The Pow-XOR Confusion 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 with 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 the same value (using unsigned n-bit integers)?

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 $k \in \mathbb{Z}$. The n is called the modulus.

Lemma 1.2
For every $x \in \mathbb{Z},\ n \in \mathbb{N}$, there exists a unique $d \in \{0, 1\}$ such that $x \equiv 2^n \cdot d + x_r \pmod{2^{n+1}}$ for some $x_r \in \mathbb{Z},\ 0 \le x_r < 2^n$.

Definition 1.3 (bit of an integer)
For every $x \in \mathbb{Z},\ n \in \mathbb{N}$, the n^{th} bit of x is the $d \in \{0, 1\}$ which satisfies 1.2.

Lemma 1.4
For every $x, y \in \mathbb{Z}$, there exists a unique $w \in \mathbb{Z}$ such that for all $n \in \mathbb{N}$, the n^{th} bit of w is 1 if and only if exactly one of the n^{th} bits of x and y is 1.

Definition 1.5 (exclusive-or / XOR)
For every $x, y \in \mathbb{Z}$, the exclusive-or/XOR of x and y is the integer w which satisfies 1.4 and is denoted by $x \oplus y = w$.

1.1.2 The Problem

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

Definition 1.6 (X_n)
X_n is the set of all solutions $(a, b) \in \mathbb{Z} \times \mathbb{Z},\ 0 \le a, b < 2^n$ 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 if, given only one or two of the three variables a, b, and n, the algorithm can efficiently enumerate all possibilities for the remaining variables.

1.2 Examples

- For all $n \in \mathbb{N},\ n \ge 1$, $1^0 \equiv 1 \pmod{2^n}$ and $1 \oplus 0 = 1$, so $(1, 0) \in X_n$.
- For all $n \in \mathbb{N},\ n \ge 1$, $(2^n - 1)^{2^n - 2} \equiv 1 \pmod{2^n}$ 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: This section contains minor spoilers for the solution. I thought this problem was pretty fun, so I encourage you to stop here and try it for yourself if you like algebra and number theory.

You might expect the size of X_n to be kind of "random-ish" and difficult to compute 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 1.7 (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
17	106406, 65796, 50758, 123914, 16398	2, 4, 6, 10, 14
18	237478, 65796, 181830, 254986, 16398	2, 4, 6, 10, 14
19	237478, 65796, 181830, 254986, 278542, 262162	2, 4, 6, 10, 14, 18
20	237478, 65796, 181830, 779274, 278542, 262162	2, 4, 6, 10, 14, 18
21	1286054, 65796, 1230406, 1827850, 1327118, 262162	2, 4, 6, 10, 14, 18
22	3383206, 2162948, 3327558, 1827850, 1327118, 262162	2, 4, 6, 10, 14, 18

- In fact, most solutions with a positive even a satisfy $a = b$. The only 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 22, the second duplicate a is 2162948, and the second absent a is 4. This means $2162948^4 = 2162948 \oplus 4 \pmod{2^{22}}$. 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 (congruence modulo an integer is an equivalence relation)
For every $n \in \mathbb{N}$, congruence modulo n is an equivalence relation (transitive, symmetric, reflexive). In other words, for all $x, y, z \in \mathbb{Z}$:

$$\text{if } x \equiv y \pmod{n}, \text{ and } y \equiv z \pmod{n} \text{ then } x \equiv z \pmod{n}$$
$$\text{if } x \equiv y \pmod{n} \text{ then } y \equiv x \pmod{n}$$
$$x \equiv x \pmod{n}$$

Lemma 2.2 (reducing the modulus)
For every $x, y \in \mathbb{Z}$, $n, n' \in \mathbb{Z}$, if $x \equiv y \pmod{n}$ and $n \equiv 0 \pmod{n'}$, then $x \equiv y \pmod{n'}$.

Lemma 2.3 (congruence modulo an integer respects ring structure)
For every $n \in \mathbb{N}$, congruence modulo n "respects" addition, subtraction, and multiplication, in the sense that if $x, x', y, y' \in \mathbb{Z}$ such that $x \equiv x' \pmod{n}$ and $y \equiv y' \pmod{n}$, then

$$x + y \equiv x' + y' \pmod{n} \qquad x - y \equiv x' - y' \pmod{n} \qquad x \cdot y \equiv x' \cdot y' \pmod{n}$$

Lemma 2.4
For every integer $x \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 1$, there exists a unique integer $x_0 \in \mathbb{Z}$, $0 \leq x_0 < n$, such that $x_0 \equiv x \pmod{n}$.

Definition 2.5 (reduction modulo an integer)
For every integer $x \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 1$, the reduction of $x \pmod{n}$ is the integer x_0 which satisfies 2.4.

Lemma 2.6 (properties of XOR)
The XOR operation is associative, has zero as an identity, is commutative, and has the property that every element is its own inverse. In other words, for all $x, y, z \in \mathbb{Z}$:

$$(x \oplus y) \oplus z = x \oplus (y \oplus z)$$
$$0 \oplus x = x$$
$$x \oplus y = y \oplus x$$
$$x \oplus x = 0$$

Lemma 2.7 (congruence modulo a power of two respects XOR)
For every $n \in \mathbb{N}$, congruence modulo 2^n "respects" XOR, in the sense that if $x, x, y', y' \in \mathbb{Z}$ such that $x \equiv x' \pmod{2^n}$ and $y \equiv y' \pmod{2^n}$, then

$$x \oplus y \equiv x' \oplus y' \pmod{2^n}$$

Definition 2.8 (even and odd (parity))
For an integer $x \in \mathbb{Z}$ to be even means that $x \equiv 0 \pmod{2}$, and for x to be odd means that $x \equiv 1 \pmod{2}$.

Lemma 2.9 (existence and uniqueness of a parity)
Every integer is either even or odd, but not both.

Lemma 2.10 (parity of a product)
A product of only odd integers is odd. A product of integers is even there is at least one even factor.

Lemma 2.11 (corollary to Euler's Theorem)
For all integers $x, y, y' \in \mathbb{Z}$, if x is odd, $y, y' \geq 0$, $y \equiv y' \pmod{2^n}$, then $x^y \equiv x^{y'} \pmod{2^{n+1}}$.

Lemma 2.12 (factoring out twos)
For every $x \in \mathbb{Z}$, there exists a unique $k \in \mathbb{N}$, $m \in \mathbb{Z}$ such that $x = (1 + m \cdot 2) \cdot 2^k$. Furthermore, $k \geq 1$ if and only if x is even.

Lemma 2.13 (lower bound on powers of two)
For every $k \in \mathbb{N}$, $2^k \geq k + 1$.

2.2 Structure of X_n

Theorem 2.14

For all $n \in \mathbb{N},\ n \geq 1,\ (a,b) \in X_n$, b is even.

Proof. Let $n \in \mathbb{N},\ n \geq 1,\ (a,b) \in X_n$, so by 1.6, $0 \leq a, b < 2^n$ and $a^b \equiv a \oplus b \pmod{2^n}$.

By 2.1, $a \equiv a \pmod{2^n}$, so by 2.7, $a \oplus a^b \equiv a \oplus (a \oplus b) \pmod{2^n}$. By 2.6, $a \oplus (a \oplus b) = (a \oplus a) \oplus b = 0 \oplus b = b$, which by substituting into the previous congruence, yields $a \oplus a^b \equiv b \pmod{2^n}$.

Also, $2^n = 0 + 2^{n-1} \cdot 2$, so $2^n \equiv 0 \pmod 2$ by 1.1, so by 2.2, $a \oplus a^b \equiv b \pmod 2$.

By 2.9, either a is even or a is odd.

- Consider the case when a is odd. Then a^b is a product of integers with only odd factors, so a^b is odd by 2.10. Since a and a^b are both odd, $a \equiv 1 \pmod 2$ and $a^b \equiv 1 \pmod 2$ by 2.8. Then, by 2.7, $a \oplus a^b \equiv 1 \oplus 1 \pmod 2$.

  Finally, $a \oplus a^b \equiv b \pmod 2$ and $a \oplus a^b \equiv 1 \oplus 1 \pmod 2$, so $b \equiv 1 \oplus 1 \pmod 2$ by 2.1. Additionally, $1 \oplus 1 = 0$ by 2.6, so by substituting this equation into the previous congruence, $b \equiv 0 \pmod 2$, which means b is even by 2.8.

- Consider the case when a is even. If b is zero, then b is already even. Otherwise if $b > 0$, then a^b is a product of integers with an even factor, so a^b is even by 2.10. Since a and a^b are both even, $a \equiv 0 \pmod 2$ and $a^b \equiv 0 \pmod 2$ by 2.8. Then, by 2.7, $a \oplus a^b \equiv 0 \oplus 0 \pmod 2$.

  Finally, $a \oplus a^b \equiv b \pmod 2$ and $a \oplus a^b \equiv 0 \oplus 0 \pmod 2$, so $b \equiv 0 \oplus 0 \pmod 2$ by 2.1. Additionally, $0 \oplus 0 = 0$ by 2.6, so by substituting this equation into the previous congruence, $b \equiv 0 \pmod 2$, which means b is even by 2.8.

In both cases, b is even. □

Theorem 2.15

For all $n \in \mathbb{N},\ n \geq 1$, for every odd $a \in \mathbb{Z},\ 0 \leq a < 2^n$ there exists a unique b such that $(a,b) \in X_n$.

Proof. The proof proceeds by induction on n.

1. Let $n = 1$. Let $a \in \mathbb{Z},\ 0 \leq a < 2^1$ such that a is odd. The only value that works is $a = 1$. What remains to be shown is that there exists a unique $b \in \mathbb{Z}$ such that $(1,b) \in X_1$.

   Existence of b: By 2.1, $1 \equiv 1 \pmod{2^1}$. Additionally, $1 = 1^0$, and $1 = 0 \oplus 1 = 1 \oplus 0$ by 2.6. By substituting these equations into the congruence, $1^0 \equiv 1 \oplus 0 \pmod{2^1}$. Then, $(a,b) = (1,0)$ satisfies both $0 \leq a, b < 2^1$ and $a^b \equiv a \oplus b \pmod{2^1}$, so by 1.6 $(1,0) \in X_1$.

   Uniqueness of b: Let b, b' such that $(1,b), (1,b') \in X_1$. Then, by 1.6, $0 \leq b, b' < 2^1$. There are only two choices for each of b, b' such that $0 \leq b, b' < 2^1$, namely 0 and 1. By 2.14 both b and b' must be even. However, of the two choices, only $b = b' = 0$ is even, which shows in particular $b = b'$.

2. Suppose that 2.15 holds for $n = n_0 \in \mathbb{N},\ n_0 \geq 1$ (inductive hypothesis). Let $a \in \mathbb{Z},\ 0 \leq a < 2^{n_0+1}$ such that a is odd. What remains to be shown is that there exists a unique $b \in \mathbb{Z}$ such that $(a,b) \in X_{n_0+1}$.

   Existence: Let a_0 be the reduction of $a \pmod{2^{n_0}}$. By the existence part of the inductive hypothesis, there exists a b_0 such that $(a_0, b_0) \in X_{n_0}$, so $0 \leq a_0, b_0 < 2^{n_0}$ and $a_0^{b_0} \equiv a_0 \oplus b_0 \pmod{2^{n_0}}$ by 1.6. The remaining proof is lengthy, so it is divided into self-contained steps (each step only uses the final result of the previous step):

   (a) By 2.1, $a_0 \equiv a_0 \pmod{2^{n_0}}$, so $a_0 \oplus a_0^{b_0} \equiv a_0 \oplus (a_0 \oplus b_0) \pmod{2^{n_0}}$ by 2.7. By 2.6, $a_0 \oplus (a_0 \oplus b_0) = (a_0 \oplus a_0) \oplus b_0 = 0 \oplus b_0 = b_0$. By substituting into the previous congruence, $a_0 \oplus a_0^{b_0} \equiv b_0 \pmod{2^{n_0}}$. Note that $a_0 \equiv a \pmod{2^{n_0}}$ by 2.5. Therefore, $a_0^{b_0} \equiv a^{b_0} \pmod{2^{n_0}}$ by 2.3 (powers are iterated products). So, by 2.7, $a_0 \oplus a_0^{b_0} \equiv a \oplus a^{b_0} \pmod{2^{n_0}}$. The left-hand-side is congruent to $b_0 \pmod{2^{n_0}}$, so $b_0 \equiv a \oplus a^{b_0} \pmod{2^{n_0}}$ by 2.1.

(b) Let b be the reduction of $a \oplus a^{b_0} \pmod{2^{n_0+1}}$, so $0 \le b < 2^{n_0+1}$ and $b \equiv a \oplus a^{b_0} \pmod{2^{n_0+1}}$ by 2.5. Since $b \equiv a \oplus a^{b_0} \pmod{2^{n_0}}$ and $b_0 \equiv a \oplus a^{b_0} \pmod{2^{n_0}}$, by 2.1 $b \equiv b_0 \pmod{2^{n_0}}$. Since a is odd, by 2.11 it follows that $a^b \equiv a^{b_0} \pmod{2^{n_0+1}}$.

(c) By 2.6, $a^{b_0} = 0 \oplus a^{b_0} = (a \oplus a) \oplus a^{b_0} = a \oplus (a \oplus a^{b_0})$, so by substituting this equality into the congruence from the previous step, $a^b \equiv a \oplus (a \oplus a^{b_0}) \pmod{2^{n_0+1}}$. Since b was defined as the reduction of $a \oplus a^{b_0} \pmod{2^{n_0+1}}$, by 2.5 $b \equiv a \oplus a^{b_0} \pmod{2^{n_0+1}}$. By 2.6, $a \equiv a \pmod{2^{n_0}+1}$, so by 2.7, $a \oplus b \equiv a \oplus (a \oplus a^{b_0}) \pmod{2^{n_0+1}}$. Finally, by 2.1, $a \oplus b \equiv a \oplus (a \oplus a^{b_0}) \pmod{2^{n_0+1}}$ and $a^b \equiv a \oplus (a \oplus a^{b_0}) \pmod{2^{n_0+1}}$ together imply that $a^b \equiv a \oplus b \pmod{2^{n_0+1}}$.

Uniqueness of b: Let b, b' such that $(a, b), (a, b') \in X_{n+1}$. Let a_0, b_0, b'_0 be the reductions of a, b, b' $\pmod{2^{n_0}}$, respectively. The remaining proof is lengthy, so it is divided into self-contained parts (the results of both parts will be used afterwards):

(a) Since $a_0 \equiv a \pmod{2^{n_0}}$ by 2.5, $a_0^{b_0} \equiv a^{b_0} \pmod{2^{n_0}}$ and $a_0^{b'_0} \equiv a^{b'_0} \pmod{2^{n_0}}$ by 2.3 (powers are iterated products).

Since $2^{n_0} = 0 + 2 \cdot 2^{n_0-1}$, by 1.1 $2^{n_0} \equiv 0 \pmod{2^{n_0-1}}$. Also by 2.5 $b_0 \equiv b \pmod{2^{n_0}}$ and $b'_0 \equiv b' \pmod{2^{n_0}}$, so then by 2.2, $b_0 \equiv b \pmod{2^{n_0-1}}$ and $b'_0 \equiv b' \pmod{2^{n_0-1}}$. Since it is also true that a is odd, $a^{b_0} \equiv a^b \pmod{2^{n_0}}$ and $a^{b'_0} \equiv a^{b'} \pmod{2^{n_0}}$ by 2.11.

By 2.1 $a_0^{b_0} \equiv a^{b_0} \equiv a^b \pmod{2^{n_0}}$ implies that $a_0^{b_0} \equiv a^b \pmod{2^{n_0}}$ and similarly $a_0^{b'_0} \equiv a^{b'_0} \equiv a^{b'} \pmod{2^{n_0}}$ implies that $a_0^{b'_0} \equiv a^b \pmod{2^{n_0}}$.

(b) Since $(a, b), (a, b') \in X_{n_0+1}$, by 1.6 $a^b \equiv a \oplus b \pmod{2^{n_0+1}}$, and $a^{b'} \equiv a \oplus b' \pmod{2^{n_0+1}}$. Since $2^{n_0+1} = 0 + 2 \cdot 2^{n_0}$, so by 1.1 $2^{n_0+1} \equiv 0 \pmod{2^{n_0}}$, and by 2.2, $a^b \equiv a \oplus b \pmod{2^{n_0}}$, and $a^{b'} \equiv a \oplus b' \pmod{2^{n_0}}$.

(c) By 2.5 $a_0 \equiv a \pmod{2^{n_0}}, b_0 \equiv b \pmod{2^{n_0}}, b'_0 \equiv b' \pmod{2^{n_0}}$. Therefore, by 2.7, $a_0 \oplus b_0 = a \oplus b \pmod{2^{n_0}}$ and $a_0 \oplus b'_0 \equiv a \oplus b' \pmod{2^{n_0}}$.

In summary, the three parts above show that

$$\begin{aligned} a_0^{b_0} &\equiv a^b \pmod{2^{n_0}} \\ a^b &\equiv a \oplus b \pmod{2^{n_0}} \\ a_0 \oplus b_0 &\equiv a \oplus b \pmod{2^{n_0}} \end{aligned} \qquad \begin{aligned} a_0^{b'_0} &\equiv a^{b'} \pmod{2^{n_0}} \\ a^{b'} &\equiv a \oplus b' \pmod{2^{n_0}} \\ a_0 \oplus b'_0 &\equiv a \oplus b' \pmod{2^{n_0}} \end{aligned}$$

Therefore, using 2.1, $a_0^{b_0} \equiv a_0 \oplus b_0 \pmod{2^{n_0}}$ and $a_0^{b'_0} \equiv a_0 \oplus b'_0 \pmod{2^{n_0}}$. Since it also true that $0 \le a_0, b_0, b'_0 < 2^{n_0}$, by 1.6 $(a_0, b_0), (a_0, b'_0) \in X_{n_0}$. By the uniqueness part of the inductive hypothesis, it follows that $b_0 = b'_0$. What remains to be shown is that in fact $b = b'$.

By 2.5, $b \equiv b_0 \pmod{2^{n_0}}$. Substituting $b_0 = b'_0$ yields $b \equiv b'_0 \pmod{2^{n_0}}$. By 2.5, $b'_0 \equiv b' \pmod{2^{n_0}}$, so $b \equiv b' \pmod{2^{n_0}}$.

Finally, by 2.11, since a is odd, $a^b \equiv a^{b'} \pmod{2^{n_0+1}}$. But since $(a, b), (a, b') \in X_{n_0+1}$, by 1.6 $a^b \equiv a \oplus b \pmod{2^{n_0+1}}$ and $a^{b'} \equiv a \oplus b' \pmod{2^{n_0+1}}$. Combining these three congruences by 2.1 yields $a \oplus b \equiv a \oplus b' \pmod{2^{n_0}+1}$. Since $a \equiv a \pmod{2^{n_0}+1}$ by 2.1, by 2.7 $a \oplus (a \oplus b) \equiv a \oplus (a \oplus b') \pmod{2^{n_0+1}}$. By 2.6, $a \oplus (a \oplus b) = (a \oplus a) \oplus b = 0 \oplus b = b$, and $a \oplus (a \oplus b') = (a \oplus a) \oplus b' = 0 \oplus b' = b'$. Substituting these two equations into the previous congruence at last gives $b \equiv b' \pmod{2^{n_0+1}}$.

By 2.4, there is a unique integer $b_s \in \mathbb{Z},\ 0 \le b_s < 2^{n_0+1}$ such that $b_s \equiv b \pmod{2^{n_0+1}}$. However, $0 \le b < 2^{n_0+1}$ and $b \equiv b \pmod{2^{n_0+1}}$ by 2.1, and similarly $0 \le b' < 2^{n_0+1}$ and $b \equiv b' \pmod{2^{n_0+1}}$. The uniqueness of b_s implies that $b = b_s = b'$, so in particular $b = b'$.

By the principle of induction, for every odd $a \in \mathbb{Z},\ 0 \le a < 2^n$ there exists a unique b such that $(a, b) \in X_n$, for all $n \in \mathbb{Z},\ n \ge 1$. $\square$

Theorem 2.16

Let $n \in \mathbb{N}$, $n \geq 1$. For every positive even $b \in \mathbb{Z}$, $0 < b < 2^n$, there exists a unique even $a \in \mathbb{Z}$ such that $(a, b) \in X_n$.

Proof. Let $b \in \mathbb{Z}$ be a positive even integer.

By 2.12, since b is even, $b = (1 + m \cdot 2) \cdot 2^k$ for some $k \in \mathbb{N}, m \in \mathbb{Z}, k \geq 1$. Since also $b = (1 + m \cdot 2) \cdot 2^k \geq 2^k > k + 1$ by 2.13.

Let $\{n_i\}_{n=0}^{\infty}$ be a sequence in $\mathbb{N}$ and let $\{a_i\}_{i=0}^{\infty}$ be a sequence in $\mathbb{Z}$ defined recursively as

$$n_0 = k + 1 \qquad n_{i+1} = n_i + (k - 1),$$

$$a_0 = 2^k \qquad a_{i+1} = a_i^b \oplus b.$$

The proof proceeds by induction on i to show that for all $i \geq 0$, a_i is the unique solution for a to the system $0 \leq a < 2^{n_i}$, $a^b \equiv a \oplus b \pmod{2^{n_i}}$, $a \equiv 0 \pmod 2$.

1. Let $i = 0$.

   Since, $0 \leq a_0 = 2^k < 2^{k+1}$, a_0 solves the first part of the system.

   $a_0 = 2^k + 0 \cdot 2^{k+1}$, so by 1.1 $a_0 \equiv 2^k \pmod{2^{k+1}}$ and similarly $b = (1 + m \cdot 2) \cdot 2^k = 2^k + m \cdot 2^{k+1}$, so $b \equiv 2^k \pmod{2^{k+1}}$ by 1.1.

   By 2.7, $a_0 \oplus b \equiv 2^k \oplus 2^k \pmod{2^{k+1}}$. By 2.6, $2^k \oplus 2^k = 0$, so substituting this equality into the previous congruence produces $a_0 \oplus b \equiv 0 \pmod{2^{k+1}}$. Since $b > k + 1$ and $k \geq 1$, $b \cdot k > k + 1$. $a_0 = 2^k$, so $a_0^b = 2^{bk} = 0 + 2^{bk-k-1} \cdot 2^{k+1}$, and so by 1.1 $a_0^b \equiv 0 \pmod{2^{k+1}}$. Since $a_0^b \equiv 0 \pmod{2^{k+1}}$ and $a_0 \oplus b \equiv 0 \pmod{2^{k+1}}$ it follows from 2.1 that $a_0^b \equiv a_0 \oplus b \pmod{2^{k+1}}$. So, a_0 solves the second part of the system.

   Finally, $k \geq 1$, so $a_0 = 2^k = 0 + 2^{k-1} \cdot 2$, so $a_0 \equiv 0 \pmod 2$ by 1.1. Thus a_0 satisfies the third part of the system.

   Since a_0 satisfies all three parts of the system, it is a solution to the whole system. What is left is to show that a_0 is the unique solution.

   Consider another solution to the system, say a'. By the third part of the system, $a' \equiv 0 \pmod 2$, which means $a' = 0 + a_r \cdot 2 = a_r \cdot 2$ for some $a_r \in \mathbb{Z}$ by 1.1. Then since $b > k + 1$, $a'^b = (a_r \cdot 2)^b = 0 + (a_r^b \cdot 2^{b-k-1}) \cdot 2^{k+1}$, which means $a'^b \equiv 0 \pmod{2^{k+1}}$. Now since a' satisfies the second part of the solution, $a'^b \equiv a' \oplus b \pmod{2^{k+1}}$. By 2.1, the previous two congruences imply that $a' \oplus b \equiv 0 \pmod{2^{k+1}}$. By 2.1, $b \equiv b \pmod{2^{k+1}}$, so $(a' \oplus b) \oplus b \equiv 0 \oplus b \pmod{2^{k+1}}$. By 2.6, $(a' \oplus b) \oplus b = a' \oplus (b \oplus b) = a' \oplus 0 = 0 \oplus a' = a'$ and $0 \oplus b = b$, so substituting into the last congruence yields $a' \equiv b \pmod{2^{k+1}}$. Finally, using the fact that $a_0 \equiv b \pmod{2^{k+1}}$ and that a_0 satisfies the third part of the system, which is that $0 \leq a_0 < 2^{k+1}$, it must be the case that a_0 is the reduction of $b \pmod{2^{k+1}}$ by 2.4. However, $0 \leq 2^k < 2^{k+1}$ and $2^k \equiv b \pmod{2^{k+1}}$ (by 2.1), so 2^k is the reduction of $b \pmod{2^{k+1}}$. Therefore, $a' = 2^k$.

□

2.3 The Algorithm

TODO

3 Proving the Preliminary Stuff

TODO