Problem 12255
(American Mathematical Monthly, Vol.128, May 2021)

Proposed by B. Shala (Slovenia).

Given a positive integer a_0, define $a_1, \ldots, a_n$ recursively by $a_i = 1^2 + 2^2 + \cdots + a_{i-1}^2$ for $i \geq 1$. Is it true that, given any subset A of $\{1, \ldots, n\}$, there is a positive integer a_0 such that, for $1 \leq i \leq n$, 6 divides a_i if and only if $i \in A$?

Solution proposed by Roberto Tauraso, Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy.

Solution. The answer is affirmative. We will show a recursive procedure that given a binary string $\mathbf{b}$ of length n, allows to find two positive integers $a_0(0, \mathbf{b})$, which is not a multiple of 6, and $a_0(1, \mathbf{b})$, which is a multiple of 6, such that, for $1 \leq i \leq n$, 6 divides a_i if and only if $(\mathbf{b})_i = 1$.

First we introduce some notations. Let

$$f(N) = 1^2 + 2^2 + \cdots + N^2 = \frac{N(N+1)(2N+1)}{6}$$

then, $a_i = f(a_{i-1})$. Notice that, for any $M \in \mathbb{N}$, the polynomial equations

$$f(6N+1) = (6N+1)(3N+1)(4N+1) = M \qquad (0) \quad , \quad f(6N) = N(6N+1)(12N+1) = M \qquad (1)$$

have simple roots modulo 6, $M - 1$ and M respectively, and therefore, by Hensel's Lifting Lemma, these roots correspond, via Chinese Remainder Theorem, to roots of the same equations modulo any power of 6. Let $N_0(M, m)$ be such root of (0) modulo 6^m and let $N_1(M, m)$ be the root of (1) modulo 6^m.

For $n = 1$, we let

$$a_0(0, 0) = 1 \quad , \quad a_0(1, 0) = 6 \quad , \quad a_0(0, 1) = 4 \quad , \quad a_0(1, 1) = 36.$$

For $n > 1$, let

$$a_0(0, 0\mathbf{b}) = 6N_0(a_0(0, \mathbf{b}), m) + 1 \quad , \quad a_0(1, 0\mathbf{b}) = 6N_1(a_0(0, \mathbf{b}), m)$$

and

$$a_0(0, 1\mathbf{b}) = 6N_0(a_0(1, \mathbf{b}), m) + 1 \quad , \quad a_0(1, 1\mathbf{b}) = 6N_1(a_0(1, \mathbf{b}), m)$$

where m is chosen large enough such that, for $2 \leq i \leq n$, the *new* a_i keeps the same divisibility by 6 of the *old* a_{i-1}. $\square$