A proof that $\frac{m^3-m}{3}$ is an integer for any odd $m \in \mathbb{N}$

Lukas Prokop

30th of December 2015

Background

In Donald Knuth's 21st Annual Christmas Lecture: Universal Commafree Codes, he claims:

> This is the problem that Eastman saw. If you have any odd block length, whatsoever $3, 5, 7, \ldots$. Block length 1 isn't too interesting. But $3, 5, 7, 9, 11$ and you have an m-letter alphabet. The number of possible three-letter words is m cubed, but then you have to throw out the cases that all are equal and you divide it by three in order to figure out the cycles. This *is always an integer* and this is the best you can get.
>
> $$\frac{m^3 - m}{3}$$

Claim

$$\frac{m^3 - m}{3} \in \mathbb{N} \qquad \forall \text{ odd } m \in \mathbb{N}$$

Proof

Proof. It holds that any odd integer $m \in \mathbb{N}$ can be represented as $2k + 1$ with $k \in \mathbb{N}$.

$$\begin{aligned}
\frac{m^3 - m}{3} &= \frac{(2k+1)^3 - (2k+1)}{3} \\
&= \frac{(2k+1)^3 - 2k - 1}{3} \\
&= \frac{8k^3 + 3 \cdot 4k^2 + 3 \cdot 2k + 1 - 2k - 1}{3} \\
&= \frac{8k^3 + 12k^2 + 4k}{3}
\end{aligned}$$

We now switch to divisibility notation. $n \mid k$ is a true statement if and only if k has n as its divisor. We need to prove $3 \mid 8k^3 + 12k^2 + 4k$:

$$\begin{aligned} &3 \mid 8k^3 + 4k \\ &3 \mid (3 \cdot 2 + 2)k^3 + (3 + 1)k \\ &3 \mid 3 \cdot (2k^3 + k) + 2k^3 + k \end{aligned}$$

It holds that

$$\begin{aligned} x \mid x \cdot y + z \qquad &\Leftrightarrow \qquad x \mid z \\ \Rightarrow 3 \mid 2k^3 + k \end{aligned}$$

It holds that any integer $k \in \mathbb{N}$ can be represented as one of $3n + 0$, $3n + 1$ or $3n + 2$ with $n \in \mathbb{N}$. We make a case distinction:

$k = 3n + 0$

$$\begin{aligned} &3 \mid 2(3n)^3 + (3n) \\ &3 \mid 2 \cdot 27n^3 + 3n \\ &3 \mid 2 \cdot 3 \cdot 9n^3 + 3n \\ &3 \mid 3 \cdot (18n^3 + n) \end{aligned}$$

The right-hand side has a divisor 3 and therefore the statement of the last line holds.

$k = 3n + 1$

$$\begin{aligned} &3 \mid 2(3n + 1)^3 + (3n + 1) \\ &3 \mid 2 \cdot (27n^3 + 3 \cdot 9n^2 + 3 \cdot 3n + 1) + 3n + 1 \\ &3 \mid 2 \cdot (27n^3 + 3 \cdot 9n^2 + 3 \cdot 3n) + 2 + 3n + 1 \\ &3 \mid 2 \cdot (27n^3 + 3 \cdot 9n^2 + 3 \cdot 3n) + 3n + 3 \\ &3 \mid 3 \cdot (18n^3 + 18n^2 + 6n) + 3 \cdot (3n + 1) \\ &3 \mid 3 \cdot (18n^3 + 18n^2 + 6n + 3n + 1) \end{aligned}$$

The right-hand side has a divisor 3 and therefore the statement of the last line holds.

$k = 3n + 2$

$$\begin{aligned} &3 \mid 2(3n + 2)^3 + (3n + 2) \\ &3 \mid 2 \cdot (27n^3 + 18n^2 + 12n + 8) + 3n + 2 \\ &3 \mid 54n^3 + 36n^2 + 24n + 16 + 3n + 2 \\ &3 \mid 54n^3 + 36n^2 + 24n + 3n + 18 \\ &3 \mid 3 \cdot (18n^3 + 12n^2 + 8n + n + 6) \end{aligned}$$

The right-hand side has a divisor 3 and therefore the statement of the last line holds.

We covered all cases and all cases have been proven to be true statements. So the proof is finished. □