Reversible primes

Cathy Swaenepoel

IMJ-PRG, Université Paris Cité

Joint work with C. Dartyge, B. Martin, J. Rivat and I. Shparlinski.

One World Numeration Seminar,

January 30, 2024.

Digits

Representation of an integer $k > 0$ in base $b \geqslant 2$:

$$k = \sum_{j=0}^{n-1} \varepsilon_j(k) b^j$$

where $\varepsilon_j(k) \in \{0, \dots, b-1\}$ and $\varepsilon_{n-1}(k) \neq 0$.

base b expansion $\xleftrightarrow{\text{independence?}}$ multiplicative representation
(as a product of prime factors)

Digits of primes

- **Mauduit–Rivat (2010)**: The sum of digits of primes is well distributed mod m.
- **Maynard (2019)**: There are infinitely many primes with no digit 7 in base 10.
- **Bourgain (2015), S. (2020)**: Primes with a positive proportion of prescribed digits.
- **Martin–Mauduit–Rivat (2019)**: Primes which are "équilibrés" in base b (example in base 2: $(1010011)_2 = 83$).
- **Col (2009)**:
  - Upper bound for the number of palindromic primes less than x.
  - There are infinitely many binary palindromes k such that $\Omega(k) \leqslant 60$. Tuxanidy–Panario (preprint 2023): 60 can be replaced by 6.

Reverse

For a positive integer k written in base b as

$$k = \sum_{j=0}^{n-1} \varepsilon_j(k) b^j,$$

where $\varepsilon_j(k) \in \{0, \ldots, b-1\}$ and $\varepsilon_{n-1}(k) \neq 0$, we define the "**reverse**" of k by:

$$\overleftarrow{k} = \sum_{j=0}^{n-1} \varepsilon_j(k) b^{n-1-j}.$$

Example in base $b = 2$: The reverse of $k = 23 = (10111)_2$ is $\overleftarrow{k} = (11101)_2 = 29$.

Reversible primes

Now $b = 2$. Let $\Theta(n)$ be the number of n-bit reversible primes:

$$\Theta(n) = |\{a \in [2^{n-1}, 2^n) : a \text{ and } \overleftarrow{a} \text{ are prime}\}|.$$

Example: $$\Theta(5) = |\{ \underset{(10001)_2}{\overset{17}{\|}} , \underset{(10111)_2}{\overset{23}{\|}} , \underset{(11101)_2}{\overset{29}{\|}} , \underset{(11111)_2}{\overset{31}{\|}} \}| = 4.$$

Problem: Estimate $\Theta(n)$ as $n \to +\infty$.

Conjecture: There exists $c > 0$ such that

$$\Theta(n) = \frac{2^n}{n^2} (c + o(1)) \qquad (n \to +\infty).$$

Results

We define $\mathcal{B}_n = \{a \in [2^{n-1}, 2^n) : a \text{ odd}\}$ (note that $a \in \mathcal{B}_n \Rightarrow \overleftarrow{a} \in \mathcal{B}_n$) and

$$\Theta(n, z) = |\{a \in \mathcal{B}_n : P^-(a\overleftarrow{a}) \geqslant z\}|$$

where $P^-(a\overleftarrow{a})$ is the smallest prime factor of $a\overleftarrow{a}$.

Theorem 1 (DMRSS 2024+)

1. *For any* $\gamma \in (0, 1)$*, we have*

$$\Theta(n, 2^{\gamma n}) \ll_\gamma \frac{2^n}{n^2}.$$

2. *For any* $\gamma \in \left(0, \frac{1}{2\beta_2}\right)$*, there exists* $n_0 = n_0(\gamma)$ *such that for* $n \geqslant n_0$*, we have*

$$\Theta(n, 2^{\gamma n}) \gg_\gamma \frac{2^n}{n^2}.$$

Remark: $\beta_2 \approx 4.2664.$

Results

Recall that $\varTheta(n) = |\{a \in [2^{n-1}, 2^n) : a \text{ and } \overleftarrow{a} \text{ are prime}\}|$
and $\varTheta(n, z) = |\{a \in \mathcal{B}_n : P^-(a\overleftarrow{a}) \geqslant z\}|$.

Remark: $\varTheta(n) \leqslant \varTheta(n, z)$ for any $z \leqslant 2^{n-1}$.

Corollary 2 (DMRSS 2024+)

For any $n \geqslant 1$, we have

$$\varTheta(n) \ll \frac{2^n}{n^2}.$$

Remark: If $a < 2^n$ and $P^-(a) \geqslant 2^{\gamma n}$ then $\Omega(a) < \frac{1}{\gamma}$. Our limit for $\frac{1}{\gamma}$ is $2\beta_2 \approx 8.53$.

Corollary 3 (DMRSS 2024+)

There exists n_0 such that for $n \geqslant n_0$, we have

$$|\{a \in \mathcal{B}_n : \max(\Omega(a), \Omega(\overleftarrow{a})) \leqslant 8\}| \gg \frac{2^n}{n^2}.$$

Results

As an application of the techniques developed to prove Theorem 1, we obtain:

Theorem 4 (DMRSS 2024+)

There exists an absolute constant $c > 0$ such that for $n \geqslant 1$, we have

$$|\{a \in \mathcal{B}_n : a \textit{ and } \overleftarrow{a} \textit{ are squarefree}\}| = |\mathcal{B}_n| \left(\frac{66}{\pi^4} + O\left(\exp(-c\sqrt{n})\right) \right).$$

Proof of Theorem 1

Approach to estimate $\Theta(n,z)$

Denoting $P(z) = \prod_{3 \leqslant p < z} p$, we have

$$\Theta(n,z) = |\{a \in \mathcal{B}_n : \gcd(a\overleftarrow{a}, P(z)) = 1\}|.$$

$\Theta(n,z)$ is the "sifting function" for the sequence $\mathcal{A} = (a\overleftarrow{a})_{a \in \mathcal{B}_n}$.

Good approximation of the number of terms of $\mathcal{A}$ which are divisible by d, on average over $d \mid P(z)$. See Lemma 5 below.

Sieve $\Downarrow$

Two-dimensional sieve (Diamond–Halberstam–Richert 1988)

Estimate of the sifting function for $\mathcal{A}$. $\Rightarrow$ Theorem 1

Remark: $\beta_2 \approx 4.2664$ is the "sieving limit".

Number of terms of $\mathcal{A}$ divisible by d

For d squarefree and odd, we need a good approximation of

$$T_n(d) := |\{a \in \mathcal{B}_n : d \mid a\overleftarrow{a}\}|.$$

Heuristic: Pick $a \in \mathcal{B}_n$ at random. $\mathbb{P}(d \mid a\overleftarrow{a}) \approx$?

- For $p \geqslant 5$, $\mathbb{P}(p \mid a\overleftarrow{a}) = \mathbb{P}(p \mid a) + \mathbb{P}(p \mid \overleftarrow{a}) - \mathbb{P}(p \mid a \text{ and } p \mid \overleftarrow{a}) \approx \frac{1}{p} + \frac{1}{p} - \frac{1}{p^2} = \frac{2p-1}{p^2}$.
- $\overleftarrow{a} \equiv (-1)^{n-1} a \bmod 3$. Thus $\mathbb{P}(3 \mid a\overleftarrow{a}) = \mathbb{P}(3 \mid a) \approx \frac{1}{3}$.
- For $p_1 \neq p_2$, $\mathbb{P}(p_1 p_2 \mid a\overleftarrow{a}) \approx \mathbb{P}(p_1 \mid a\overleftarrow{a})\,\mathbb{P}(p_2 \mid a\overleftarrow{a})$.

We therefore expect that

$$\mathbb{P}(d \mid a\overleftarrow{a}) \approx \frac{f(d)}{d}$$

where f is the multiplicative function defined by

$$f(p) = \begin{cases} 0 & \text{if } p = 2, \\ 1 & \text{if } p = 3, \\ \frac{2p-1}{p} & \text{if } p \geqslant 5, \end{cases} \qquad \text{and} \qquad f(p^\nu) = 0 \text{ for any } \nu \geqslant 2.$$

Recall that $T_n(d) = |\{a \in \mathcal{B}_n : d \mid a\overleftarrow{a}\}|$. We define

$$R_n(d) = T_n(d) - \frac{f(d)}{d}|\mathcal{B}_n|$$

and prove that $|R_n(d)|$ is small on average:

Lemma 5 (Main technical result)

Let $\xi \in (0, \frac{1}{2})$. There exists $c = c(\xi) > 0$ such that for any $n \geqslant 1$, we have

$$\sum_{\substack{d < 2^{\xi n} \\ d \text{ odd, sf}}} 4^{\Omega(d)} |R_n(d)| \ll_\xi 2^n \exp(-c\sqrt{n}).$$

Proof of Lemma 5

Recall that $R_n(d) = T_n(d) - \frac{f(d)}{d}|\mathcal{B}_n|$ with $T_n(d) = |\{a \in \mathcal{B}_n : d \mid a\overleftarrow{a}\}|$.

Notation: $\mathrm{e}(x) = \exp(2\pi i x)$, $x \in \mathbb{R}$.

Expression of $R_n(d)$ with exponential sums

$$T_n(d) = \sum_{\substack{0\leqslant u,v<d \\ uv\equiv 0 \bmod d}} \sum_{a\in\mathcal{B}_n} \mathbf{1}_{a\equiv u \bmod d}\, \mathbf{1}_{\overleftarrow{a}\equiv v \bmod d}$$

$$= \sum_{\substack{0\leqslant u,v<d \\ uv\equiv 0 \bmod d}} \sum_{a\in\mathcal{B}_n} \left(\frac{1}{d}\sum_{0\leqslant h_1<d} \mathrm{e}\left(\frac{h_1(a-u)}{d}\right)\right)\left(\frac{1}{d}\sum_{0\leqslant h_2<d} \mathrm{e}\left(\frac{h_2(\overleftarrow{a}-v)}{d}\right)\right)$$

$$= \frac{1}{d^2}\sum_{0\leqslant h_1,h_2<d} \left(\sum_{\substack{0\leqslant u,v<d \\ uv\equiv 0 \bmod d}} \mathrm{e}\left(\frac{-h_1u-h_2v}{d}\right)\right)\left(\sum_{a\in\mathcal{B}_n} \mathrm{e}\left(\frac{h_1a+h_2\overleftarrow{a}}{d}\right)\right)$$

$$= \underbrace{\frac{f(d)}{d}|\mathcal{B}_n|}_{\substack{\text{contri. of } (h_1,h_2)=(0,0) \\ (\text{if } 3\nmid d)}} + \underbrace{R_n(d)}_{\text{contri. of } (h_1,h_2)\neq(0,0)}.$$

Denoting $F_n(\alpha,\vartheta) = \frac{1}{|\mathcal{B}_n|}\sum_{a\in\mathcal{B}_n} \mathrm{e}(\alpha\overleftarrow{a}-\vartheta a)$, the sum in blue is equal to $|\mathcal{B}_n|\cdot F_n\left(\frac{h_2}{d},\frac{-h_1}{d}\right)$.

Upper bounds of $|F_n|$

$$F_n(\alpha, \vartheta) = \frac{1}{|\mathcal{B}_n|} \sum_{a \in \mathcal{B}_n} \mathrm{e}(\alpha \overleftarrow{a} - \vartheta a).$$

Lemma 6 (Pointwise bound)

For $d \in \mathbb{N}$ and $h \in \mathbb{Z}$ such that d is odd and $d \nmid 3h$, we have

$$\max_{\alpha \in \mathbb{R}} \left| F_n\left(\alpha, \frac{h}{d}\right) \right| \ll \exp\left(\frac{-c_0\, n}{\log\left(\frac{4d}{3}\right)} \right) \quad \textit{with} \quad c_0 = 0.0308\ldots.$$

Lemma 7 (Bound on average)

Let $\xi \in (0, \frac{1}{2})$. There exists $\delta = \delta(\xi) > 0$ such that if $D_1 D_2 D_3 \leqslant 2^{\xi n}$ then

$$\sum_{\substack{d_1, d_2, d_3 \\ D_i \leqslant d_i < 2D_i \\ \gcd(d_i, 6) = 1}} \sum_{\substack{0 < h_1 < d_2 d_3 \\ \gcd(h_1, d_2 d_3) = 1}} \sum_{\substack{0 < h_2 < d_1 d_3 \\ \gcd(h_2, d_1 d_3) = 1}} \left| F_n\left(\frac{h_2}{d_1 d_3}, \frac{h_1}{d_2 d_3} \right) \right| \ll_\xi D_1 D_2 D_3^2 \left(D_1 D_2 D_3\right)^{-\delta}.$$

Arguments for Lemma 6 (Pointwise bound)

$$F_n(\alpha, \vartheta) = \frac{1}{|\mathcal{B}_n|} \sum_{a \in \mathcal{B}_n} \mathrm{e}(\alpha \overleftarrow{a} - \vartheta a).$$

1. **Product formula**: Writing a and $\overleftarrow{a}$ in base 2, we obtain

$$|F_n(\alpha, \vartheta)| = \prod_{j=1}^{n-2} |U(\alpha 2^{n-1-j} - \vartheta 2^j)| \quad \text{where} \quad |U(x)| = \frac{|1 + \mathrm{e}(x)|}{2} = |\cos \pi x|.$$

Recall that $|F_n(\alpha,\vartheta)| = \prod_{j=1}^{n-2} |U(\alpha 2^{n-1-j} - \vartheta 2^j)|$ where $|U(x)| = \frac{|1+\mathrm{e}(x)|}{2}$.

2. **Bound uniform in α:** By judiciously grouping the product terms, we obtain

$$\max_{\alpha\in\mathbb{R}} |F_n(\alpha,\vartheta)| \leqslant \prod_{j=1}^{n-3} \left(\frac{1}{4}|U(3\vartheta 2^j)| + \frac{3}{4}\right)^{1/3}.$$

Proof: This follows from:

- $|F_n(\alpha,\vartheta)|^3 \leqslant \prod_{j=1}^{n-3} |U(\alpha 2^{n-1-j} - \vartheta 2^j) U^2(\alpha 2^{n-1-(j+1)} - \vartheta 2^{j+1})|$,
- $|U(x)U^2(y)| \leqslant \frac{1}{4}|U(x-2y)| + \frac{3}{4}, \qquad (x,y)\in\mathbb{R}^2.$

3. For $\vartheta = \frac{h}{d}$, “several” terms of the product are “small” (classical).

4. **Cauchy–Schwarz inequality**.
5. For fixed d_2, d_3 and h_1, since the points $\frac{h_2}{d_1 d_3}$ are $(4D_1^2 d_3)^{-1}$-spaced modulo 1, we obtain by the **large sieve inequality**:

$$\sum_{D_1 \leqslant d_1 < 2D_1} \sum_{\substack{0 < h_2 < d_1 d_3 \\ \gcd(h_2, d_1 d_3) = 1}} \left| F_m \left(\frac{h_2}{d_1 d_3}, \frac{h_1}{d_2 d_3} \right) \right|^2 \ll (2^m + D_1^2 d_3)\, 2^{-m}.$$

6. Use Argument 2 and the **Sobolev–Gallagher inequality** to bound

$$\sum_{d_2} \sum_{d_3} \sum_{h_1} \max_{\alpha \in \mathbb{R}} \left| F_\ell \left(\alpha, \frac{h_1}{d_2 d_3} \right) \right|^2 .$$

Conjecture on $\Theta(n)$

Recall that $\Theta(n) = |\{a \in [2^{n-1}, 2^n) : a$ and $\overleftarrow{a}$ are prime$\}|$ and let $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$.

By a simple heuristic argument, we may expect that $\Theta(n) \approx \Theta_{\mathsf{exp}}(n)$ where

$$\Theta_{\mathsf{exp}}(n) = \frac{3\left(\mathrm{Li}(2^n) - \mathrm{Li}(2^{n-1})\right)^2}{2^{n-1}} = (3 + o(1))\frac{2^{n-1}}{(\log 2^n)^2} \qquad (n \to +\infty).$$

This agrees with the values of $\Theta(n)$ (see below).

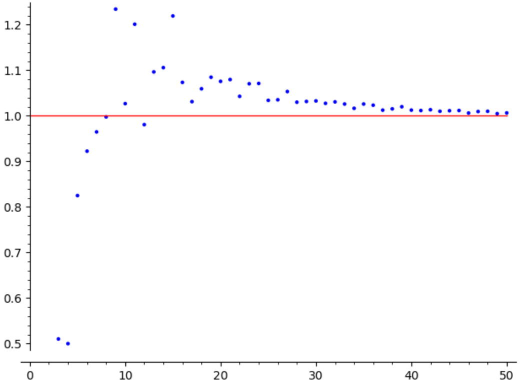
Conjecture:

$$\Theta(n) = (3 + o(1))\frac{2^{n-1}}{(\log 2^n)^2} \qquad (n \to +\infty).$$

Values of $\Theta(n)$

n	$\Theta(n)$	n	$\Theta(n)$
31	7377931	41	4222570054
32	13878622	42	8056984176
33	25958590	43	15315267089
34	48421044	44	29274821854
35	92163237	45	55976669028
36	173672988	46	106505783902
37	325098134	47	204628057694
38	617741968	48	392422557460
39	1177573074	49	749026893680
40	2221353224	50	1440435348050

Values of $\Theta(n)$ for $30 < n \leqslant 50$.



Graph of $\Theta(n)/\Theta_{\text{exp}}(n)$.

Conclusion

- With a sieve argument, we obtain:
  - an upper bound (of the expected order of magnitude) for the number of n-bit **reversible primes**,
  - a lower bound for the number of n-bit **reversible almost primes (at most 8 prime factors)**.
- We obtain an asymptotic formula for the number of n-bit **reversible squarefree integers**.

Conclusion

- With a sieve argument, we obtain:
  - an upper bound (of the expected order of magnitude) for the number of n-bit **reversible primes**,
  - a lower bound for the number of n-bit **reversible almost primes (at most 8 prime factors)**.
- We obtain an asymptotic formula for the number of n-bit **reversible squarefree integers**.

Thank you for your attention!