Problem for 2014 December

Communicated by Dan Jurca

Recall the following two functions α and ν_2, where $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$, the set of nonnegative integers, and $\mathbf{N}^+ = \mathbf{N} - \{0\}$.

i. $\alpha : \mathbf{N} \to \mathbf{N}$ by $\alpha(n) =$ the number of 1's in the binary representation of n.
   For example, $\alpha(\text{thirteen}) = \alpha(13_{10}) = \alpha(1101_2) = 3$.

ii. For each prime number p there exists the function $\nu_p : \mathbf{N}^+ \to \mathbf{N}$ as follows.

$$\begin{aligned} n \in \mathbf{N}^+ \;\Rightarrow\; n &= \prod_{p \text{ prime}} p^{\nu_p(n)} \\ &= 2^{\nu_2(n)} \times 3^{\nu_3(n)} \times 5^{\nu_5(n)} \times 7^{\nu_7(n)} \times 11^{\nu_{11}(n)} \times \cdots \end{aligned}$$

Here we need only ν_2; and $n \in \mathbf{N}^+ \;\Rightarrow\; \nu_2(n) = a$ if there exists $b \in \mathbf{N}$ such that $n = 2^a(2b+1)$; *i.e.*, $\nu_2(n)$ equals the number of 2's in the expression of n as a product of prime numbers.
For example, since $600 = 8 \times 75 = 2^3(2 \cdot 37 + 1)$, we have $\nu_2(600) = 3$.

The following is part (c) of a problem which appears, with different notation, on page 11 of *Fundamentals of the Average Case Analysis of Particular Algorithms* by Rainer Kemp.

Show that $\nu_2(n!) = n - \alpha(n)$.

Solution by Dan Jurca

Lemma 1. $1 \le n \;\Rightarrow\; \alpha(n) = \alpha(n-1) + 1 - \nu_2(n)$.

Proof.

We observe the following.

i. $0 \le a \;\Rightarrow\; \alpha(2^a) = 1$, since the binary representation of 2^a is a 1 followed by a 0's.
ii. $0 \le a \;\Rightarrow\; \alpha(2^a - 1) = a$, since the binary representation of $2^a - 1$ is a 1's.
iii. $0 \le a$ and $0 \le c \;\Rightarrow\; \alpha(2^a \cdot c) = \alpha(c)$, since the binary representation of $2^a \cdot c$ is the binary representaion of c followed by a 0's.
iv. $0 \le b \;\Rightarrow\; \alpha(2b+1) = \alpha(2b) + 1$, since the binary representation of $2b$ ends with a 0.
v. $0 \le c \le 2^a \;\Rightarrow\; \alpha(2^a b + c) = \alpha(2^a b) + \alpha(c)$, since there exists no 1 in both the binary representation of $2^a b$ and the binary representation of c.

Therefore if $n = 2^a(2b+1)$, then $n = 2^a \cdot 2b + 2^a$ so $n - 1 = 2^a \cdot 2b + (2^a - 1)$ and $\alpha(n-1) = \alpha(2^a \cdot 2b + (2^a - 1)) = \alpha(2^a \cdot 2b) + \alpha(2^a - 1) = \alpha(2b) + a$. Hence, $\alpha(n) = \alpha(2^a(2b+1)) = \alpha(2b+1) = \alpha(2b) + 1 = (\alpha(n-1) - a) + 1 = \alpha(n-1) + 1 - a = \alpha(n-1) + 1 - \nu_2(n)$, proving lemma 1.

Lemma 2. $1 \le n_1$ and $1 \le n_2 \;\Rightarrow\; \nu_2(n_1 \cdot n_2) = \nu_2(n_1) + \nu_2(n_2)$.

Proof.

If $n_1 = 2^{a_1}(2b_1 + 1)$ and $n_2 = 2^{a_2}(2b_2 + 1)$, then

$$\begin{aligned} n_1 \cdot n_2 &= 2^{a_1 + a_2}\,((2b_1 + 1)(2b_2 + 1)) \\ &= 2^{a_1 + a_2}\,(2(2b_1 b_2 + b_1 + b_2) + 1) \quad \text{so that} \\ \nu_2(n_1 \cdot n_2) &= a_1 + a_2 \\ &= \nu_2(n_1) + \nu_2(n_2), \quad \text{proving lemma 2.} \end{aligned}$$

Proposition. $0 \le n \;\Rightarrow\; \nu_2(n!) = n - \alpha(n)$.

Proof.

$\nu_2(0!) = \nu_2(1) = \nu_2(2^0(2 \cdot 0 + 1)) = 0 = 0 - 0 = 0 - \alpha(0)$; *i.e.*, $\nu_2(0!) = 0 - \alpha(0)$. Now suppose $1 \le n$ and $\nu_2((n-1)!) = (n-1) - \alpha(n-1)$. Then

$$\begin{aligned} \nu_2(n!) &= \nu_2(n \cdot (n-1)!) \\ &= \nu_2(n) + \nu_2((n-1)!) && \text{by lemma 2} \\ &= \nu_2(n) + (n-1) - \alpha(n-1) && \text{by the inductive hypothesis} \\ &= \nu_2(n) + (n-1) - (\alpha(n) - 1 + \nu_2(n)) && \text{by lemma 1} \\ &= n - \alpha(n), \end{aligned}$$

and the proposition follows by induction on n.

Remark. Legendre has generalized this to primes other than 2.

Also solved by Ruben Soto (CSUEB class of 2006)