On Representing Natural Numbers as Differences of Two Distinct Prime Powers

Anish Sola

January 29, 2026

Abstract

We study representations of integers as differences of prime powers,

$$n = p^a - q^b,$$

with distinct prime bases $p \neq q$ and distinct exponents $a \neq b$. We focus on the positive-exponent setting ($a, b \geq 1$) and on the proper-prime-power variant ($a, b \geq 2$), for which the problem is closer in spirit to Goldbach- and Pillai-type questions. We prove elementary structural constraints (notably parity restrictions), propose first-moment heuristics, and outline a computational program.

1 Introduction

Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ and let $\mathbb{P}$ denote the set of primes.

We study a Goldbach-type representation problem in which an integer n is written as a difference of two prime powers, with the two prime bases distinct and with distinct exponents.

2 Definitions and conjectures

Definition 1 (Prime powers and representations)**.** *A* prime power *is a number of the form p^a with $p \in \mathbb{P}$ and $a \in \mathbb{Z}_{\geq 1}$. For $n \in \mathbb{Z}$ define*

$$R(n) := \#\Big\{(p, q, a, b) \in \mathbb{P}^2 \times \mathbb{Z}_{\geq 1}^2 : \ p \neq q, \ a \neq b, \ p^a - q^b = n\Big\},$$

counting ordered *representations.*

Conjecture 1 (Prime-power difference conjecture)**.** *For every $n \in \mathbb{N}$ one has $R(n) \geq 1$; equivalently, each $n \geq 1$ admits*

$$n = p^a - q^b$$

with distinct primes $p \neq q$ and exponents $a, b \geq 1$ satisfying $a \neq b$.

Definition 2 (Minimal size)**.** *For $n \geq 1$ define*

$$M(n) := \min\{\max(p^a, q^b) : (p, q, a, b) \text{ is counted by } R(n)\},$$

with $M(n) = \infty$ if $R(n) = 0$.

Conjecture 2 (Linear-size representations)**.** *There exists an absolute constant $C > 0$ such that for every $n \geq 1$ one has $M(n) \leq Cn$.*

Conjecture 3 (Abundance on average)**.** *One has*

$$\frac{1}{N} \sum_{n \leq N} R(n) \to \infty \qquad \text{as } N \to \infty.$$

2.1 Small examples

The following explicit representations illustrate the constraints $p \neq q$ and $a \neq b$.

$$\begin{aligned} 1 &= 5^1 - 2^2, \\ 2 &= 3^2 - 7^1, \\ 3 &= 2^3 - 5^1, \\ 4 &= 3^2 - 5^1, \\ 5 &= 2^3 - 3^1, \\ 6 &= 5^2 - 19^1, \\ 7 &= 2^4 - 3^2, \\ 8 &= 5^2 - 17^1, \\ 9 &= 2^4 - 7^1, \\ 10 &= 3^3 - 17^1. \end{aligned}$$

2.2 Proper prime powers

For $n \in \mathbb{Z}$ define

$$R_{\geq 2}(n) := \#\{(p, q, a, b) : p \neq q,\ a \neq b,\ a, b \geq 2,\ p^a - q^b = n\}.$$

Conjecture 4 (Proper prime-power difference conjecture)**.** *There exists $N_0 \geq 1$ such that for every $n \geq N_0$ one has $R_{\geq 2}(n) \geq 1$.*

Remark 1. Conjecture 1 is the main (positive-exponent) problem. Conjecture 4 is a substantially harder "proper prime powers only" variant.

3 Unconditional results and basic examples

Theorem 1 (Two explicit infinite families)**.** *For every integer $a \geq 2$ the numbers $2^a - 3$ and $3^a - 5$ satisfy Conjecture 1 via*

$$2^a - 3 = 2^a - 3^1, \qquad 3^a - 5 = 3^a - 5^1.$$

Remark 2 (A concrete partial direction: fixing $b = 1$). Theorem 1 shows that the exponent pattern $b = 1$ already produces infinitely many values of both parities: $2^a - 3$ is odd for all $a \geq 2$, while $3^a - 5$ is even for all $a \geq 2$. This does not approach an "all sufficiently large n" statement, but it isolates a natural subproblem: for which n does there exist a representation $n = p^a - q$ with q prime and $a \geq 2$?

Theorem 2 (An infinite family for proper prime powers)**.** *For every integer $t \geq 2$ one has*

$$n_t := 2^{2t} - 3^3,$$

and n_t admits a representation counted by $R_{\geq 2}(n_t)$. In particular, infinitely many integers satisfy the constraints of Conjecture 4.

Proof. Take $(p, q, a, b) = (2, 3, 2t, 3)$. Then $p \neq q$, $a, b \geq 2$, and $a \neq b$ since $2t \neq 3$ for integer t. Also $n_t > 0$ for $t \geq 2$ because $2^{2t} \geq 16 > 27 = 3^3$. □

4 Elementary constraints

4.1 Parity

[Odd integers force the prime 2] Let $n \geq 1$ be odd. If $n = p^a - q^b$ with distinct primes $p \neq q$ and exponents $a, b \geq 1$, then exactly one of p, q equals 2.

Proof. If both p and q are odd, then $p^a \equiv q^b \equiv 1 \pmod 2$ for all $a, b \geq 1$, hence $p^a - q^b$ is even, contradicting that n is odd. Thus at least one of p, q equals 2. Since $p \neq q$, exactly one equals 2. □

[Even integers force odd bases] Let $n \geq 2$ be even. If $n = p^a - q^b$ with distinct primes $p \neq q$ and exponents $a, b \geq 1$, then both p and q are odd.

Proof. If one of p, q equals 2, then one of p^a, q^b is even and the other is odd (because any odd prime power is odd), so $p^a - q^b$ is odd. Hence an even value cannot occur unless both bases are odd. □

Remark 3. Proposition 4.1 shows that for odd n, any representation as a difference of two prime powers must involve the prime 2.

[A mod 4 refinement when 2 occurs] Assume $n = p^a - q^b$ with distinct primes $p \neq q$ and exponents $a, b \geq 1$.

1. If $p = 2$ and $a \geq 2$, then $n \equiv -q^b \pmod 4$, so $n \equiv 1 \pmod 4$ when $q \equiv 3 \pmod 4$ and b is odd, and $n \equiv 3 \pmod 4$ otherwise.

2. If $q = 2$ and $b \geq 2$, then $n \equiv p^a \pmod 4$, so $n \equiv 1 \pmod 4$ if $p \equiv 1 \pmod 4$ or a is even, and $n \equiv 3 \pmod 4$ if $p \equiv 3 \pmod 4$ and a is odd.

Proof. If $a \geq 2$ then $2^a \equiv 0 \pmod 4$, giving (1). If $b \geq 2$ then $2^b \equiv 0 \pmod 4$, giving (2). The remaining congruence statements follow from $q^b \equiv q \pmod 4$ when b is odd and $q^b \equiv 1 \pmod 4$ when b is even for odd q. □

4.2 Congruences and local admissibility

For fixed exponents a, b and modulus m, the sets

$$\mathcal{P}_a(m) := \{p^a \bmod m : p \in \mathbb{P},\ \gcd(p, m) = 1\}, \qquad \mathcal{P}_b(m) := \{q^b \bmod m : q \in \mathbb{P},\ \gcd(q, m) = 1\}$$

are typically strict subsets of $\mathbb{Z}/m\mathbb{Z}$.

Definition 3 (Local admissibility)**.** *Fix a modulus $m \geq 2$. An integer n is m-*admissible *for Conjecture 1 if there exist residues $u, v \in \mathbb{Z}/m\mathbb{Z}$ and exponents $a, b \geq 1$ with $a \neq b$ such that*

$$u \in \mathcal{P}_a(m), \quad v \in \mathcal{P}_b(m), \quad \textit{and} \quad u - v \equiv n \pmod m.$$

Remark 4. A genuine congruence obstruction to Conjecture 1 would manifest as a modulus m for which some residue class fails to be m-admissible. Proposition 4.1 can be interpreted as a first "local" restriction at $m = 2$.

Theorem 3 (Infinitely many solutions in each residue class mod 4)**.** *For each residue class $r \in \{0, 1, 2, 3\}$ there exist infinitely many $n \equiv r \pmod 4$ that satisfy Conjecture 1. Moreover, one may choose representations with $b = 1$.*

Proof. We exhibit explicit infinite families.

- $r \equiv 1 \pmod 4$: for any even $a \geq 2$, $2^a - 3 \equiv 1 \pmod 4$ and $2^a - 3 = 2^a - 3^1$.
- $r \equiv 3 \pmod 4$: for any odd $a \geq 3$, $2^a - 3 \equiv 3 \pmod 4$.
- $r \equiv 0 \pmod 4$: for any even $a \geq 2$, $3^a - 5 \equiv 0 \pmod 4$.
- $r \equiv 2 \pmod 4$: for any odd $a \geq 3$, $3^a - 5 \equiv 2 \pmod 4$.

Each family is infinite and uses distinct primes with exponents a and 1. □

Theorem 4 (Proper prime powers in each residue class mod 4)**.** *For each residue class $r \in \{0, 1, 2, 3\}$ there exist infinitely many $n \equiv r \pmod 4$ such that $R_{\geq 2}(n) \geq 1$.*

Proof. We give explicit infinite families.

- $r \equiv 1 \pmod 4$: take $n_t = 2^{2t} - 3^3$ from Theorem 2; then $n_t \equiv 1 \pmod 4$.
- $r \equiv 3 \pmod 4$: for $t \geq 3$, $m_t := 2^{2t} - 5^2 > 0$ satisfies $m_t \equiv 3 \pmod 4$ and is represented by $(p, q, a, b) = (2, 5, 2t, 2)$.
- $r \equiv 0 \pmod 4$: for $t \geq 2$, $\ell_t := 5^{2t} - 13^2 > 0$ satisfies $\ell_t \equiv 0 \pmod 4$ and is represented by $(p, q, a, b) = (5, 13, 2t, 2)$.
- $r \equiv 2 \pmod 4$: for $t \geq 2$, $k_t := 5^{2t} - 3^3 > 0$ satisfies $k_t \equiv 2 \pmod 4$ and is represented by $(p, q, a, b) = (5, 3, 2t, 3)$.

All families have exponents at least 2, distinct primes, and distinct exponents. □

5 Heuristics: a model and predictions

We sketch a probabilistic model intended to explain why representations should exist and why they should be plentiful.

5.1 A first-moment heuristic for $\mathbb{E}R(n)$

Fix $n \geq 1$ and consider candidate values of q^b. If we restrict attention to representations with $q^b \leq X$, then we are asking whether $n + q^b$ is a prime power. The prime case dominates, so we approximate

$$\mathbb{P}(n + q^b \text{ is prime}) \approx \frac{1}{\log(n + q^b)}.$$

Summing this over all prime powers $q^b \leq X$ suggests a first-moment estimate

$$\mathbb{E}R(n; X) \approx \sum_{q^b \leq X} \frac{1}{\log(n + q^b)} \approx \frac{\#\{q^b \leq X\}}{\log(n + X)}. \tag{1}$$

Using $\#\{q^b \le X\} = \pi(X) + O(X^{1/2}) \sim X/\log X$ gives the rough prediction

$$\mathbb{E}R(n;X) \approx \frac{X}{\log X\ \log(n+X)}.$$

In particular, taking $X \asymp n$ yields

$$\mathbb{E}R(n;n) \asymp \frac{n}{(\log n)^2},$$

which tends to infinity. This is consistent with Conjecture 3 and suggests that not only should representations exist, but there should typically be many of them.

5.2 Why the linear-size strengthening is plausible

The estimate above also motivates Conjecture 2: if one searches only among prime powers $q^b \le Cn$, the heuristic still predicts

$$\mathbb{E}R(n;Cn) \asymp \frac{n}{(\log n)^2},$$

so restricting to prime powers of size $O(n)$ should still leave many opportunities for $n + q^b$ to be prime.

5.3 Why the model might fail

The heuristic treats primality of the shifted values $n + q^b$ as roughly independent across different prime powers and ignores local congruence biases. A serious obstruction would have to manifest as a strong systematic congruence restriction forcing $n + q^b$ to be composite for all admissible q^b in a large range.

Remark 5. The estimates in this section are intended as motivation only; they are not evidence in the absence of either rigorous bounds or extensive computation.

5.4 Exponents ≥ 2

If one insists on $a, b \ge 2$, the available set of prime powers up to X drops to

$$\sum_{k\ge 2} \pi(X^{1/k}) \asymp \frac{X^{1/2}}{\log X},$$

and the same first-moment computation suggests a much smaller expected count. For instance, taking $X \asymp n$ and restricting to $q^b \le X$ with $b \ge 2$ gives the heuristic

$$\mathbb{E}R_{\ge 2}(n;X) \approx \sum_{q^b \le X,\ b\ge 2} \frac{1}{\log(n+q^b)} \asymp \frac{X^{1/2}}{\log X\ \log(n+X)}.$$

In particular, at $X \asymp n$ this is of order $\sqrt{n}/(\log n)^2$, far smaller than the $n/(\log n)^2$ prediction when exponent 1 is allowed. This gap is one reason Conjecture 4 is plausibly much deeper.

6 Related problems

The conjecture sits near classical additive/multiplicative representation questions. Examples include Goldbach-type problems (integers as sums/differences of primes) and problems on gaps between powers (e.g., Pillai-type questions on $x^a - y^b = n$). We include a short bibliography to orient future work.

7 Computational program and evidence

We recommend the following experimental protocol.

7.1 Search strategy

Fix a bound N and attempt to find, for each $1 \le n \le N$, at least one representation. It is useful to track two nested problems separately:

- Conjecture 1: allow all exponents ≥ 1;
- Conjecture 4: restrict to exponents ≥ 2.

A practical search is:

1. Choose the target conjecture and a search window B for prime powers $q^b \le B$.
2. Enumerate candidate prime powers q^b in the allowed exponent range.
3. For each n and each candidate q^b, test whether $n + q^b$ is a prime power p^a in the allowed exponent range and with $a \ne b$.
4. Record the smallest-size solution (minimizing $\max(p^a, q^b)$) and the exponent pair (a, b).

7.2 What to report (paper-ready)

To make computational work scientifically useful (and comparable across implementations), we recommend reporting:

- the verification range $[1, N]$ and the search cutoff B;
- the maximum observed minimal size ratio

$$\max_{1 \le n \le N} \frac{M(n)}{n}$$

  (or the analogous quantity for $R_{\ge 2}$);
- the list of the "hardest" values of n (those with largest $M(n)$) together with an explicit minimizing representation;
- the empirical distribution of exponent pairs (a, b) in minimizing representations.

8 Conditional strengthenings (clearly conjectural)

The following strengthenings capture the kind of "all sufficiently large n" statement that would push the project beyond a conjectural framework. We state them explicitly as conjectures.

Conjecture 5 (Fixed $b = 1$ for large even integers)**.** *There exists $N_1 \ge 1$ such that for every even $n \ge N_1$ there are a prime q and a prime power p^a with $a \ge 2$ such that*

$$n = p^a - q.$$

Conjecture 6 (Density-one proper prime-power representations)**.** *The set*

$$\{n \in \mathbb{N} : R_{\ge 2}(n) \ge 1\}$$

has natural density 1.

9 Open questions

Question 1 (Density of representations)**.** *Does* $R(n) \to \infty$ *along a density-one subset of integers? Can one obtain lower bounds for* $R(n)$ *on average?*

Question 2 (Both exponents at least 2)**.** *Is it still true that every sufficiently large* $n \in \mathbb{N}$ *can be written as* $p^a - q^b$ *with* $a, b \geq 2$*,* $p \neq q$*, and* $a \neq b$*?*