Far East Journal of Mathematical Education
© 2015 Pushpa Publishing House, Allahabad, India
Published Online: May 2015
http://dx.doi.org/10.17654/FJMEFeb2015_015_024
Volume 14, Number 1, 2015, Pages 15-24 **ISSN: 0973-5631**

ABOUT A DIVISIBILITY PROPERTY OF INTEGERS

Péter Körtesi

Institute of Mathematics
University of Miskolc
Miskolc-Egyetemváros
H 3515 Miskolc, Hungary

Abstract

Investigating the expression $(n+1)^p - n^p$ for natural n and prime p we will show some interesting properties of divisibility of integers and a way to follow up a simple idea, to obtain nice generalisations while teaching elementary algebra. We will make use of some theorems suitable for secondary school mathematics teaching.

The Story of the Problem

While teaching mathematical induction in a secondary vocational school, one of the students, Attila Nemes has "discovered" the following interesting property: if a number of the form $(n+1)^3 - n^3$ is divided by 3, the remainder always will be a multiple of 3 plus 1, in other words congruent to 1 mod 3. I have shown him the proof, he got disappointed, but continued his "investigations" using a pocket calculator. We worked similarly about three-four weeks, discovering, and finding the proof of some properties, which are equivalent to the so-called Fermat little theorem. In the following, I will sum up our findings, which finally appeared in a joint paper [1].

Received: December 15, 2014; Accepted: January 8, 2015

Keywords and phrases: primes and twin primes, binomial coefficients, Bézout theorem, Fermat's little theorem.

Communicated by K. K. Azad

Divisibility Properties of Positive Integers

Proposition P.1. *For any* $p \geq 3$ *prime, and* $n \in \mathbb{N}$, *we have*:

$$(n+1)^p - n^p = p \cdot M_p + 1, \text{ where } M_p \in \mathbb{Z} \text{ and } n(n+1) \mid M_p.$$

Remark R.1. If $p \geq 5$, then in the above proposition, we will have: $(n^2 + n + 1) \mid M_p$ as well.

Proof. Let $p \geq 3$ be a prime and *n* be an arbitrary natural number. We have

$$(n+1)^p - n^p = C_p^0 n^p + C_p^1 n^{p-1} + C_p^2 n^{p-2} + \cdots + C_p^{p-1} n + C_p^p - n^p.$$

In other words,

$$(n+1)^p - n^p = C_p^1 n^{p-1} + C_p^2 n^{p-2} + \cdots + C_p^{p-1} n + 1. \qquad (1)$$

It is easy to see that

$$C_p^k = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k(k-1)(k-2)\cdots 3.2.1}\, p \cdot L_k, \quad 1 \leq k < p,$$

where L_k is an integer as the binomial coefficients C_p^k are integers and the factor *p* is a prime, $1 \leq k < p$, so it has no divisors, while the possible simplifications are done. Summing up:

$$C_p^k = p \cdot L_k, \quad 1 \leq k < p \quad \text{and} \quad L_k \in \mathbb{Z}.$$

Let us introduce the notation $L_k n^{p-k} = L'_k \in \mathbb{Z}$ in relation (1):

$$\begin{aligned}(n+1)^p - n^p &= pL'_1 + pL'_2 + \cdots + pL'_{p-1} + 1\\ &= p(L'_1 + L'_2 + \cdots + L'_{p-1}) + 1,\end{aligned}$$

hence

$$(n+1)^p - n^p = p \cdot M_p + 1, \text{ where } M_p = L'_1 + L'_2 + \cdots + L'_{p-1} \in \mathbb{Z}. \quad (2)$$

Now we need to show $n(n+1) | M_p$, and if $p \geq 5$, then $(n^2 + n + 1) | M_p$.

(a) First, based on the relation (1), we can see

$$n | M_p. \tag{3}$$

(b) We can express $p \cdot M_p$ from the relation (2): $p \cdot M_p = (n+1)^p - n^p - 1$, in other words, $p \cdot M_p$ is a polynomial in n. Let us denote it

$$f(n) = p \cdot M_p = (n+1)^p - n^p - 1.$$

Using the Bézout theorem for $f(n)$, we will show that $(n+1) | f(n)$. Indeed, $f(-1) = 0p - (-1) - 1 = 0$ (as $p \geq 3$ is prime, so $p = 2k+1$), hence $(n+1) | f(n)$, in other words, $(n+1) | p \cdot M_p$, and as p is a prime, we finally have:

$$(n+1) | M_p. \tag{4}$$

(c) If $p \geq 5$, then we need to show $(n^2 + n + 1) | M_p$.

Let us consider again the polynomial $f(n)$ introduced in before, and use again the Bézout theorem to show that $(n - n_1) | f(n)$ and $(n - n_2) | f(n)$, where n_1 and n_2 are the complex roots of the quadratic polynomial $n^2 + n + 1$, i.e.,

$$n_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3},$$

$$n_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}.$$

Remark R.2. Considering divisibility by 6 the prime $p \geq 5$ can belong only to the residue classes $6k+1$ or $6k+5$, as all other $6k$, $6k+2$, $6k+3$, $6k+4$ are divided by 2 or 3. Consequently, let us consider the following two cases:

(c_1) If the prime $p \geq 5$ has the form $6k+1,\ k \in \mathbb{Z},$ then

$$f(n_1) = (n_1+1)^{6k+1} - n_1^{6k+1} - 1$$

and we know that

$$n_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3},$$

and we compute $n_1 + 1 = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$. Hence,

$$f(n_1) = \cos\frac{(6k+1)\pi}{3} + i\sin\frac{(6k+1)\pi}{3} - \cos\frac{(6k+1)2\pi}{3}$$

$$- i\sin\frac{(6k+1)2\pi}{3} - 1$$

$$= \cos\left(2k\pi + \frac{\pi}{3}\right)^3 + i\sin\left(2k\pi + \frac{\pi}{3}\right)$$

$$- \cos\left(4k\pi + \frac{2\pi}{3}\right) - i\sin\left(4k\pi + \frac{2\pi}{3}\right) - 1,$$

$$f(n_1) = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} - \cos\frac{2\pi}{3} - i\sin\frac{2\pi}{3} - 1$$

$$= \frac{1}{2} + i\frac{\sqrt{3}}{2} + \frac{1}{2} - i\frac{\sqrt{3}}{2} - 1 = 0,$$

$$f(n_1) = 0,\ \text{consequently,}\ (n - n_1) \mid f(n). \tag{5}$$

Similarly, for n_2, we have

$$n_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} \quad \text{and} \quad n_2 + 1 = \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}.$$

$$f(n_2) = \cos\frac{(6k+1)5\pi}{3} + i\sin\frac{(6k+1)5\pi}{3} - \cos\frac{(6k+1)4\pi}{3}$$

$$- i\sin\frac{(6k+1)4\pi}{3} - 1$$

$$= \cos\left(10k\pi + \frac{5_{\pi}^{3}}{3}\right) + i\sin\left(10k\pi + \frac{5\pi}{3}\right)$$

$$- \cos\left(8k\pi + \frac{4\pi}{3}\right) - i\sin\left(8k\pi + \frac{4\pi}{3}\right) - 1,$$

$$f(n_2) = \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3} - \cos\frac{4\pi}{3} - i\sin\frac{4\pi}{3} - 1$$

$$= \frac{1}{2} - i\frac{\sqrt{3}}{2} + \frac{1}{2} + i\frac{\sqrt{3}}{2} - 1 = 0,$$

$$f(n_2) = 0, \text{ thus } (n - n_2) \mid f(n). \tag{6}$$

(c_2) If the prime p has the form $6k + 5$, with $k \in \mathbb{Z}$, and we know that:

$$n_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} \text{ and } n_1 + 1 = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3},$$

respectively,

$$n_2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} \text{ and } n_2 + 1 = \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}.$$

Thus,

$$f(n_2) = \cos\frac{(6k+5)5\pi}{3} + i\sin\frac{(6k+5)5\pi}{3} - \cos\frac{(6k+5)4\pi}{3}$$

$$- i\sin\frac{(6k+5)4\pi}{3} - 1$$

$$= \cos\left(10k\pi + \frac{25\pi}{3}\right) + i\sin\left(10k\pi + \frac{25\pi}{3}\right) - \cos\left(8k\pi + \frac{20\pi}{3}\right)$$

$$- i\sin\left(8k\pi + \frac{20\pi}{3}\right) - 1,$$

$$f(n_2) = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} - \cos\frac{2\pi}{3} - i\sin\frac{2\pi}{3} - 1 = 0,$$

$$f(n_2) = 0, \text{ and thus } (n - n_2) \mid f(n). \tag{6$'$}$$

Similarly, for n_1,

$$f(n_1) = \cos\frac{(6k+5)\pi}{3} + i\sin\frac{(6k+5)\pi}{3} - \cos\frac{(6k+5)2\pi}{3}$$

$$- i\sin\frac{(6k+5)2\pi}{3} - 1$$

$$= \cos\left(2k\pi + \frac{5\pi}{3}\right) + i\sin\left(2k\pi + \frac{5\pi}{3}\right) - \cos\left(4k\pi + \frac{10\pi}{3}\right)$$

$$- i\sin\left(4k\pi + \frac{10\pi}{3}\right) - 1,$$

$$f(n_1) = \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3} - \cos\frac{4\pi}{3} - i\sin\frac{4\pi}{3} - 1 = 0,$$

$$f(n_1) = 0, \text{ thus } (n - n_1) \mid f(n), \text{ too.} \tag{5′}$$

Based on (5), (6), respectively, on (5′), (6′), it is clear that

$$(n^2 + n + 1) \mid f(n). \tag{7}$$

The given property can be generalized if taking $n + k$ instead of $n + 1$.

Proposition P.2. *If* $p \geq 3$ *is a prime, n and k are natural numbers, then*

$$(n+k)^p - n^p = p \cdot n \cdot k(n+k) \cdot M + k^p, \text{ where } M \in \mathbb{Z}.$$

Proof. Let $p \geq 3$ be a prime, *n* and *k* be two natural numbers.

One can write:

$$(n+k)^p - n^p = C_p^0 n^p + C_p^1 n^{p-1}k + C_p^2 n^{p-2}k^2 + \cdots + C_p^{p-1} nk^{p-1}$$

$$+ C_p^p k^p - n^p,$$

$$(n+k)^p - n^p = C_p^1 n^{p-1}k + C_p^2 n^{p-2}k^2 + \cdots + C_p^{p-1} nk^{p-1} + k^p. \tag{8}$$

From the previous proof, we know that $C_p^k = p \cdot L_k$ and take $L_k' = L_k n^{p-k}$.

$$(n+k)^p - n^p = pL_1'k + pL_2'k^2 + \cdots + pL_{p-1}'k^{p-1} + k^p,$$

thus $(n+k)^p - n^p = p \cdot \overline{M}_p + k^p$, where $\overline{M}_p = L_1'k + L_2'k^2 + \cdots + L_{p-1}'k^{p-1} \in \mathbb{Z}$.

We need to prove that

(a) $n \mid \overline{M}_p$ (b) $(n+k) \mid \overline{M}_p$ (c) $k \mid \overline{M}_p$.

According to the relation (8),

$$(n+k)^p - n^p = C_p^1 n^{p-1}k + C_p^2 n^{p-2}k^2 + \cdots + C_p^{p-1} nk^{p-1} + k^p$$

$$= p \cdot \overline{M}_p + k^p$$

or

$$C_p^1 n^{p-1}k + C_p^2 n^{p-2}k^2 + \cdots + C_p^{p-1} nk^{p-1} = p \cdot \overline{M}_p$$

and because *p* is a prime, it follows that

$$n \mid \overline{M}_p \text{ and } k \mid \overline{M}_p. \tag{9}$$

(b) Let us denote now $p \cdot \overline{M}_p = \bar{f}(n) = (n+k)^p - n^p - k^p$.

According to the Bézout theorem,

$$f(-k) = 0 - (-k)^p - k^p = 0, \text{ we have } (n+k) \mid \bar{f}(n),$$

$$\text{thus } (n+k) \mid \overline{M}_p. \tag{10}$$

Another possible generalization of Proposition P.1 is the following:

Proposition P.3. *If* $p \geq 3$ *is a prime, respectively, n and k are positive integers, then*

$$(n+k)^p - n^p = p \cdot \overline{\overline{M}}_p + k, \text{ where } \overline{\overline{M}}_p \in \mathbb{Z}.$$

Proof. Let us apply Proposition P.1 for the integers $n, n+1, \ldots, n+k$

$-1,\ n+k,$ consequently, we will have respectively,

$$(n+1)^p - n^p = p\cdot M_{p,1} + 1,$$

$$(n+2)^p - (n+1)^p = p\cdot M_{p,2} + 1,\ \ldots,$$

$$(n+k-1)^p - (n+k-2)^p = p\cdot M_{p,k-1} + 1,$$

$$(n+k)^p - (n+k-1)^p = p\cdot M_{p,k} + 1.$$

Summing up all, we have

$$(n+k)^p - n^p = p(M_{p,1} + M_{p,2} + M_{p,3} + \cdots + M_{p,k-1} + M_{p,k}) + k \tag{11}$$

and thus

$$(n+k)^p - n^p = p * \overline{\overline{M}}_p + k.$$

Applications

(1) As a simple consequence of Proposition P.3, it follows the Fermat's little theorem.

If we put $n = 0$ and $k = a$, then according to P.3, $a^p - 0 = p\cdot\overline{\overline{M}}_p + a$, hence $a^p - a = p\cdot\overline{\overline{M}}_p$ (Fermat's little theorem).

(2) Based on Propositions P.2 and P.3, we can prove the same theorem in another way as well:

From P.2, we have $(n+a)^p - n^p = p\cdot\overline{M}_p + a^p$ $(k = a)$.

From P.3, we have $(n+a)^p - n^p = p\cdot\overline{\overline{M}}_p + a$ $(k = a)$.

Their difference is $0 = p\cdot M' + a^p - a,$ and thus $a^p - a = p * M',$ where $M' = \overline{M}_p - \overline{\overline{M}}_p \in \mathbb{Z}.$

The Follow Up of the Story, or Does Computer Algebra Help?

Propositions P.1-P.3 were presented in the Self Made Mathematics Group organized for talented secondary school students, and we have used computer algebra tools to check the validity of the properties. While factoring the polynomial $f(n) = (n+1)^p - n^p - 1$ for different values of the prime p, we did observe that it works indeed for all primes we checked, moreover for some of the primes, the polynomial is divided not only by the quadratic factor $n^2 + n + 1$, but even its square, $(n^2 + n + 1)^2$ appears as a factor. We became excited, and we continued the factoring, just as in the case with the pocket calculator, but now we used the power of computer algebra. We did the checking up the computer slowed down, and even more, and soon we did formulate a new "conjecture". From the series of checking, it seemed that the new property is valid only for the upper pair of twin primes over 5, like for 7, 13 or 19.

Proposition P.4. *For any* $p \geq 7$, *prime, such as* $p - 2$ *is prime as well, and* $n \in \mathbb{N}$, *we have*

$$(n+1)^p - n^p = p \cdot M_p + 1, \textit{ where } M_p \in \mathbb{Z} \textit{ and } n(n+1)(n^2+n+1)^2 \mid M_p.$$

Proof. If $p \geq 7$ is such a prime, it can be only of the form $6k+1$, as $p-2$ can be only of the form $6k-1$, equivalent to $6k+5$. Take now the derivative of the polynomial $f(n) = (n+1)^p - n^p - 1$ will be $f'(n) =$ $p(n+1)^{p-1} - pn^{p-1}$. We have to show that both $f'(n_1)$ and $f'(n_2)$ are 0, for $n_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ and $n_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos\frac{4\pi}{3} +$ $i\sin\frac{4\pi}{3}$.

Indeed, as before, we compute $n_1 + 1 = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$ and $n_2 + 1 = \frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}$.

For $p = 6k + 1,$ we have $p - 1 = 6k,$ and thus

$$f'(n_1) = p(n_1 + 1)^{p-1} - pn_1^{p-1}$$

$$= p\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)^{6k} - p\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)^{6k}$$

$$= p(\cos 2k\pi + i\sin 2k\pi) - p(\cos 4k\pi + i\sin 4k\pi) = p - p = 0.$$

Similarly,

$$f'(n_2) = p(n_2 + 1)^{p-1} - pn_2^{p-1}$$

$$= p\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right)^{6k} - p\left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right)^{6k}$$

$$= p(\cos 10k\pi + i\sin 10k\pi) - p(\cos 8k\pi + i\sin 8k\pi) = p - p = 0.$$

As we have proven that both the polynomial and its derivative are divided by $n - n_1$ and $n - n_2,$ this means that both $(n - n_1)^2$ and $(n - n_2)^2,$ and thus $(n^2 + n + 1)^2$ is a factor of $f(n) = (n + 1)^p - n^p - 1.$

Reference

[1] P. Körtesi and A. Nemes, Az egész számok egy tulajdonsága, Matematikai Lapok, Kolozsvár (Romania) XCI(8) (1986), 283-287.