2-Adic Stratification of Odd Primes via XOR Signatures

Thiago Fernandes Motta Massensini Silva

thiago@massensini.com.br

Abstract

We present a complete classification of odd primes based on the 2-adic valuation and elementary binary operations. For each odd prime P, we define a signature (T, K), where T is the 2-adic valuation of an even neighbor of P and K is obtained via the XOR operation between adjacent integers. We prove that every odd prime belongs to exactly one of three disjoint families, determined explicitly. In particular, twin primes are characterized by the relation $K = 2^{T+1} - 2$, while non-twin primes are divided into two complementary families according to whether $v_2(P-1) \geq 2$ or $v_2(P-1) = 1$. All proofs are elementary and do not rely on any conjectural hypotheses.

1 Introduction

This work establishes a complete stratification of odd primes into three mutually exclusive families, using only the 2-adic valuation and the binary XOR operator.

The central idea consists of assigning to each odd prime P two invariants:

- a valuation $T = v_2(P+1)$ if P is a twin prime, or $T = v_2(P-1)$ otherwise;
- a signature K obtained by applying XOR to integers adjacent to P.

The pair (T, K) assumes, for each odd prime, one of the forms specified in Theorem 5.1. The classification is complete, deterministic, and without exceptions.

2 Fundamental Definitions

Definition 2.1 (2-adic valuation). *For a nonzero integer m, we define*

$$v_2(m) = \max\{k \geq 0 : 2^k \mid m\}.$$

Equivalently, $v_2(m)$ is the number of consecutive trailing zeros in the binary representation of m.

Definition 2.2 (T-Value)**.** *Let P be an odd prime. We define*

$$T = \begin{cases} v_2(P+1), & \text{if } (P, P+2) \text{ is a twin prime pair,} \\ v_2(P-1), & \text{otherwise.} \end{cases}$$

Definition 2.3 (K-Value)**.** *Let P be an odd prime. We define*

$$K = \begin{cases} P \oplus (P+2), & \text{if } (P, P+2) \text{ is a twin prime pair,} \\ (P-1) \oplus (P+1), & \text{otherwise,} \end{cases}$$

where $\oplus$ denotes the bitwise XOR operator.

Definition 2.4 (2-adic signature)**.** *The pair (T, K) is called the* 2-adic signature *of the prime P.*

Remark 2.5. *The construction of (T, K) depends on knowing beforehand whether $P + 2$ is prime. Therefore, (T, K) does not constitute an independent test for twin primality, but rather a* structural classification *of odd primes.*

3 Auxiliary Lemma

Lemma 3.1. *Let $n \geq 0$ be an integer whose binary representation ends with exactly $\rho \geq 0$ bits equal to 1. Then*

$$n \oplus (n+1) = 2^{\rho+1} - 1.$$

Proof. We write n in binary as

$$n = (\cdots b)\underbrace{11\cdots1}_{\rho \text{ ones}},$$

where b is the bit immediately to the left of the final block of ones.

Adding 1 to n, the ρ final bits equal to 1 become 0, and the bit b is incremented. Thus, in the $\rho + 1$ least significant positions, n and $n + 1$ are bitwise complementary, while the higher-order bits remain equal.

Therefore,

$$n \oplus (n+1) = \underbrace{11\cdots1}_{\rho+1 \text{ ones}} = 2^{\rho+1} - 1.$$

□

4 Structural Families

We prove that every odd prime belongs to exactly one of the following families:

$$\mathcal{C}_{\text{twin}} = \{(T, 2^{T+1} - 2) : T \geq 1\},$$

$$\mathcal{C}_{\geq 2} = \{(T, 2) : T \geq 2\},$$

$$\mathcal{C}_{T=1} = \{(1, 2^m - 2) : m \geq 3\}.$$

4.1 Family I: Twin Primes

Theorem 4.1 (Characterization of twin primes)**.** *If* $(P, P+2)$ *is a twin prime pair and* $T = v_2(P+1)$*, then*

$$K = P \oplus (P+2) = 2^{T+1} - 2.$$

In particular, $(T, K) \in \mathcal{C}_{\mathrm{twin}}$*.*

Proof. Let $P + 1 = 2^T M$ with M odd and $T \geq 1$. Then

$$P = 2^T M - 1, \qquad P + 2 = 2^T M + 1.$$

The number $2^T M$ has a binary representation ending in exactly T zeros. Subtracting 1 produces T final bits equal to 1:

$$P = (\cdots)\underbrace{11\cdots1}_{T \text{ ones}}.$$

Adding 1 to $2^T M$ produces a single bit 1 in the least significant position:

$$P + 2 = (\cdots)\underbrace{00\cdots01}_{T \text{ zeros followed by } 1}.$$

The bits of order $\geq T+1$ coincide in P and $P+2$. In positions $0, 1, \ldots, T$:

- Position 0: both have bit 1, so XOR $= 0$.
- Positions $1, 2, \ldots, T$: P has bit 1, $P+2$ has bit 0, so XOR $= 1$.

Therefore,

$$K = P \oplus (P+2) = 2^1 + 2^2 + \cdots + 2^T = 2^{T+1} - 2.$$

□

4.2 Family II: Non-Twins with $T \geq 2$

Theorem 4.2. *If* P *is a non-twin prime and* $T = v_2(P-1) \geq 2$*, then*

$$K = (P-1) \oplus (P+1) = 2.$$

In particular, $(T, K) \in \mathcal{C}_{\geq 2}$*.*

Proof. We write $P - 1 = 2^T M$ with M odd and $T \geq 2$. Since $T \geq 2$, we have $4 \mid (P-1)$, so $P - 1$ ends in $\cdots 00_2$.

Then $P + 1 = (P-1) + 2$ ends in $\cdots 10_2$.

The two integers $P - 1$ and $P + 1$ coincide in all bits of order ≥ 2 and differ only in the bit at position 1. Therefore,

$$K = (P-1) \oplus (P+1) = 10_2 = 2.$$

□

4.3 Family III: Non-Twins with $T = 1$

Theorem 4.3. *If P is a non-twin prime and $T = v_2(P-1) = 1$, then there exists $m \geq 3$ such that*

$$K = (P-1) \oplus (P+1) = 2^m - 2.$$

In particular, $(T, K) \in \mathcal{C}_{T=1}$.

Proof. We have $P - 1 = 2M$ with M odd (since $v_2(P-1) = 1$). Then

$$K = (P-1) \oplus (P+1) = 2M \oplus (2M+2) = 2 \cdot (M \oplus (M+1)),$$

where the last equality follows from the fact that multiplication by 2 is equivalent to shifting all bits one position to the left.

Since M is odd, its binary representation ends in at least one bit 1. Let $\rho \geq 1$ be the number of consecutive final bits equal to 1 in M. By Lemma 3.1,

$$M \oplus (M+1) = 2^{\rho+1} - 1.$$

Therefore,

$$K = 2(2^{\rho+1} - 1) = 2^{\rho+2} - 2.$$

Setting $m = \rho + 2$, we have $m \geq 3$ (since $\rho \geq 1$) and $K = 2^m - 2$. $\square$

5 Main Theorem

Theorem 5.1 (2-adic stratification of primes)**.** *For every odd prime P, the signature (T, K) belongs to exactly one of the three families:*

$$\mathcal{C}_{\text{twin}}, \quad \mathcal{C}_{\geq 2}, \quad \mathcal{C}_{T=1}.$$

These families are mutually disjoint and exhaustive.

Proof. **Exhaustiveness:** Let P be an odd prime.

- If $(P, P+2)$ is a twin prime pair, then $(T, K) \in \mathcal{C}_{\text{twin}}$ by Theorem 4.1.
- If P is not a twin and $T = v_2(P-1) \geq 2$, then $(T, K) \in \mathcal{C}_{\geq 2}$ by Theorem 4.2.
- If P is not a twin and $T = v_2(P-1) = 1$, then $(T, K) \in \mathcal{C}_{T=1}$ by Theorem 4.3.

Since P is odd, $P - 1$ is even, so $v_2(P-1) \geq 1$. The three cases are exhaustive.

Disjointness: We verify that the families do not intersect.

- $\mathcal{C}_{\text{twin}} \cap \mathcal{C}_{\geq 2} = \emptyset$: In $\mathcal{C}_{\geq 2}$, we have $K = 2$. In $\mathcal{C}_{\text{twin}}$, $K = 2$ would require $T = 1$. But $\mathcal{C}_{\geq 2}$ requires $T \geq 2$.
- $\mathcal{C}_{\text{twin}} \cap \mathcal{C}_{T=1} = \emptyset$: In $\mathcal{C}_{T=1}$, we have $T = 1$ and $K = 2^m - 2$ with $m \geq 3$, so $K \geq 6$. In $\mathcal{C}_{\text{twin}}$ with $T = 1$, we would have $K = 2$. Since $6 \neq 2$, there is no intersection.
- $\mathcal{C}_{\geq 2} \cap \mathcal{C}_{T=1} = \emptyset$: Disjoint by definition, since $\mathcal{C}_{\geq 2}$ requires $T \geq 2$ and $\mathcal{C}_{T=1}$ requires $T = 1$.

$\square$

6 Examples

Table 1 illustrates the classification.

P	Twin?	(T, K)	Family
5	Yes	$(1, 2)$	$\mathcal{C}_{\text{twin}}$
71	Yes	$(3, 14)$	$\mathcal{C}_{\text{twin}}$
7	No	$(1, 14)$	$\mathcal{C}_{T=1}$
47	No	$(1, 30)$	$\mathcal{C}_{T=1}$
13	No	$(2, 2)$	$\mathcal{C}_{\geq 2}$
97	No	$(5, 2)$	$\mathcal{C}_{\geq 2}$

Table 1: Signatures (T, K) for selected primes.

7 Conclusion

The pair (T, K) provides a complete and deterministic stratification of odd primes into three mutually exclusive families:

- $\mathcal{C}_{\text{twin}}$: twin primes, characterized by $K = 2^{T+1} - 2$;
- $\mathcal{C}_{\geq 2}$: non-twin primes with $v_2(P - 1) \geq 2$, characterized by $K = 2$;
- $\mathcal{C}_{T=1}$: non-twin primes with $v_2(P - 1) = 1$, characterized by $K = 2^m - 2$ with $m \geq 3$.

All results derive exclusively from properties of binary representation and 2-adic valuation, without analytical or conjectural hypotheses.

Natural extensions include the investigation of analogous structures for p-adic valuations with odd p, as well as possible connections with local p-adic L-functions.