On a problem of Erdős concerning the digits of 2^n in base 3 – and Hensel's lemma

Thomas Stoll

CIRM, 08/11/2019

in memoriam Christian Mauduit

joint work with H. Kaneko (Tsukuba, Japan)

Université de Lorraine / Institut Élie Cartan de Lorraine

Motivation - original problem

Erdős squarefree conjecture

Erdős squarefree conjecture: The central binomial coefficient $\binom{2n}{n}$ is never squarefree for $n > 4$.

Erdős squarefree conjecture

Erdős squarefree conjecture: The central binomial coefficient $\binom{2n}{n}$ is never squarefree for $n > 4$.

Solved.

Proved :

- by Sarkőzy (1985) for all sufficiently large n and,
- independently, by Granville and Ramaré (1996) and Velammal (1995) for all $n > 4$.

Since $4 \mid \binom{2n}{n}$ for $n \neq 2^k$ it is sufficient to study $\binom{2^{k+1}}{2^k}$.

Erdős squarefree conjecture'

Erdős squarefree conjecture' : The central binomial coefficient $\binom{2n}{n}$ is divisible by 4 or 9 for every $n > 4$ except $n = 64$ and $n = 256$.

Erdős squarefree conjecture'

Erdős squarefree conjecture' : The central binomial coefficient $\binom{2n}{n}$ is divisible by 4 or 9 for every $n > 4$ except $n = 64$ and $n = 256$.

Unsolved !

- Goetgheluck (1988): True for $n \leq 2^{4.2 \cdot 10^7}$.
- Holdum, Klausen, and Rasmussen (2015) : True for $n \leq 2^{10^{13}}$; the set of k such that 9 does not divide $\binom{2^{k+1}}{2^k}$ is of density 0.

Some Unconventional Problems in Number Theory

A mélange of simply posed conjectures with frustratingly elusive solutions.

Paul Erdös
Hungarian Academy of Sciences
University of Colorado
Boulder, CO 80309

I state some curious, unusual, and mostly unsolved problems in various branches of number theory.

Factorial Powers

1. Put $f(n)=\Sigma(1/p)$ for $p<n$ and $p\nmid\binom{2n}{n}$. In a previous paper [6] written with Graham, Ruzsa and Straus, we conjectured that there is an absolute constant C so that for all $n, f(n)<C$. I further conjectured for $n>4$, $\binom{2n}{n}$ is never squarefree. It is surprising that this simple conjecture presents so many difficulties.

Since $\binom{2n}{n}\equiv 0 \pmod 4$ except if $n=2^k$, we "only" have to prove that $\binom{2^{k+1}}{2^k}$ is divisible by the square of an odd prime for $k\geqslant 3$. But this does not seem easy. I conjecture that for $k>8$, 2^k is not the sum of distinct powers of 3. (However, $2^8=256=3^5+3^2+3+1$.) This conjecture would imply that for $k\geqslant 9$ $\binom{2^{k+1}}{2^k}\equiv 0 \pmod 3$, but as far as I see there is no method at our disposal to attack this conjecture. There is no doubt that for $n>n_0(k,\alpha)$, $\binom{2n}{n}\equiv 0 \pmod{p^\alpha}$ for some $p>k$. For $p>2, p^2\nmid\binom{342}{171}$ and there is a good chance that this is the greatest $\binom{2n}{n}$ with this property. In other words, for $n>171$, the number $\binom{2n}{n}$ is perhaps divisible by the square of an odd prime.

2. Let $M(n;k)=[n+1,\ldots,n+k]$ be the least common multiple of the integers $n+i$ for $1\leqslant i\leqslant k$. I conjecture that for $m\geqslant n+k, M(n;k)\neq M(m;k)$, or more generally for $l\geqslant k$ and $m\geqslant n+k, M(n;k)\neq M(m;l)$. Unfortunately, I do not see any method to attack these very attractive conjectures. Probably $M(n;k)=M(m;l)$ has very few solutions when $m\geqslant n+k$ and $l>1$. I only know $M(4;3)=M(13;2)$ and $M(3;4)=M(19;2)$. If, similarly, we put $A(n;k)=\Pi_{i=1}^{k}(n+i)$, then I conjecture also that $A(n;k)=A(m;l)$ probably has very few solutions for $m\geqslant n+k$ and $l>1$.

Suppose that $k\geqslant 3$ and $m\geqslant n+k$. Observe that then, for each $k, M(n;k)>M(m;k)$ has infinitely many solutions. Yet I cannot decide whether the same is true for $M(n;k)>M(m;k+1)$. (The referee found two solutions, namely $M(96;7)>M(104;8)$ and $M(132;7)>M(139;8)$.) Let n_k denote the smallest solution of $M(n;k)>M(m;k)$. Try to determine or



P. Erdős, Some Unconventional Problems in Number Theory, *Math. Mag.* **52** (1979), pp. 67–70.

Erdős' approach (to the squarefree conjecture):

- Kummer's theorem (1852): for p prime,

$$p^m \mid\mid \binom{2^{k+1}}{2^k} \Leftrightarrow m = \#\text{carries when adding } 2^k + 2^k \text{ in base } p.$$

Erdős' approach (to the squarefree conjecture):

- Kummer's theorem (1852): for p prime,

$$p^m \,||\, \binom{2^{k+1}}{2^k} \;\Leftrightarrow\; m = \#\text{carries when adding } 2^k + 2^k \text{ in base } p.$$

- 3 does not divide $\binom{2^{k+1}}{2^k} \Leftrightarrow$ the ternary expansion of 2^n omits the digits 2.

Erdős' approach (to the squarefree conjecture):

- Kummer's theorem (1852): for p prime,

$$p^m \,||\, \binom{2^{k+1}}{2^k} \;\Leftrightarrow\; m = \#\text{carries when adding } 2^k + 2^k \text{ in base } p.$$

- 3 does not divide $\binom{2^{k+1}}{2^k} \Leftrightarrow$ the ternary expansion of 2^n omits the digits 2.

" I conjecture that for $k > 8$, 2^k is not the sum of distinct powers of 3 [...] but as far as I see there is no method at our disposal to attack this conjecture."
(Erdős ternary digits conjecture)

Examples

n	2^n	$(2^n)_3$	
0	**1**	**1**	$2^0 = 3^0$
1	2	2	
2	**4**	**11**	$2^2 = 3^1 + 3^0$
3	8	22	
4	16	121	
5	32	1012	
6	64	2101	
7	128	11202	
8	**256**	**100111**	$2^8 = 3^5 + 3^2 + 3^1 + 3^0$
9	512	200222	
10	1024	1101221	
11	2048	2210212	
12	4096	12121201	

Examples

n	2^n	$(2^n)_3$	
0	**1**	**1**	$2^0 = 3^0$
1	2	2	
2	**4**	**11**	$2^2 = 3^1 + 3^0$
3	8	22	
4	16	121	
5	32	1012	
6	64	2101	
7	128	11202	
8	**256**	**100111**	$2^8 = 3^5 + 3^2 + 3^1 + 3^0$
9	512	200222	
10	1024	1101221	
11	2048	2210212	
12	4096	12121201	

Heuristically:

$$\approx \sum_n \left(\frac{2}{3}\right)^{\text{length of expansion of } 2^n \text{ in base } 3} \approx \sum_n \left(\frac{2}{3}\right)^{n\,\frac{\log 2}{\log 3}} < \infty.$$

Conjectures

Erdős ternary digits conjecture:

$\{n : (2^n)_3$ does not contain any digit "2"$\} = \{0, 2, 8\}$.

Conjectures

Erdős ternary digits conjecture:

$\{n : (2^n)_3$ does not contain any digit "2"$\} = \{0, 2, 8\}$.

Widely open !

Conjectures

Erdős ternary digits conjecture:

$\{n : (2^n)_3$ does not contain any digit "2"$\} = \{0, 2, 8\}$.

Widely open !

. . . **- weak form:**

$\#\{n : (2^n)_3$ does not contain any digit "2"$\} < \infty$.

Conjectures

Erdős ternary digits conjecture:

$\{n : (2^n)_3$ does not contain any digit "2"$\} = \{0, 2, 8\}$. Widely open !

. . . **- weak form:**

$\#\{n : (2^n)_3$ does not contain any digit "2"$\} < \infty$. Widely open !

Conjectures

Erdős ternary digits conjecture:

$\{n : (2^n)_3 \text{ does not contain any digit “2”}\} = \{0, 2, 8\}$. Widely open !

. . . **- weak form:**

$\#\{n : (2^n)_3 \text{ does not contain any digit “2”}\} < \infty$. Widely open !

. . . **- even weaker form:**

$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} = o(x^{\log 2/\log 3})$.

Conjectures

Erdős ternary digits conjecture:

$\{n : (2^n)_3 \text{ does not contain any digit “2”}\} = \{0, 2, 8\}$. Widely open !

. . . **- weak form:**

$\#\{n : (2^n)_3 \text{ does not contain any digit “2”}\} < \infty$. Widely open !

. . . **- even weaker form:**

$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} = o(x^{\log 2/\log 3})$.

Widely open !

Conjectures

Erdős ternary digits conjecture:

$\{n : (2^n)_3 \text{ does not contain any digit “2”}\} = \{0, 2, 8\}$. Widely open !

. . . **- weak form:**

$\#\{n : (2^n)_3 \text{ does not contain any digit “2”}\} < \infty$. Widely open !

. . . **- even weaker form:**

$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} = o(x^{\log 2/\log 3})$.

Widely open !

. . . **- flexible form:**

$\#\{n < x : (2^n)_3 \text{ contains at most } \psi_1(n) \text{ digits “2”}\} \leq \psi_2(x)$.

Results

- **Gupta (1978):**

$$\{n < 4374 : (2^n)_3 \text{ does not contain any digit “2”}\} = \{0, 2, 8\}.$$

Results

- **Gupta (1978):**

$$\{n < 4374 : (2^n)_3 \text{ does not contain any digit “2”}\} = \{0, 2, 8\}.$$

- **Narkiewicz (1980):**

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \leq 1.62\, x^{\log 2/\log 3}.$$

Results

- **Gupta (1978):**

$$\{n < 4374 : (2^n)_3 \text{ does not contain any digit “2”}\} = \{0, 2, 8\}.$$

- **Narkiewicz (1980):**

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \leq 1.62\, x^{\log 2/\log 3}.$$

- **Kennedy/Cooper (2001):** a, b integers with $(a, b) = 1$, then

$$\#\{n < x : (a^n)_b \text{ does not contain any digit} \geq \text{“}b/2\text{”}\} \leq C_b x^{\log((b+1)/2)/\log b}.$$

Results

- **Gupta (1978):**

$$\{n < 4374 : (2^n)_3 \text{ does not contain any digit “2”}\} = \{0, 2, 8\}.$$

- **Narkiewicz (1980):**

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \leq 1.62\, x^{\log 2/\log 3}.$$

- **Kennedy/Cooper (2001):** a, b integers with $(a, b) = 1$, then

$$\#\{n < x : (a^n)_b \text{ does not contain any digit} \geq \text{“}b/2\text{”}\} \leq C_b x^{\log((b+1)/2)/\log b}.$$

- **Holdun/Klausen/Rasmussen (2015):** improvements of the multiplicative constants in Narkiewicz (1980) and Kennedy/Cooper (2001).

Proof of Narkiewicz (1980)

Narkiewicz (1980):

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \leq 1.62\, x^{\log 2/\log 3}.$$

Proof of Narkiewicz (1980)

Narkiewicz (1980):

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \leq 1.62\, x^{\log 2/\log 3}.$$

- Write
$$2^n = 3^{m_0} + 3^{m_1} + \cdots + 3^{m_s}$$
with $0 = m_0 < m_1 < \cdots < m_s$.

Proof of Narkiewicz (1980)

Narkiewicz (1980):

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \le 1.62\, x^{\log 2/\log 3}.$$

- Write
$$2^n = 3^{m_0} + 3^{m_1} + \cdots + 3^{m_s}$$
with $0 = m_0 < m_1 < \cdots < m_s$.
- Reduce modulo 3^k. Then the RHS takes one of the 2^{k-1} values
$$1 + \varepsilon_1 \cdot 3 + \cdots + \varepsilon_{k-1} \cdot 3^{k-1}, \qquad \varepsilon_i \in \{0, 1\}.$$

Proof of Narkiewicz (1980)

Narkiewicz (1980):

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \leq 1.62\, x^{\log 2/\log 3}.$$

- Write
$$2^n = 3^{m_0} + 3^{m_1} + \cdots + 3^{m_s}$$
with $0 = m_0 < m_1 < \cdots < m_s$.
- Reduce modulo 3^k. Then the RHS takes one of the 2^{k-1} values
$$1 + \varepsilon_1 \cdot 3 + \cdots + \varepsilon_{k-1} \cdot 3^{k-1}, \qquad \varepsilon_i \in \{0, 1\}.$$

- Thus, 2^{k-1} possibilities for $2^n \pmod{3^k}$.

Proof of Narkiewicz (1980)

Narkiewicz (1980):

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \leq 1.62\, x^{\log 2/\log 3}.$$

- Write
$$2^n = 3^{m_0} + 3^{m_1} + \cdots + 3^{m_s}$$
with $0 = m_0 < m_1 < \cdots < m_s$.
- Reduce modulo 3^k. Then the RHS takes one of the 2^{k-1} values
$$1 + \varepsilon_1 \cdot 3 + \cdots + \varepsilon_{k-1} \cdot 3^{k-1}, \qquad \varepsilon_i \in \{0, 1\}.$$

- Thus, 2^{k-1} possibilities for $2^n \pmod{3^k}$.
- 2 is primitive root for every power of 3, there are only 2^{k-1} residue classes mod $2 \cdot 3^{k-1}$ in which n can lie.

Proof of Narkiewicz (1980)

Narkiewicz (1980):

$$\#\{n < x : (2^n)_3 \text{ does not contain any digit “2”}\} \leq 1.62\, x^{\log 2/\log 3}.$$

- Write
$$2^n = 3^{m_0} + 3^{m_1} + \cdots + 3^{m_s}$$
with $0 = m_0 < m_1 < \cdots < m_s$.
- Reduce modulo 3^k. Then the RHS takes one of the 2^{k-1} values
$$1 + \varepsilon_1 \cdot 3 + \cdots + \varepsilon_{k-1} \cdot 3^{k-1}, \qquad \varepsilon_i \in \{0, 1\}.$$

- Thus, 2^{k-1} possibilities for $2^n \pmod{3^k}$.
- 2 is primitive root for every power of 3, there are only 2^{k-1} residue classes mod $2 \cdot 3^{k-1}$ in which n can lie.
- Count.

Linear forms in logarithms

- **Stewart (1980):** Let a, b be multiplicatively independent. Then there exists $C = C(a, b)$ such that for all $n \geq n_0$,

$$(\#\text{ digits} \neq \alpha \text{ of } (n)_a\ ) + (\#\text{ digits} \neq \beta \text{ of } (n)_b) \geq \frac{\log\log n}{\log\log\log n + C}.$$

Linear forms in logarithms

- **Stewart (1980):** Let a, b be multiplicatively independent. Then there exists $C = C(a, b)$ such that for all $n \geq n_0$,

$$(\#\text{ digits} \neq \alpha \text{ of } (n)_a\ ) + (\#\text{ digits} \neq \beta \text{ of } (n)_b) \geq \frac{\log\log n}{\log\log\log n + C}.$$

Apply for ($a = 2$, $n \to 2^n$, $\alpha = 0$, and $b = 3$, $\beta = 0$):

$$(\#\text{ digits} = 1 \text{ of } (2^n)_3\ ) + (\#\text{ digits} = 2 \text{ of } (2^n)_3\ ) \geq c\frac{\log n}{\log\log n}, \qquad n \geq n_0.$$

The number of non-zero digits in $(2^n)_3$ is unbounded.

Linear forms in logarithms

- **Stewart (1980):** Let a, b be multiplicatively independent. Then there exists $C = C(a, b)$ such that for all $n \geq n_0$,

$$(\#\text{ digits} \neq \alpha \text{ of } (n)_a\ ) + (\#\text{ digits} \neq \beta \text{ of } (n)_b) \geq \frac{\log\log n}{\log\log\log n + C}.$$

Apply for ($a = 2$, $n \to 2^n$, $\alpha = 0$, and $b = 3$, $\beta = 0$):

$$(\#\text{ digits} = 1 \text{ of } (2^n)_3\ ) + (\#\text{ digits} = 2 \text{ of } (2^n)_3\ ) \geq c\frac{\log n}{\log\log n}, \qquad n \geq n_0.$$

The number of non-zero digits in $(2^n)_3$ is unbounded.

No information on the individual count of the 1's and 2's.

Average results

Let $d_{n,m}$ be the number of digits "2" within the first m digits $a_0, a_1, \ldots a_{m-1}$ of 2^n in base 3,

$$2^n = a_0 + a_1 \cdot 3 + \cdots + a_{m-1} \cdot 3^{m-1} + \cdots + a_N \cdot 3^N, \quad N \approx n \cdot \frac{\log 2}{\log 3}$$

- $$\lim_{n\to\infty} \frac{d_{n,N}}{N} = \frac{1}{3} \qquad \text{or} \qquad \lim_{n\to\infty} \frac{d_{n,m_n}}{m_n} = \frac{1}{3},$$

  for some suitable $m_n \to \infty$, m_n monotone, would prove Erdős ternary digits conjecture (weak form).

Average results

Let $d_{n,m}$ be the number of digits "2" within the first m digits $a_0, a_1, \ldots a_{m-1}$ of 2^n in base 3,

$$2^n = a_0 + a_1 \cdot 3 + \cdots + a_{m-1} \cdot 3^{m-1} + \cdots + a_N \cdot 3^N, \quad N \approx n \cdot \frac{\log 2}{\log 3}$$

- $$\lim_{n\to\infty} \frac{d_{n,N}}{N} = \frac{1}{3} \qquad \text{or} \qquad \lim_{n\to\infty} \frac{d_{n,m_n}}{m_n} = \frac{1}{3},$$
  for some suitable $m_n \to \infty$, m_n monotone, would prove Erdős ternary digits conjecture (weak form).

- **Dupuy et Weirich (2016):**
  $$\lim_{m\to\infty} \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{d_{n,m}}{m} = \frac{1}{3}.$$

Average results

Let $d_{n,m}$ be the number of digits "2" within the first m digits $a_0, a_1, \dots a_{m-1}$ of 2^n in base 3,

$$2^n = a_0 + a_1 \cdot 3 + \cdots + a_{m-1} \cdot 3^{m-1} + \cdots + a_N \cdot 3^N, \quad N \approx n \cdot \frac{\log 2}{\log 3}$$

- $$\lim_{n\to\infty} \frac{d_{n,N}}{N} = \frac{1}{3} \qquad \text{or} \qquad \lim_{n\to\infty} \frac{d_{n,m_n}}{m_n} = \frac{1}{3},$$
  for some suitable $m_n \to \infty$, m_n monotone, would prove Erdős ternary digits conjecture (weak form).

- **Dupuy et Weirich (2016):**
$$\lim_{m\to\infty} \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{d_{n,m}}{m} = \frac{1}{3}.$$

- **Yu (2018+):**
$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{d_{n,m_n}}{m_n} = \frac{1}{3}.$$

Variations

- **Lagarias (2009):** For all $\lambda > 0$ and $x \geq x_0(\lambda)$,

$$\#\{n < x : (\lfloor \lambda 2^n \rfloor)_3 \text{ does not contain any digit “2”}\} \leq 25\, x^{0.9725}.$$

Variations

- **Lagarias (2009):** For all $\lambda > 0$ and $x \geq x_0(\lambda)$,

$$\#\{n < x : (\lfloor \lambda 2^n \rfloor)_3 \text{ does not contain any digit “2”}\} \leq 25\, x^{0.9725}.$$

  There are uncountably many λ such that there are infinitely many such (exceptional) n's.

Variations

- **Lagarias (2009):** For all $\lambda > 0$ and $x \geq x_0(\lambda)$,

$$\#\{n < x : (\lfloor \lambda 2^n \rfloor)_3 \text{ does not contain any digit “2”}\} \leq 25\, x^{0.9725}.$$

  There are uncountably many λ such that there are infinitely many such (exceptional) n's.

$$\dim_H\{\lambda > 0 : \#\{n : (\lfloor \lambda 2^n \rfloor)_3 \text{ does not contain any digit “2”}\} = \infty\} = \frac{\log 2}{\log 3}.$$

  (Work by Abram, Lagarias (2014), Abram, Lagarias, Bolshakov (2017) etc.)

Variations

- **Lagarias (2009):** For all $\lambda > 0$ and $x \geq x_0(\lambda)$,

$$\#\{n < x : (\lfloor \lambda 2^n \rfloor)_3 \text{ does not contain any digit “2”}\} \leq 25\, x^{0.9725}.$$

  There are uncountably many λ such that there are infinitely many such (exceptional) n's.

$$\dim_H\{\lambda > 0 : \#\{n : (\lfloor \lambda 2^n \rfloor)_3 \text{ does not contain any digit “2”}\} = \infty\} = \frac{\log 2}{\log 3}.$$

  (Work by Abram, Lagarias (2014), Abram, Lagarias, Bolshakov (2017) etc.)

- **Burrell/Yu (2019+):**

$$\#\{n < x : n \text{ contains only digits “0”, “1” in bases 3, 4 and 5}\} \leq C_\varepsilon x^\varepsilon$$

  (Uses an improvement of Yu on Furstenberg's slicing problem.)

Patterns

Soient p, q multiplicatively independent positive integers.

- **Lagarias conjecture (2009):** Any given finite pattern $P = a_1 a_2 \cdots a_k$ of consecutive q-ary digits occurs in $(p^n)_q$, for all sufficiently large $n > n_0(P)$.

Patterns

Soient p, q multiplicatively independent positive integers.

- **Lagarias conjecture (2009):** Any given finite pattern $P = a_1 a_2 \cdots a_k$ of consecutive q-ary digits occurs in $(p^n)_q$, for all sufficiently large $n > n_0(P)$.
- **Furstenberg conjecture (1970):** same statement for $(p^n)_{pq}$ instead of $(p^n)_q$.

Patterns

Soient p, q multiplicatively independent positive integers.

- **Lagarias conjecture (2009):** Any given finite pattern $P = a_1 a_2 \cdots a_k$ of consecutive q-ary digits occurs in $(p^n)_q$, for all sufficiently large $n > n_0(P)$.
- **Furstenberg conjecture (1970):** same statement for $(p^n)_{pq}$ instead of $(p^n)_q$.

Weak Erdős conjecture is the case $p = 2$, $q = 3$, $P = 2$ in Lagarias' conjecture.

Patterns

Soient p, q multiplicatively independent positive integers.

- **Lagarias conjecture (2009):** Any given finite pattern $P = a_1 a_2 \cdots a_k$ of consecutive q-ary digits occurs in $(p^n)_q$, for all sufficiently large $n > n_0(P)$.
- **Furstenberg conjecture (1970):** same statement for $(p^n)_{pq}$ instead of $(p^n)_q$.

Weak Erdős conjecture is the case $p = 2$, $q = 3$, $P = 2$ in Lagarias' conjecture.

Questions:

- Can we avoid a fixed pattern P in the q-ary digital expansions of $p, p^2, p^3, \ldots$?
- If not, how long must we wait to "see" P ?
- What about repeated patterns $PP \cdots P$?

Main result - Patterns in exponential functions

Theorem (Kaneko, S. (2018))

Let $p \geq 2$ be a prime, m not a power of p, and

$$P = a_1 a_2 \cdots a_k$$

be any finite pattern of consecutive p-ary digits. Then:

(1) *There exist $c_1, c_2 > 0$ only depending on p, m and P such that*

$$\#\{n < x : (m^n)_p \text{ contains} \geq c_1 \log n \text{ occurrences of } P\} \geq c_2 x.$$

(2) *There exists $c_3 = c_3(p, m)$ and $n < c_3 p^{kL}$ such that $(m^n)_p$ contains L consecutive occurrences of P.*

(3) *There exists $c = c(P) > 0$ such that*

$$\limsup_{n \to \infty} \frac{\#\text{ patterns } P \text{ in } (m^n)_p}{\log n} \geq \frac{c}{\log p} > 0.$$

Hensel's lemma - basic statement

Basic statement:

Let $f(X) \in \mathbb{Z}_p[X]$. Suppose that $u \in \mathbb{Z}_p$ is such that

$$f(u) \equiv 0 \pmod{p}, \qquad \text{and} \qquad f'(u) \not\equiv 0 \pmod{p}.$$

Then there exists an unique $\xi \in \mathbb{Z}_p$ such that

$$f(\xi) = 0, \qquad \text{and} \qquad \xi \equiv u \pmod{p}.$$

Hensel's lemma - basic statement

Basic statement:
Let $f(X) \in \mathbb{Z}_p[X]$. Suppose that $u \in \mathbb{Z}_p$ is such that

$$f(u) \equiv 0 \pmod{p}, \qquad \text{and} \quad f'(u) \not\equiv 0 \pmod{p}.$$

Then there exists an unique $\xi \in \mathbb{Z}_p$ such that

$$f(\xi) = 0, \qquad \text{and} \quad \xi \equiv u \pmod{p}.$$

Basic statement (II):
Let $f(X) \in \mathbb{Z}_p[X] \setminus \mathbb{Z}_p$. Suppose that $u \in \mathbb{Z}_p$ is such that

$$v_p(f(u)) > 2v_p(f'(u)).$$

Then there exists a unique $\xi \in \mathbb{Z}_p$ such that

$$f(\xi) = 0, \qquad \text{and} \quad v_p(\xi - u) > v_p(f'(u)).$$

Hensel's lemma - differentiable functions

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a function and $u \in \mathbb{Z}_p$. f is differentiable modulo p^s at u if there exists $\partial_s f(u) \in \mathbb{Q}_p$ such that for any $u' \in \mathbb{Z}_p$ and all $n > N$,

$$f(u + p^n u') \equiv f(u) + p^n u' \partial_s f(u) \pmod{p^{n+s}}.$$

Hensel's lemma - differentiable functions

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a function and $u \in \mathbb{Z}_p$. f is differentiable modulo p^s at u if there exists $\partial_s f(u) \in \mathbb{Q}_p$ such that for any $u' \in \mathbb{Z}_p$ and all $n > N$,

$$f(u + p^n u') \equiv f(u) + p^n u' \partial_s f(u) \pmod{p^{n+s}}.$$

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ and $u \in \mathbb{Z}_p$. Assume that $v_p(f(u)) \geq n$ and that for all $x \in \mathbb{Z}_p$ with $x \equiv u \pmod{p^{n-j}}$ that f is differentiable modulo p^s at x with order N and that

$$v_p(\partial_s f(x)) = j,$$

with $j + N < n$ and $j < s$. Then there exists an $\xi \in \mathbb{Z}_p$ satisfying

$$f(\xi) = 0, \qquad \text{and} \quad \xi \equiv u \pmod{p^{n-j}}.$$

Hensel's lemma - differentiable functions

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a function and $u \in \mathbb{Z}_p$. f is differentiable modulo p^s at u if there exists $\partial_s f(u) \in \mathbb{Q}_p$ such that for any $u' \in \mathbb{Z}_p$ and all $n > N$,

$$f(u + p^n u') \equiv f(u) + p^n u' \partial_s f(u) \pmod{p^{n+s}}.$$

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ and $u \in \mathbb{Z}_p$. Assume that $v_p(f(u)) \geq n$ and that for all $x \in \mathbb{Z}_p$ with $x \equiv u \pmod{p^{n-j}}$ that f is differentiable modulo p^s at x with order N and that

$$v_p(\partial_s f(x)) = j,$$

with $j + N < n$ and $j < s$. Then there exists an $\xi \in \mathbb{Z}_p$ satisfying

$$f(\xi) = 0, \qquad \text{and} \quad \xi \equiv u \pmod{p^{n-j}}.$$

- Generalises **Axelsson/Khrennikov (2016):** 1-Lipschitz functions, namely $f : \mathbb{Z}_p \to \mathbb{Z}_p$ which satisfy $|f(x) - f(y)|_p \leq |x - y|_p$ for any $x, y \in \mathbb{Z}_p$.

van der Put series

For a positive integer m, write

$$m = m_0 + m_1 p + \cdots + m_k p^k,$$

where $k = \lfloor \log m / \log p \rfloor$. For $x \in \mathbb{Z}_p$ set

$$\chi(m; x) = \begin{cases} 1 & \text{if } |x - m|_p \leq p^{-1-k}, \\ 0 & \text{otherwise.} \end{cases}$$

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be any continuous function. Then there exists a unique sequence $B(f; m)$ $(m = 0, 1, \ldots)$ such that

$$f(x) = \sum_{m=0}^{\infty} B(f; m)\chi(m; x)$$

for any $x \in \mathbb{Z}_p$, the **van der Put series of** f. (van der Put 1968)

Generalized van der Put series

Let $\Phi : \mathbb{N} \to \mathbb{N}$ be a strictly increasing function. For $x \in \mathbb{Z}_p$ write

$$x = \sum_{j=0}^{\infty} \sum_{i=\Phi(-1+j)+1}^{\Phi(j)} x_i p^i.$$

Put

$$\tau(m) = \min \left\{ h \in \mathbb{N} \;\middle|\; m < p^{1+\Phi(h)} \right\}$$

and, for any $x \in \mathbb{Z}_p$,

$$\chi(m; x) := \begin{cases} 1 & \text{if } |x - m|_p \le p^{-1-\Phi(\tau(m))}, \\ 0 & \text{otherwise.} \end{cases}$$

For any continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ there exists a unique sequence $B(m) = B(f; m)$ $(m = 0, 1, \ldots)$ such that

$$f(x) = \sum_{m=0}^{\infty} B(f; m)\chi(m; x)$$

for any $x \in \mathbb{Z}_p$, the **generalized van der Put series of** f. Put

$$b(m) = b(f; m) := p^{-\tau(m)} B(f; m) \in \mathbb{Z}_p.$$

Hensel's lemma - continuous functions

Theorem (Kaneko, S. (2019))

Let $\Phi : \mathbb{N} \to \mathbb{N}$ *be strictly increasing,* $f \in \mathcal{F}(\Phi)$ *continuous,* $u < p^{1+\Phi(n_0)}$ *and*

$$f(u) \equiv 0 \pmod{p^{1+h+n_0}}.$$

Suppose that there exists $(S(n))_{n \geq n_0}$ *with*

$$S(n) \subset \left(0, p^{\Phi(n+1)-\Phi(n)}\right), \quad \#S(n) = p-1,$$

such that for any nonnegative integers n, m *with*

$$n \geq n_0, \quad m < p^{1+\Phi(n)}, \quad m \equiv u \pmod{p^{1+\Phi(n_0)}},$$

we have

$$\left\{ b\left(m + ip^{1+\Phi(n)}\right) \bmod p^{h+1} \;\middle|\; i \in S(n) \right\} = \left\{ p^h, 2p^h, \ldots, (p-1)p^{h+1} \right\}.$$

Then there exists $\xi \in \mathbb{Z}_p$ *such that*

$$f(\xi) = 0, \qquad \xi \equiv u \pmod{p^{1+\Phi(n_0)}}.$$

Main result - Patterns in exponential functions

Theorem (Kaneko, S. (2018))

Let $p \geq 2$ be a prime, m not a power of p, and

$$P = a_1 a_2 \cdots a_k$$

be any finite pattern of consecutive p-ary digits. Then:

(1) *There exist $c_1, c_2 > 0$ only depending on p, m and P such that*

$$\#\{n < x : (m^n)_p \text{ contains} \geq c_1 \log n \text{ occurrences of } P\} \geq c_2 x.$$

(2) *There exists $c_3 = c_3(p, m)$ and $n < c_3 p^{kL}$ such that $(m^n)_p$ contains L consecutive occurrences of P.*

(3) *There exists $c = c(P) > 0$ such that*

$$\limsup_{n \to \infty} \frac{\#\text{ patterns } P \text{ in } (m^n)_p}{\log n} \geq \frac{c}{\log p} > 0.$$

Key moments in the proof

- Let $P = a_1 a_2 \cdots a_k$ and $b_{p,L}$ be the integer whose p-ary expansion is

$$\underbrace{PP\cdots P}_{L}\underbrace{00\cdots 0}_{c}1, \qquad L' = kL + c + 1$$

Key moments in the proof

- Let $P = a_1 a_2 \cdots a_k$ and $b_{p,L}$ be the integer whose p-ary expansion is

$$\underbrace{PP\cdots P}_{L}\underbrace{00\cdots 0}_{c}1, \qquad L' = kL + c + 1$$

- Put $g : \mathbb{Z}_p \to \mathbb{Z}_p$ with

$$g(u) = (m^{p-1})^u = (1 + ap^e)^u$$

with $a \nmid p$, and set $f(u) = g(u) - b_{p,L}$.

Key moments in the proof

- Let $P = a_1 a_2 \cdots a_k$ and $b_{p,L}$ be the integer whose p-ary expansion is

$$\underbrace{PP\cdots P}_{L}\underbrace{00\cdots 0}_{c}1, \qquad L' = kL + c + 1$$

- Put $g : \mathbb{Z}_p \to \mathbb{Z}_p$ with

$$g(u) = (m^{p-1})^u = (1 + ap^e)^u$$

  with $a \nmid p$, and set $f(u) = g(u) - b_{p,L}$.
- For $e \geq 2$ or $p \geq 3$, $g(u)$ is differentiable modulo p^{e+1} at any $u \in \mathbb{Z}_p$ with order 0 and $\partial_{e+1} g(u) = ap^e$.

Key moments in the proof

- Let $P = a_1 a_2 \cdots a_k$ and $b_{p,L}$ be the integer whose p-ary expansion is

$$\underbrace{PP\cdots P}_{L}\underbrace{00\cdots 0}_{c}1, \qquad L' = kL + c + 1$$

- Put $g : \mathbb{Z}_p \to \mathbb{Z}_p$ with

$$g(u) = (m^{p-1})^u = (1 + ap^e)^u$$

  with $a \nmid p$, and set $f(u) = g(u) - b_{p,L}$.
- For $e \geq 2$ or $p \geq 3$, $g(u)$ is differentiable modulo p^{e+1} at any $u \in \mathbb{Z}_p$ with order 0 and $\partial_{e+1} g(u) = ap^e$.
- Generalized Hensel gives $\xi \in \mathbb{Z}_p$ such that $g(\xi) = b_{p,L}$.

Key moments in the proof

- Let $P = a_1 a_2 \cdots a_k$ and $b_{p,L}$ be the integer whose p-ary expansion is

$$\underbrace{PP\cdots P}_{L}\underbrace{00\cdots 0}_{c}1, \qquad L' = kL + c + 1$$

- Put $g : \mathbb{Z}_p \to \mathbb{Z}_p$ with

$$g(u) = (m^{p-1})^u = (1 + ap^e)^u$$

  with $a \nmid p$, and set $f(u) = g(u) - b_{p,L}$.
- For $e \geq 2$ or $p \geq 3$, $g(u)$ is differentiable modulo p^{e+1} at any $u \in \mathbb{Z}_p$ with order 0 and $\partial_{e+1} g(u) = ap^e$.
- Generalized Hensel gives $\xi \in \mathbb{Z}_p$ such that $g(\xi) = b_{p,L}$.
- Let $N \equiv \xi \pmod{p^{L'}}$ with $p^{L'} \leq N < 2p^{L'}$.

Key moments in the proof

- Let $P = a_1 a_2 \cdots a_k$ and $b_{p,L}$ be the integer whose p-ary expansion is

$$\underbrace{PP\cdots P}_{L}\underbrace{00\cdots 0}_{c}1, \qquad L' = kL + c + 1$$

- Put $g : \mathbb{Z}_p \to \mathbb{Z}_p$ with

$$g(u) = (m^{p-1})^u = (1 + ap^e)^u$$

  with $a \nmid p$, and set $f(u) = g(u) - b_{p,L}$.
- For $e \geq 2$ or $p \geq 3$, $g(u)$ is differentiable modulo p^{e+1} at any $u \in \mathbb{Z}_p$ with order 0 and $\partial_{e+1} g(u) = ap^e$.
- Generalized Hensel gives $\xi \in \mathbb{Z}_p$ such that $g(\xi) = b_{p,L}$.
- Let $N \equiv \xi \pmod{p^{L'}}$ with $p^{L'} \leq N < 2p^{L'}$.
- Since $u, u' \in \mathbb{Z}_p$ with $v_p(u - u') \geq N$ implies $v_p(g(u) - g(u')) \geq N + 1$,

$$m^{(p-1)N} = g(N) \equiv g(\xi) = b_{q,L} \pmod{p^{L'}}.$$

Key moments in the proof

- Let $P = a_1 a_2 \cdots a_k$ and $b_{p,L}$ be the integer whose p-ary expansion is

$$\underbrace{PP\cdots P}_{L}\underbrace{00\cdots 0}_{c}1, \qquad L' = kL + c + 1$$

- Put $g : \mathbb{Z}_p \to \mathbb{Z}_p$ with

$$g(u) = (m^{p-1})^u = (1 + ap^e)^u$$

  with $a \nmid p$, and set $f(u) = g(u) - b_{p,L}$.
- For $e \geq 2$ or $p \geq 3$, $g(u)$ is differentiable modulo p^{e+1} at any $u \in \mathbb{Z}_p$ with order 0 and $\partial_{e+1} g(u) = ap^e$.
- Generalized Hensel gives $\xi \in \mathbb{Z}_p$ such that $g(\xi) = b_{p,L}$.
- Let $N \equiv \xi \pmod{p^{L'}}$ with $p^{L'} \leq N < 2p^{L'}$.
- Since $u, u' \in \mathbb{Z}_p$ with $v_p(u - u') \geq N$ implies $v_p(g(u) - g(u')) \geq N + 1$,

$$m^{(p-1)N} = g(N) \equiv g(\xi) = b_{q,L} \pmod{p^{L'}}.$$

Thank you !