

Lemma. If $n \geq s \geq 0$ are integers and $v(n)$ is the binary digit sum of n then $v(n - s) \geq v(n) - v(n \& s)$.

Proof. We assume n, s is the smallest counterexample (smallest n and for that n the smallest s) such that $v(n - s) < v(n) - v(n \& s)$.

If $s = 0$ then substituting this we get a contradiction:

$$\begin{aligned} v(n - s) &< v(n) - v(n \& s) \\ v(n) &< v(n) - v(0) \\ v(n) &< v(n) \end{aligned}$$

We may therefor assume that $s \geq 1$.

We will now assume that n, s have a binary digit in their binary expansion in common and denote this 2^b . We may define $n' = n - 2^b, s' = s - 2^b$. From this we get the following contradiction:

$$\begin{aligned} v(n - s) &< v(n) - v(n \& s) \\ v(n' + 2^b - s' - 2^b) &< v(n' + 2^b) - v(n' \& s' + 2^b) \\ v(n' - s') &< v(n') + 1 - v(n' \& s') - 1 \\ v(n' - s') &< v(n') - v(n' \& s') \end{aligned}$$

We may therefor assume that $v(n \& s) = 0$ and so we must have $n > s$. Let us now assume that both n, s are even. We may define $n = 2n'$ and $s = 2s'$. From this we get the following contradiction:

$$\begin{aligned} v(n - s) &< v(n) \\ v(2n' - 2s') &< v(2n') \\ v(n' - s') &< v(n') \end{aligned}$$

If n is odd but s is even we may define $n = 2n' + 1$ and $s = 2s'$. Since $n > s$ we have $2n' + 1 > 2s'$ leading to $n' \geq s'$. From this we get the following contradiction:

$$\begin{aligned} v(n - s) &< v(n) \\ v(2n' + 1 - 2s') &< v(2n' + 1) \\ v(n' - s') + 1 &< v(n') + 1 \\ v(n' - s') &< v(n') \end{aligned}$$

If n is even and s is odd we may define $n = n' + 1$ and $s = s' + 1$. Since $n > s$ we have $n' > s'$. If the lowest set bit in the binary representation of n is $2^l, l \geq 1$, then we have $v(n') = v(n) + l - 1$. This is from the transition of 1 followed by

l 0's in n to a zero followed by l 1's in n' . n' and s' may have bits in common in bit positions $1 \dots l-1$. So we must have $0 \leq v(n' \& s') \leq l-1$ and hence $-l+1 \leq -v(n' \& s') \leq 0$. From this we get the following contradiction:

$$\begin{aligned} v(n-s) &< v(n) \\ v(n'+1-s'-1) &< v(n')-l+1 \\ v(n'-s') &< v(n')-v(n' \& s') \end{aligned}$$