On Multiplying by 12

A half decade theorem finally proven

by
Willy Vasquez
November 15th, 2013

Abstract

As a middle schooler, number theory absolutely fascinated me. As an MIT student, it still does, which is why I set out to prove why an algorithm I discovered in middle school works for multiplying numbers by 12. With the encouragement of Sandra Bayona and proof of a lemma by Andrés Salgado-Bierman, we can successfully call this a case closed. Along the way we learned some fascinating details.

1. Introduction

Back in middle school I had tons of free time to kill, so I would spend it either playing with numbers or hacking video games. I guess you could say I was destined for MIT. Regardless, one evening while playing with my collection of numbers, I discovered an interesting method to multiply any number by 12 that I was not sure why it worked. I kept this method to myself until arriving to high school, where I shared with my physics teacher, Dr. Howe, my method for multiplying by 12. I asked him why it worked to which he replied "You tell me."Due to my basic maths background I was not able to accomplish this at the time. But now, thanks to a rekindling of the problem courtesy of Sandra Bayona, I have successfully managed to prove it with the help of Andrés Salgado-Bierman, instead of studying for my exam.

2. The Method

Take a number n you want to multiply by 12. Divide n by 5 and throw away the remainder. Call this number x. Add n and x then take 2 times your units digit of n, discard any tens digit, then append it to the end of $n + x$.

Examples

$$63$$
$$63/5 = 12r3$$
$$63 + 12 = 75$$
$$3 * 2 = 6$$
$$ans : 756$$

$$117$$
$$117/5 = 23r2$$
$$117 + 23 = 140$$
$$7 * 2 \mod 10 = 4$$
$$ans : 1404$$

As you can see, it holds for these examples. Now we want to prove that this method of multiplying by 12 works for all $n \in \mathbb{Z}$.

3. Proof of Method

Proof. To begin the proof of this method, we must create a proper encoding of decimal numbers.

Any decimal number can be written as a sum of basic units multiplied to a power of 10. Take $n \in \mathbb{Z}$,

$$n = a_0 + a_1 10 + a_2 10^2 + \dots$$

where $a_i \in \{0 - 9\}$. This can also be written as

$$n = \sum_{i=0}^{d} a_i 10^i$$

With this encoding we can utilize each units digit as we please. We will primarily be focusing on a_0 and n for the rest of this proof.

With this encoding of decimals, we can write our method using math notation:

$$10(n + \left\lfloor \frac{n}{5} \right\rfloor) + (2a_0 \mod 10) \tag{1}$$

Let's break this down in order to show how this equation matches the method.

1. $\alpha = \lfloor \frac{n}{5} \rfloor$ is the number of times 5 goes into n.

2. $\beta = (n + \alpha)$ is our number plus the number of times 5 goes into it.

3. $\gamma = 2a_0 \mod 10$ is twice the units digit of n with the tens digit removed if $2a_0 > 9$.

4. $\delta = 10(\beta) + \gamma$ is our new units digit appended to the added value. This would be our final answer.

Now that we've shown it is similar, we want to show that this equals $12n$.

Let us rewrite $\lfloor \frac{n}{5} \rfloor$ so we don't have to work with the awkward floor function. This function returns how many times 5 goes into n disregarding the remainder. We can write n as

$$n = 5x + y$$

Where x is the number we are looking for and $y = a_0 \mod 5$. Solving for x gives us

$$x = \frac{n - (a_0 \mod 5)}{5}$$

Putting it back into (1) gives us

$$10(n + \frac{n - (a_0 \mod 5)}{5}) + (2a_0 \mod 10) \tag{2}$$

And further simplifying the above equation leads to:

$$12n - 2(a_0 \mod 5) + (2a_0 \mod 10) \tag{3}$$

We're almost there! Now we just need the last two members to cancel out. This is where we use Andrés' Lemma:

Andrés' Lemma. *For $a, b, c \in \mathbb{Z}_{>0}$, $(ba \mod bc) = b(a \mod c)$.*

Proof. We start by simplifying $(ba \mod bc)$.

We choose $a = xc + y$, where y < c. Substituting this in gives

$$(xbc + by \mod bc)$$

by multiplying b times $xc+y$. Using the distributive property of modulus[1], we transform this into

$$((xbc \mod bc) + (by \mod bc)) \mod bc$$

Since the first element is a multiple of bc, it reduces to 0, and the second turns to just $by \mod bc$ due to the identity rule of modulus[1]. Since $y < c$, we know that $by < bc$ so the remainder under division would just be by.

We take the same approach with $b(a \mod c)$.

We substitute $a = xc + y$, with $y < c$ once again, and get

$$b((xc + y) \mod c)$$

xc again is a multiple of c so that disappears, and since $y < c$ the remainder we would have would just be y, leading us to the simplification of by as well.

Since they both end up reducing to by, these two operations are equal. ■

Applying this transformation to (3) results in

$$12n - 2a_0 + 2a_0 \tag{4}$$

which cancels out to

$$12n \tag{5}$$

Hence completing our proof. ■

4. Conclusion

And there we go! After nearly 7 years of not knowing why this works, it has finally been proven. Thanks to Andrés' Lemma we also discovered an interesting trick about composite modulus and factors. Although it seemed like a trivial fact, the Internet let me down as I was searching for modulus with composite N, so we went ahead and proved it ourselves.

As for other methods of multiplying numbers with this similar style, they probably exist but I have not experimented with my numbers. A huge thank you again to Andrés Salgado-Bierman and Sandra Bayona for pushing me towards this research. A shout out to Dr. Howe as well for first giving me the challenge of proving this little trick. For now though, I must go back to my studies.

References

[1] "Modulo Operation." *Wikipedia.* Wikimedia Foundation, 11 Oct. 2013. Web. 15 Nov. 2013. $< http://en.wikipedia.org/wiki/Modulo\_operation >$.