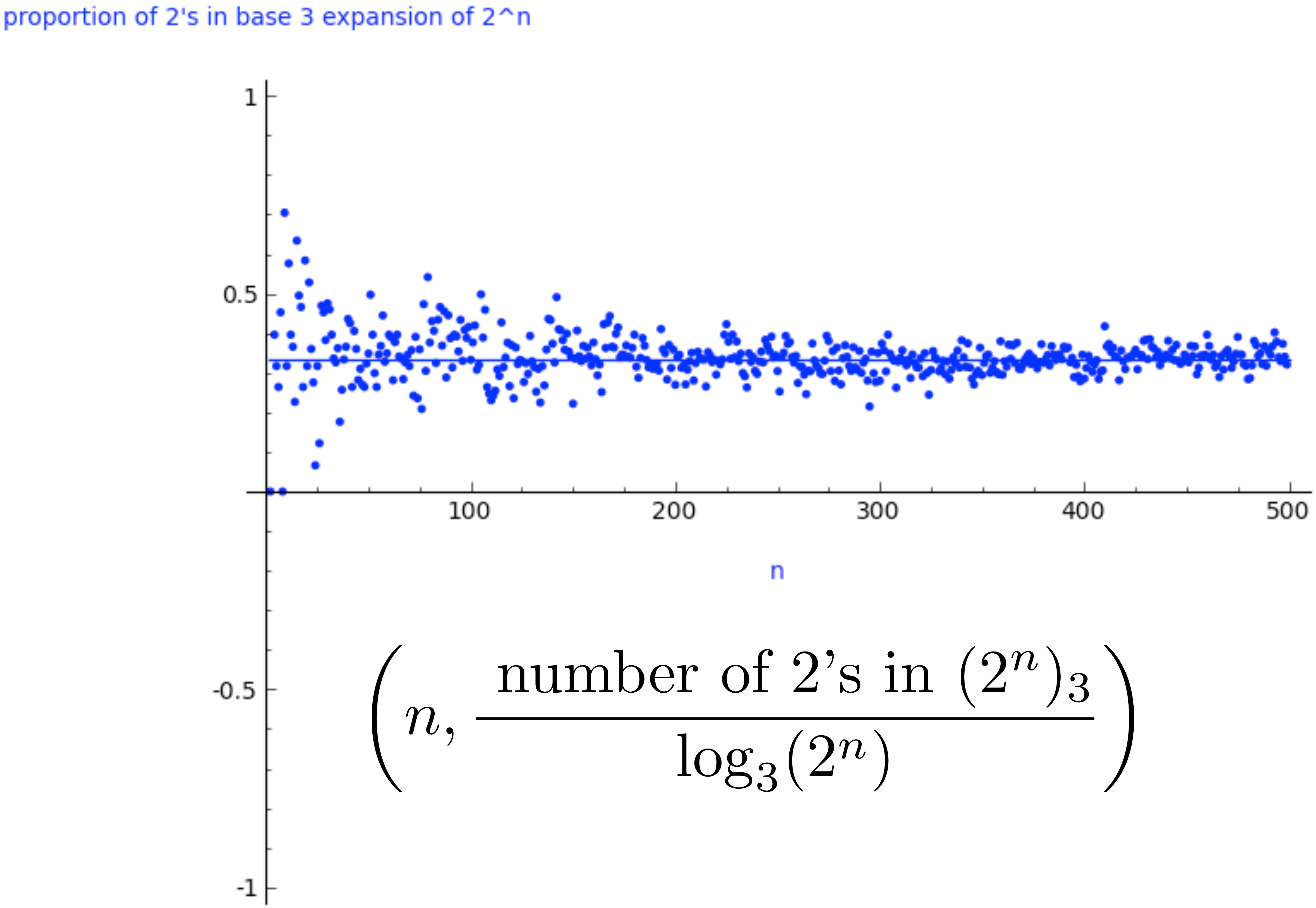
$(n, \frac{\text{number of 1's in } (5^n)_2}{\log_2(5^n)})$
1.2
1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0
2000
4000
6000
8000
10000



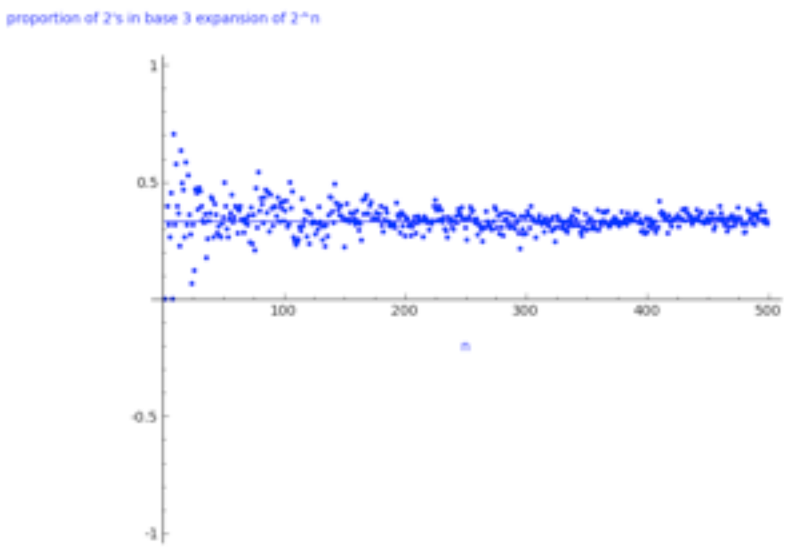

$$\left(n, \frac{\text{number of 1's in } (3^n + n^4)_2}{\log_2(3^n + n^4)}\right)$$




$$(n, \frac{\text{number of 3's in } (5^n)_7}{\log_7(5^n)})$$




$$\left(n, \frac{\text{number of 2's in } (2^n)_3}{\log_3(2^n)}\right)$$

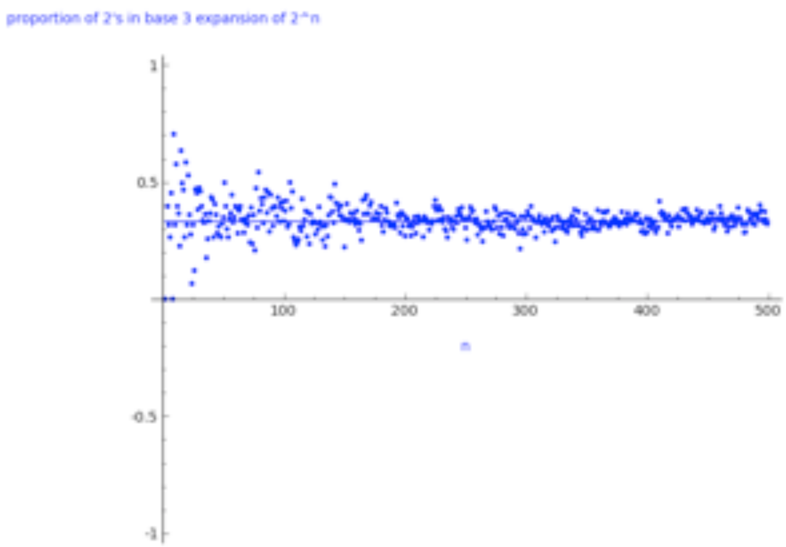



$$\left(n, \frac{\text{number of 2's in } (2^n)_3}{\log_3(2^n)}\right)$$

$$d_n = \text{ number of 2's in } (2^n)_3$$

**Data Says:**

$$\lim_{n\to\infty} \frac{d_n}{\log_3(2^n)} = \frac{1}{3}$$




$$\left(n, \frac{\text{number of 3's in } (2^n)_3}{\log_3(2^n)}\right)$$

$$\lim_{n\to\infty} \frac{d_n}{\log_3(2^n)} = \frac{1}{3}$$

**Erdos (1979):**

$X >> 0$ implies $N(X) = 0$

$$N(X) := \#\{n \leq X : (3^n)_2 \text{ omits a } 2\}$$

# Previous Work:

$$N(X) := \#\{n \le X : (3^n)_2 \text{ omits a } 2\}$$

Narkiewicz (1980):

$$N(X) \le \beta_0 X^{\alpha_0}$$

$$\beta_0 = 1.62\ldots$$

$$\alpha_0 = \log_3(2) \approx 0.6309$$

Lagarias (2009):

$$N(X) \le \beta_1 X^{\alpha_1}$$

$\beta_1, \alpha_1$ (explicit)

(more general)

Rem: bounds of this type can't give conj

# General Setup:

$$p = \text{ prime}$$

$$q = \text{ prime}$$

$$a \in \{0, \ldots, q-1\}$$

$$d_n = \text{ number of } a\text{'s in } (p^n)_q$$

$$d_{n,m} = \text{ number of } a\text{'s in first } m \text{ bits}$$

$$\frac{d_{n,m}}{m}$$ = proportion ...

$$d_{n,m} = \text{ number of } a\text{'s in first } m \text{ bits}$$

# Two considerations

1) $m = \lceil \log_q(p^n) \rceil$

$$\frac{d_{n,m}}{m} \sim \frac{d_n}{\log_q(p^n)}$$

2) average

$$\frac{d_n}{\log_q(p^n)} \approx \frac{1}{N}\sum_{n=1}^{N}\frac{d_{n,m}}{m}$$

$$d_{n,m} = \text{ number of } a\text{'s in first } m \text{ bits}$$

**Prop (D., Weirich)** *

1)
$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{d_{n,m}}{m} = A(m)$$

2)
$$\lim_{m\to\infty} A(m) = \frac{1}{q}$$

$$\left( \quad A(m) = \frac{1}{q} \quad \right)$$

Rem. If $\lim_{n\to\infty} \frac{d_n}{\log_q(p^n)}$ exists limit the same example: p = 3, q = 2

| | | |
|---|---|---|
| 1 | 1 | |
| 11 | 3 | |
| 1001 | 9 | powers of 3 in binary |
| 11011 | 27 | |
| 1010001 | 81 | |

* first m bits are periodic
* period is the order of 3 mod 2^m

* first m bits are periodic
* period is the order of 3 mod 2^m

$$(\text{ first } m \text{ bits of } p^n) = (\text{image of } p^n \text{ in } \mathbf{Z}/q^m)$$

$$H_m = \text{ group generated by } p \text{ in } (\mathbf{Z}/q^m)^\times$$

$$h_m = \#H_m = \text{ order of } p \text{ mod } q^m$$

**Lemma.**

$$\lim_{N\to\infty} \sum_{n=1}^{\infty} \frac{d_{n,m}}{m} = \frac{1}{h_m} \sum_{n=1}^{h_m} \frac{d_{n,m}}{m}$$

$$d_{n,m} = \text{ number of } a\text{'s in first } m \text{ bits}$$

# Let's compute using the formula: $\lim_{N\to\infty}\sum_{n=1}^{\infty}\frac{d_{n,m}}{m} = \frac{1}{h_m}\sum_{n=1}^{h_m}\frac{d_{n,m}}{m}$

$$
\begin{aligned}
A(m) &= \frac{1}{h_m}\sum_{n-1}^{h_m}\frac{d_{n,m}}{m} \\
&= \frac{1}{mh_m}\sum_{b=1}^{h_m} d_{n,m} \\
&= \frac{t(m)}{mh_m}
\end{aligned}
$$

$$
\begin{aligned}
t(m) &= \sum_{n=1}^{h_m} d_{n,m} \\
&= \text{total \# of bits equal to 1 varying over } H(m)
\end{aligned}
$$

**Lemma.**

$$A(m) = \left(1 - \frac{1}{m}\right) A(m-1) + \frac{1}{(q-1)qm}(k_m - 1)$$

$k_m = q$ or $1$

$$\ker((\mathbf{Z}/q^{m+1})^\times \to (\mathbf{Z}/q^m)^\times) = \mathbf{Z}/q$$

$$K_m := \ker(H_m \to H_{m-1}) \leq \mathbf{Z}/q$$

$$\#K_m := k_m$$

typical elt of kernel

$$1 + a \cdot q^m \mod q^{m+1}$$

$$a \in \{0, 1, \ldots, q-1\}$$

$$K_m = \mathbf{Z}/q \qquad \Longrightarrow \qquad aw_{n-1}$$

$$K_m = 1 \qquad \Longrightarrow \qquad 0w_{n-1}$$

**Lemma.**

$$A(m) = \left(1 - \frac{1}{m}\right) A(m-1) + \frac{1}{(q-1)qm}(k_m - 1)$$

Proof: By induction and cases

$K_m = \mathbf{Z}/q$ $\quad k_m = q$ $\quad$ more equally distributed

$aw_{n-1}$

$K_m = 1$ $\quad k_m = 1$ $\quad$ same bit distribution as before

$0w_{n-1}$

$$A(m) = \left(1 - \frac{1}{m}\right) A(m-1) + \frac{1}{(q-1)qm}(k_m - 1)$$

**notation:**

$$\bar{k}_n = k_n - 1$$

$$\bar{k}_1 := q - 1$$

**Lemma:**

$$A(n) = \frac{1}{q(q-1)} \frac{\bar{k}_1 + \cdots + \bar{k}_n}{n}$$

**point:**

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \frac{d_{n,m}}{m} = A(m)$$

$$d_{n,m} = \text{ number of } a\text{'s in first } m \text{ bits}$$

$$A(m) = \left(1 - \frac{1}{m}\right) A(m-1) + \frac{1}{(q-1)qm}(k_m - 1) \longrightarrow A(n) = \frac{1}{q(q-1)} \frac{\bar{k}_1 + \cdots + \bar{k}_n}{n}$$

$$\begin{aligned}
A(n+1) &= \frac{n}{n+1} A(n) + \frac{\bar{k}_{n+1}}{q(q-1)(n+1)} \\
&= \frac{1}{q(q-1)(n+1)} + \frac{\bar{k}_{n+1}}{q(q-1)(n+1)} \\
&= \frac{1}{q(q-1)(n+1)} [\bar{k}_1 + \cdots + \bar{k}_n] + \frac{\bar{k}_{n+1}}{q(q-1)(n+1)} \\
&= \frac{1}{q(q+1)} \frac{\bar{k}_1 + \cdots + \bar{k}_n}{n+1}
\end{aligned}$$

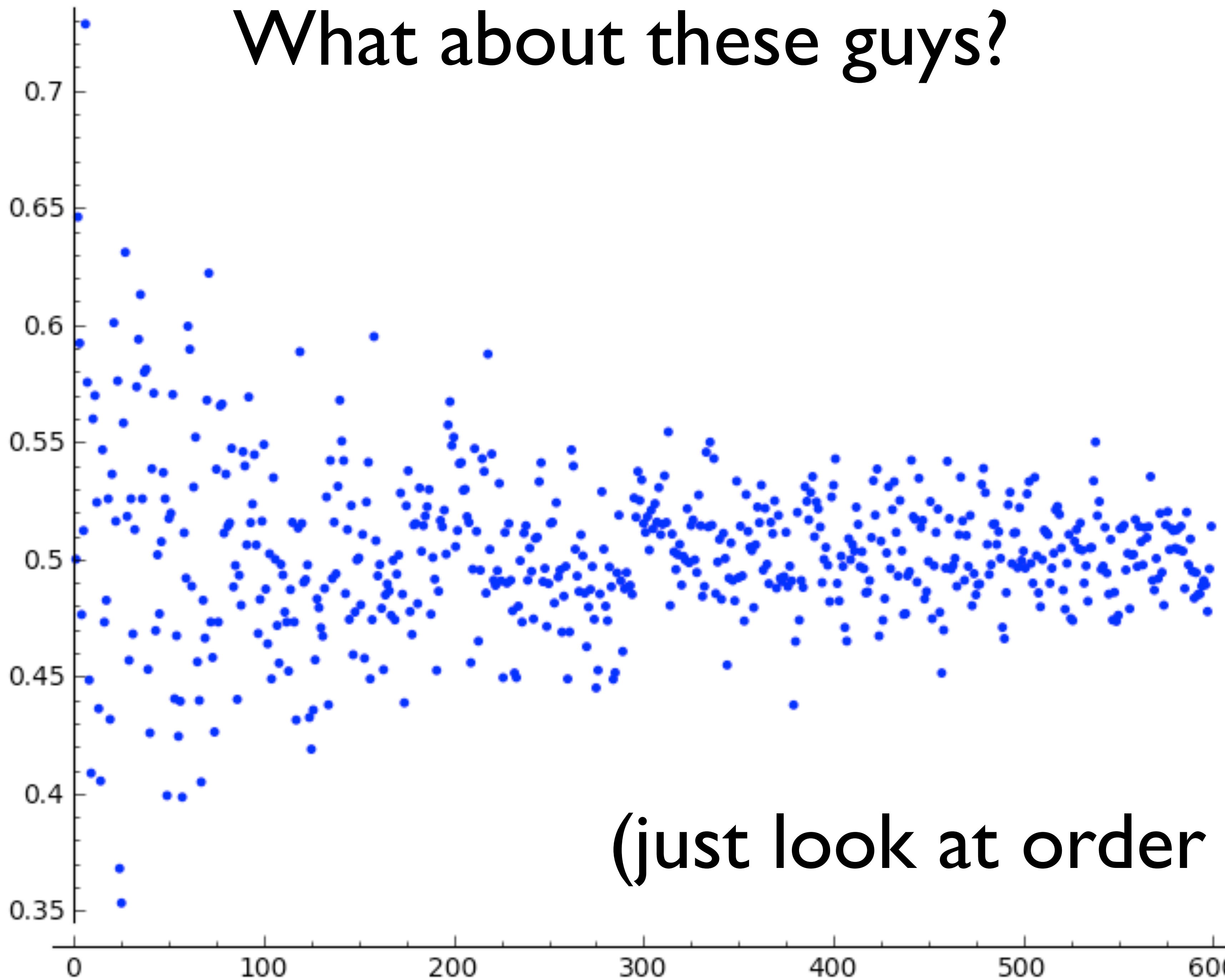
$$A(n) = \frac{1}{q(q-1)} \frac{\bar{k}_1 + \cdots + \bar{k}_n}{n}$$

Corollary:

$$A = 1/q \iff \lim_{n\to\infty} \frac{1}{n(q-1)} \sum_{j=1}^{n} \bar{k}_j = 1$$

Reduces to studying $\langle p \rangle$ inside $(\mathbf{Z}/q^m)^\times$

# What about these guys?




(just look at order of growth)

$$\left(n, \frac{\text{number of 1's in } (3^n + n^4)_2}{\log_2(3^n + n^4)}\right)$$