# The Pow-XOR Equivalence Problem and an Efficient Solution

Akshay Trivedi

## 1 Problem Statement

When writing equations over ASCII text, people often use the '^' character to denote exponentiation. For example, `2 ^ 3 + 4` means $2^3+4$ which evaluates to $12$. Many programming languages use the same symbol for the "bitwise exclusive or" operation, and under this definition the expression `(2 ^ 3) + 4` evaluates to 5. For what values of $a$ and $b$ do these two meanings of '^' make the expression `a ^ b` take on the same value (using unsigned $n$-bit integers, i.e. modulo $2^n$)?

### 1.1 Formal Problem Statement

#### 1.1.1 Preliminary Stuff

The symbol $\mathbb{N}$ denotes the set of natural numbers including zero; i.e. $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

The symbol $\mathbb{Z}$ denotes the set of integers, which are the natural numbers and their negations (additive inverses); i.e. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

**Definition 1.1 (congruence modulo an integer)**
*Let $x, y \in \mathbb{Z},\ n \in \mathbb{N}$. For $x$ and $y$ to be congruent modulo $n$, denoted by $x \equiv y \pmod{n}$, means that $x = y + k \cdot n$ for some $k \in \mathbb{Z}$.*

**Lemma 1.2**
*There exists a unique binary operation $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ that assigns to every $x, y \in \mathbb{Z}$ some $f(x, y) \in \mathbb{Z}$ with the following properties:*

1. *This operation is associative, has zero as an identity, has the property that every element is its own inverse, and is commutative. In other words, for all integers $x, y, z \in \mathbb{Z}$:*

$$\begin{gathered}\textit{Associativity: } f(f(x,y),z) = f(x,f(y,z)) \\ \textit{Zero Identity: } f(0,x) = f(x,0) = x \\ \textit{Self-inverse: } f(x,x) = 0 \\ \textit{Commutativity: } f(x,y) = f(y,x)\end{gathered}$$

2. *For all natural numbers $n \in \mathbb{N}$, congruence modulo $2^n$ respects $f$; in other words, for all $x_1, x_2, y_1, y_2 \in \mathbb{Z}$,*

$$\textit{if } x_1 \equiv x_2 \pmod{2^n} \textit{ and } y_1 \equiv y_2 \pmod{2^n} \textit{ then } f(x_1, y_1) \equiv f(x_2, y_2) \pmod{2^n}.$$

*proof.*

**Definition 1.3 (bitwise exclusive or / XOR)**
*For every $x, y \in \mathbb{Z}$, the bitwise exclusive or/XOR of $x$ and $y$ is the $x \oplus y \in \mathbb{Z}$ assigned to them by the operation described in 1.2; i.e. $x \oplus y = f(x, y)$.*

#### 1.1.2 The Problem

Let $n \in \mathbb{N}$.

**Definition 1.4 ($X_n$)**
*$X_n$ is the set of all solutions $(a, b) \in \mathbb{Z} \times \mathbb{Z},\ 0 \leq a, b < 2^n$ to the congruence $a^b \equiv a \oplus b \pmod{2^n}$.*

The problem is to design an efficient algorithm which, given $n$, enumerates all of of $X_n$. Bonus points: given any of the three variables $a, b \in \mathbb{Z},\ n \in \mathbb{N}$, enumerate the possibilities for the rest of the variables.

## 1.2 Examples

- For all $n \in \mathbb{N},\ n \geq 1$, $1^0 \equiv 1 \pmod{2^n}$ and $1 \oplus 0 = 1$, so $(1,0) \in X_n$.
- For all $n \in \mathbb{N},\ n \geq 1$, $(2^n-1)^{2^n-2} \equiv 1 \pmod{2^n}$ and $(2^n-1) \oplus (2^n-2) \equiv 1$, so $(n-1, n-2) \in X_n$.
- $0^0 = 1 \equiv 0 = 0 \oplus 0 \pmod{2^0}$, so $(0,0) \in X_0$ (in fact, $X_0 = \{(0,0)\}$).
- $(3109287477, 2325659185) \in X_{32}$ because

$$3109287477^{869091332} \equiv 2325659185 = 3109287477 \oplus 869091332 \pmod{2^{32}}.$$

## 1.3 Properties of $X_n$ (warning: spoilers)

You might expect the size of $X_n$ to be kind of "random-ish" since modular exponentiation and bitwise exclusive-or come from different and seemingly unrelated structures on $\mathbb{Z}_{2^n}$. However, as it turns out,

**Proposition 1.5 (Strange Fact)**
*For all* $n \in \mathbb{N},\ n \geq 1$, $|X_n| = 2^n - 1$.

After observing this result, you might expect that each solution $(a,b) \in X_n$ is uniquely determined by either $a$ or $b$. My first guess was $a$ because I expected the base to dictate more properties of the exponent operation, like the number of exponents which map to unique powers $\pmod{2^n}$ which is due to Euler's Theorem.

I collected the frequencies of $a$ and $b$ for $(a,b) \in X_n$ (for $n \geq 1$), and was initially surprised by the results:

- $b$ is always even. $b = 0$ occurs exactly once, and comes from the solution $(a,b) = (1,0) \in X_n$. Every positive even integer $0 < b < 2^n$ occurs exactly twice. By summing the frequencies of $b$'s, $|X_n| = 2 \cdot (2^{n-1} - 1) + 1 = 2^n - 1$ since there are two solutions for each of the $2^{n-1} - 1$ even positive integers and one extra solution for $b = 0$.
- Every odd $a$ occurs exactly once. There are $2^{n-1}$ solutions with odd $a$.
- $a = 0$ never occurs for any $n$. *Almost* every positive even $a$ occurs once. Depending on $n$, there are a few exceptions that either occur exactly twice or never occur at all, and both kinds of exceptions are equinumerous (excluding $a = 0$). Hence there are $2^{n-1} - 1$ solutions with even $a$.

| $n$ | $a$ occuring exactly twice (duplicate values) | *nonzero* $a$ occuring zero times (absent values) |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | 6 | 2 |
| 4 | 6 | 2 |
| 5 | 6 | 2 |
| 6 | 38 | 2 |
| 7 | 38, 70 | 2, 6 |
| 8 | 166, 70 | 2, 6 |
| 9 | 422, 260, 70 | 2, 4, 6 |
| 10 | 934, 260, 582 | 2, 4, 6 |
| 11 | 1958, 260, 1606, 1034 | 2, 4, 6, 10 |
| 12 | 4006, 260, 1606, 1034 | 2, 4, 6, 10 |
| 13 | 8102, 260, 1606, 1034 | 2, 4, 6, 10 |
| 14 | 8102, 260, 1606, 9226 | 2, 4, 6, 10 |
| 15 | 8102, 260, 17990, 25610, 16398 | 2, 4, 6, 10, 14 |
| 16 | 40870, 260, 50758, 58378, 16398 | 2, 4, 6, 10, 14 |

- In fact, most solutions with a positive even $a$ satisfy $a = b$. Theonly exceptions are when $a$ is in the left-hand-side column of the table above and $b$ is the corresponding value from the right-hand-side column. So for example, in row 16, the third duplicate $a$ is 50758, and the third absent $a$ is 6. This means $50758^6 = 50758 \oplus 6 \pmod{2^{16}}$. Note that the absent $a$ takes the place of $b$ in the equation $a^b \equiv a \oplus b \pmod{2^n}$.

# 2 Solution

## 2.1 Preliminary Stuff

The following lemmas, in addition to basic integer arithmetic, are used in the proof. These lemmas have really trivial proofs, and are either generally well-known or conveniently rewritten from well-known statements.

**Lemma 2.1**
*For every $x \in \mathbb{Z},\ n \in \mathbb{N},\ n \geq 1$, there exists a unique $x_0 \in \mathbb{Z},\ 0 \leq x_0 < n$, such that $x_0 \equiv x \pmod{n}$.*

*proof.*

**Definition 2.2 (reduction modulo an integer)**
*For every $x \in \mathbb{Z},\ n \in \mathbb{N},\ n \geq 1$, the reduction of $x \pmod{n}$ is the $x_0$ which satisfies 2.1.*

# 3 Proving All of the Preliminary Stuff

## 3.1 Defining XOR

The assumption underpinning this entire document is that there is a well-defined operation satisfying the XOR axioms listed at the beginning. Indeed, not only does one exist, but it is unique. This shall now be proven by defining the XOR operation formally and showing that it alone satisfies the stated axioms.

*Proof (1.2)*
Existence:

The first step is to prove by induction on $n \in \mathbb{N}$ that every $x \in \mathbb{Z},\ 0 \leq x < 2^n$ can be written uniquely as an expression in the form $\sum_{k \in S} 2^k$ for some set of natural numbers $S \subseteq \mathbb{N},\ \max S < n$ for all $n \in \mathbb{N}$.

- When $n = 0$, the only $x \in \mathbb{Z},\ 0 \leq x < 2^n = 1$ is $x = 0$, so $S = \emptyset$ is the only set that works.
- Suppose the statement holds for $n \in \mathbb{N}$. Let $x \in \mathbb{Z},\ 0 \leq x < 2^{n+1}$. Either $0 \leq x < 2^n$ or $2^n \leq x < 2^{n+1}$.
  - If $0 \leq x < 2^n$, then by the inductive hypothesis $x$ can be written uniquely as an expression in the form $\sum_{k \in S} 2^k$ for some set of natural numbers $S \subseteq \mathbb{N},\ \max S < n < n+1$. Also, $n$ cannot be included in the set because this would put the sum over $x$, so the expression is unique.
  - If $2^n \leq x < 2^{n+1}$, then $0 \leq x - 2^n < 2^n$ so by the inductive hypothesis $x - 2^n$ can be written in the form $\sum_{k \in S} 2^k$ for some set of natural numbers $S \subseteq \mathbb{N},\ \max S < n$, which means $x$ can be written as $\sum_{k \in S} 2^k + 2^n = \sum_{k \in S \cup \{n\}} 2^k$. Also, $n$ must be included in the set because otherwise the sum would remain below $x$, so the expression is unique.

Since every $x \in \mathbb{Z}\, 0 \leq x$ is less than $2^n$ for some $n \in \mathbb{N}$, and adding higher powers of two will not produce more ways to express $x$, it follows that every nonnegative integer can be written uniquely as an expression in the form $\sum_{k \in S} 2^k$ for some finite set of natural numbers $S \subseteq \mathbb{N}$.

Next is to prove by induction on $n \in \mathbb{N}$ that every $x \in \mathbb{Z},\ -2^n \leq x < 0$ can be written uniquely as an expression in the form $-1 - \sum_{k \in S} 2^k$ for some set of natural numbers $S \subseteq \mathbb{N},\ \max S < n$.

- When $n = 0$, the only $x \in \mathbb{Z},\ -2^0 = -1 \leq x < 0$ is $x = -1$, so $S = \emptyset$ is the only set that works.
- Suppose the statement holds for $n \in \mathbb{N}$. Let $x \in \mathbb{Z},\ -2^{n+1} \leq x < 0$. Either $2^{n+1} \leq x < -2^n$ or $-2^n \leq x < 0$.
  - If $-2^n \leq x < 0$, then by the inductive hypothesis $x$ can be written uniquely as an expression in the form $-1 - \sum_{k \in S} 2^k$ for some set of natural numbers $S \subseteq \mathbb{N},\ \max S < n < n+1$. Also, $n$ cannot be included in the set because this would put the sum under $x$, so the expression is unique.

– If $-2^{n+1} \leq x < -2^n$, then $-2^n \leq x + 2^n < 0$ so by the inductive hypothesis $x + 2^n$ can be written in the form $-1 - \sum_{k \in S} 2^k$ for some set of natural numbers $S \subseteq \mathbb{N}$, $\max S < n$, which means $x$ can be written as $-1 - \sum_{k \in S} 2^k - 2^n = -1 - \sum_{k \in S \cup \{n\}} 2^k$. Also, $n$ must be included in the set because otherwise the sum would remain above $x$, so the expression is unique.

Since every $x \in \mathbb{Z} x < 0$ is greater than $-2^n$ for some $n \in \mathbb{N}$, and adding higher powers of two will not produce more ways to express $x$, it follows that every negative integer can be written uniquely as an expression in the form $-1 - \sum_{k \in S} 2^k$ for some finite set of natural numbers $S \subseteq \mathbb{N}$.

The XOR operation can then be defined as follows:

For any two finite sets of natural numbers $S_1, S_2 \subseteq \mathbb{N}$:

$$\begin{gathered}
\left(\sum_{k \in S_1} 2^k\right) \oplus \left(\sum_{k \in S_1} 2^k\right) = \left(\sum_{k \in S_1 \Delta S_2} 2^k\right) \\
\left(-1 - \sum_{k \in S_1} 2^k\right) \oplus \left(\sum_{k \in S_1} 2^k\right) = \left(-1 - \sum_{k \in S_1 \Delta S_2} 2^k\right) \\
\left(\sum_{k \in S_1} 2^k\right) \oplus \left(-1 - \sum_{k \in S_1} 2^k\right) = \left(-1 - \sum_{k \in S_1 \Delta S_2} 2^k\right) \\
\left(-1 - \sum_{k \in S_1} 2^k\right) \oplus \left(-1 - \sum_{k \in S_1} 2^k\right) = \left(\sum_{k \in S_1 \Delta S_2} 2^k\right)
\end{gathered}$$

Where $S_1 \Delta S_2$ denotes the symmetric difference of $S_1$ and $S_2$. The axioms can be checked "visually" for the above definition.

Uniqueness:

Let $f, g : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ be two operations satisfying the axioms given for XOR. By the axioms, $(\mathbb{Z}, f, 0)$ and $(\mathbb{Z}, g, 0)$ are both Abelian groups. The statement that, for all $n \in \mathbb{N}$, congruence $\pmod{2^n}$ respects $f$ and $g$ is equivalent to saying that $2^n \cdot \mathbb{Z}$ is a subgroup (with the congruence classes forming its cosets) in both of the groups $(\mathbb{Z}, f, 0)$ and $(\mathbb{Z}, g, 0)$, which is normal since both groups are Abelian, for all $n \in \mathbb{N}$. Additionally, each subgroup in the sequence $\{2^n \cdot \mathbb{Z}\}_{n=0}^{\infty}$ is a subgroup of the previous one with an index of $[2^n \cdot \mathbb{Z} : 2^{n+1} \cdot \mathbb{Z}] = 2$. Thus, for for both $(\mathbb{Z}, f, 0)$ and $(\mathbb{Z}, g, 0)$, the quotients of $\mathbb{Z}$ by each of these subgroups is uniquely determined by the previous via the induced isomorphism $\mathbb{Z}/(2^{n+1} \cdot \mathbb{Z}) \cong \mathbb{Z}_2 \times \mathbb{Z}/(2^n \cdot \mathbb{Z})$, and the first one is just the trivial group $\mathbb{Z}/\mathbb{Z}$, so quotients $\mathbb{Z}/(2^n \cdot \mathbb{Z})$ are identical for all $n \in \mathbb{N}$. As a result, for all $x, y \in \mathbb{Z}$, $f(x, y) \equiv g(x, y) \pmod{2^n}$, so $f(x, y) - g(x, y)$ divides $2^n$, for all $n \in \mathbb{N}$. Zero is the only integer that can divide every power of two, so $f(x, y) - g(x, y) = 0$ which means $f(x, y) = g(x, y)$ for all $x, y \in \mathbb{Z}$.