Parabola Volume 58, Issue 3 (2022)

Divisibility rules by repeated truncation of the unit digit

Bora Demirtas[1]

1 Introduction

Although divisibility tests are known, we mathematics lovers may not really have a solid conceptual and algorithmic comprehension on the underlying logic of divisibility rules, because we simply take it granted without questioning where these rules come from. Most of us usually resort to available resources when we need to deal with divisibility rules that are typically stated in a mechanical and uninteresting way. This leads to a lack of true understanding on how these rules work. Merely utilizing a mechanism that involves multiplying, adding, or subtracting numbers without actually grasping the analytical structure that forms the rules is likely to be unproductive and inefficient.

Let us now have our own eureka moment, and say our own version of "aha, now I see it!". The purpose of this manuscript is to provide an easy-to-follow recipe that can be employed for implementing checks for divisibility. Divisibility rules are not new; here, however, I convey a straightforward set of modular arithmetic-based principles behind divisibility rules to make them more accessible. Divisibility is consequential in a broad range of contexts. For example, checking for primality (whether a particular number N is prime or composite) for small numbers N entails testing N for division by each of the primes in turn up to $\sqrt{N}$. In this paper, I elaborate on the design and construction of these rules that can be formulated in a unified framework for any given divisor. I also generalise this framework to arbitrary bases.

This article relies heavily on modular arithmetic, so I will first give a gentle introduction to this topic, following [1].

[1]Bora Demirtas is a junior student at Oak Park and River Forest High School in Oak Park, Illinois.

2 Modular arithmetic

Imagine a clock. If it is now 10 o'clock, then in 6 hours it will be 4 o'clock: we write this as $10 + 6 \equiv 4 \pmod{12}$. Here "mod 12" means that we are using a 12-hour clock, so that 16 is replaced by 4, and we write "$\equiv$" instead of "$=$" because it is a different form of equality. Similarly, now suppose that 9 more hours pass, the time will be 1 o'clock, $4 + 9 \equiv 1 \pmod{12}$. See the clocks below for a graphical display in the above order.

This type of calculation is called clock arithmetic; if we add the hours and get a number that is 12 or larger, then we subtract 12 or a multiple of 12. The answer is then the remainder after we divide the sum by 12, and it should be one of the numbers from 0 to 11. In general, two integers x and y are *congruent mod* D if x and y leave the same remainder when divided by a positive integer D, and we write $x \equiv y \pmod{D}$.

For example, as we have seen that

$$16 \equiv 4 \pmod{12} \quad \text{and} \quad 13 \equiv 1 \pmod{12}\,.$$

The abbreviation "mod" stands for "modulo", and the formal name for clock arithmetic is *modular arithmetic*. It follows from the definition that $x \equiv y \pmod{p}$ whenever the difference $x - y$ is divisible by p. For example,

$$17 \equiv 2 \pmod{5}\,, \quad 48 \equiv 8 \pmod{10} \quad \text{and} \quad 7 \equiv -2 \pmod{9}$$

since 5 divides $17 - 2 = 15$, 10 divides $48 - 8 = 40$ and 9 divides $7 - (-2) = 9$.

Since the only remainders when we divide by p are be $0, 1, \ldots, p-1$, every integer is congruent to one of these. We can also carry out arithmetic operations on congruences as long as we stick to the same modulus. For instance, given the congruences

$$9 \equiv 2 \pmod{7} \quad \text{and} \quad 13 \equiv 6 \pmod{7}\,,$$

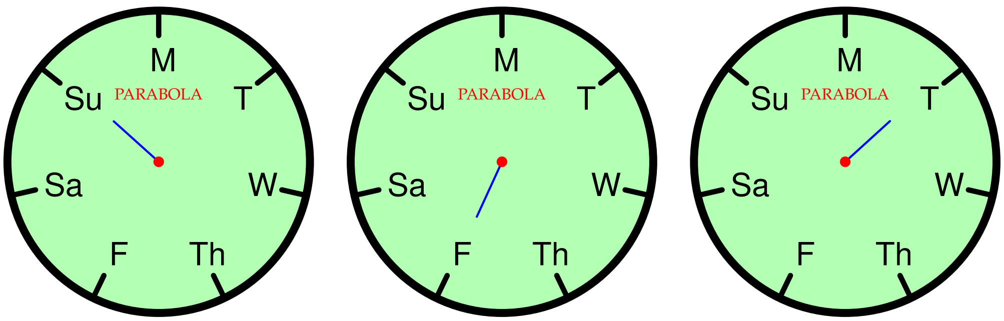
we can add, subtract, and multiply as follows:

$$\begin{aligned} 9 + 13 &\equiv 2 + 6 \equiv 8 \equiv 1 \pmod{7} \\ 9 - 13 &\equiv 2 - 6 \equiv -4 \equiv 3 \pmod{7} \\ 9 \times 13 &\equiv 2 \times 6 \equiv 12 \equiv 5 \pmod{7}\,. \end{aligned}$$

In general, if $x \equiv y \pmod p$ and $z \equiv w \pmod p$, then

$$
\begin{aligned}
x + z &\equiv y + w \pmod p \\
x - z &\equiv y - w \pmod p \\
x \times z &\equiv y \times w \pmod p .
\end{aligned}
$$

Life is much simpler with modular arithmetic because many things in life have some sort of periodicity, a phenomenon that can be naturally approached by modular thinking. A well-known example is the seven days of the week which cycle around like the hours on a clock. Suppose that each day is coded by integers ranging from 0 to 6, where 0 stands for Monday, 6 stands for Sunday, and the other days follow the obvious order. In the picture below (assuming time progresses in the forward direction), if it is now Sunday, then in five days' time it will be Friday, because $6 + 5 = 11 \equiv 4 \pmod 7$. When four more days pass, it will be Tuesday, because $4 + 4 = 8 \equiv 1 \pmod 7$.



Continuing with days of the week, in the calendar we use today, a regular year has 365 days, and a leap year has an extra day on 29 February. The leap years are those that are divisible by 4, except for the century years that are not also divisible by 400. Here is another use of modular arithmetic: since $365 \equiv 1 \pmod 7$, the day of the week on which any particular date falls advances by one each year, or two when a leap day kicks in. For example, the New Year's Eve last year, 31 December 2021, was Friday. The next one, 31 December 2022, will be Saturday, and the one after that, 31 December 2023, will be Sunday. Then, we will have a leap year in 2024, that is why we need to add one more day for that, so 31 December 2024 will fall on Tuesday.

OK, let me get a little personal. I was born on 20 August 2006. It was Sunday. When will my birthday be on Sunday again? Let me call this *super birthday*. The answer is 2023. Why? There are four leap years between my birth year and 2023 (2008, 2012, 2016 and 2020). Count one day for every year, and add one more day for each of the leap years: $2023 - 2006 + 4 \equiv 21 \equiv 0 \pmod 7$. Bingo! How about calculating your own nearest super birthday and have a bigger cake on that day? (Please remember me when you are having more cake fun.)

Here is a hopefully entertaining question: When will be the next February that has five sweet Fridays? For this to happen, the year must be a leap year, and the first and last days of the month should be Friday. Think why! There is just no other chance. Last time it happened was in 2008. The cycle of days repeats every 28 years as there are seven days in a week, and leap years happen every four years. So, the next time a February will have five Fridays will be in $2008 + 28 = 2036$!

3 Divisibility rules

After this quick introduction to modular arithmetic, let us go back to divisibility. In the division operation in the realm of integers, $N = qD + r$ where q is the quotient, D is the divisor, and $r < D$ is the remainder. Divisibility means that the remainder is 0 after dividing a number N by another number p. If that happens, N is said to be *divisible* by D, and D is said to be a *divisor* of N. In this case, $N \equiv 0 \pmod{D}$.

I will now show rules for divisibility by 2, 3, 5, 7 and 19. Then I will provide an algorithmic infrastructure for subsequent, more sophisticated rules. For each of these rules, let $N = a_n \cdots a_1 a_0$ be an $n+1$ digit integer and define $a = 10^{n-1}a_n + \cdots + a_1$. Then

$$N = 10^n a_n + \cdots + 10a_1 + a_0 = 10a + b$$

where $b = a_0$.

Divisibility rule for 2

Since $10 \equiv 0 \pmod{2}$, it follows that $N \equiv 10a + b \equiv b \pmod{2}$. Therefore, N is divisible by 2 if and only if b, the last digit of N, is even; that is, if and only if b is 0, 2, 4, 6 or 8. For instance, 126 is divisible by 2 since its last digit is 6.

Divisibility rule for 3

Since $10 \equiv 1 \pmod{3}$, it follows that

$$N = 10^n a_n + \cdots + 10a_1 + a_0 \equiv 1^n a_n + \cdots + 1a_1 + a_0 \equiv a_n + \cdots + a_1 + a_0 \pmod{3}.$$

Therefore, N is divisible by 3 if and only if the sum of digits of N is divisible by 3. For instance, 126 is divisible by 3 since its sum of digits $1 + 2 + 6 = 9$ is divisible by 3.

Divisibility rule for 5

Since $N \equiv b \pmod{5}$, it follows that $N \equiv 0 \pmod{5}$ if and only if $b \equiv 0 \pmod{5}$. Therefore, N is divisible by 5 if and only if b is either 0 or 5.
For instance, 126 is not divisible by 5 since its last digit, 6, is neither 0 nor 5.

Divisibility rule for 7

Since $1 \equiv -20 \pmod{7}$, it follows that $N \equiv 10a + b \equiv 10a - 20b \equiv 10(a - 2b) \pmod{7}$. The numbers 7 and 10 are coprime, so 7 divides $10(a-2b)$ if and only if 7 divides $a-2b$. Therefore, any number N is divisible by 7 if and only if 7 divides the number obtained by subtracting the last digit of N twice from the rest of the digits.
For instance, 126 is divisible by 7 since 7 divides $12 - 2 \times 6 = 0$.

Example. By the divisibility rules above, $N = 17276$ is divisible by 2 but not 3 or 5 since the last digit of N is 6 and since the sum of digits $1 + 7 + 2 + 7 + 6 = 23$ is not divisible by 3. To determine whether N is divisible by 7, we can use the divisibility rule for 7 and check whether 7 divides $1727 - 2 \times 6 = 1715$. To see whether this is true, we can apply the rule again: 1715 is divisible by 7 if and only if 7 divides $171 - 2 \times 5 = 161$. Let us apply the rule one more time: 161 is divisible by 7 if and only if 7 divides $16 - 2 \times 1 = 14$. Since 14 is divisible by 7, then so is 161, 1715 and $N = 17276$.

I will now present divisibility rules for 11 and 19. Before reading on, can you find such recursive rules yourself?

Divisibility rule for 11

Since $1 \equiv -10 \pmod{11}$, it follows that $N \equiv 10a + b \equiv 10a - 10b \equiv -(a - b) \pmod{11}$. Therefore, a number N is divisible by 11 if and only if 11 divides the number obtained by subtracting the last digit of N from the rest of the digits.
For instance, 126 is not divisible by 11 since 11 does not divide $12 - 6 = 6$.

A better-known rule is based on the difference of the sums of even and odd digits. In particular,

$$N = 10^n a_n + \cdots + 10a_1 + a_0 \equiv (-1)^n a_n + \cdots - a_1 + a_0 \pmod{11}.$$

Then N is divisible by 11 if and only if 11 divides the difference of the odd-positioned digits of N and the even-positioned digits of N. For example, 4323 is divisible by 11 since the difference of $4 + 2 = 6$ and $3 + 3 = 6$ is 0 which is divisible by 11.

Divisibility rule for 19

Since $1 \equiv 20 \pmod{19}$, it follows that $N \equiv 10a + b \equiv 10a + 20b \equiv 10(a + 2b) \pmod{19}$. Numbers 10 and 19 are coprime, so 19 divides $10(a+2b)$ if and only if 19 divides $a+2b$. Therefore, a number N is divisible by 19 if and only if 19 divides the number obtained by adding the last digit of N twice to the rest of the digits.
For instance, 456 is divisible by 19 since 19 divides $45 + 2 \times 6 = 57$.

Example. By the divisibility rules above, $N = 192807263$ is divisible by 11 since the difference of $1+2+0+2+3 = 8$ and $9+8+7+6 = 30$ is -22 which is divisible by 11. To determine whether $N = 17276$ is divisible by 19, we can use the divisibility rule for 19 and check whether 19 divides $1727 + 2 \times 6 = 1739$. To see whether this is true, we can apply the rule again: 1739 is divisible by 19 if and only if 19 divides $173 + 2 \times 9 = 191$. Since 191 is not divisible by 19, neither 1739 nor $N = 17276$ are divisible by 19.

Do you see a pattern emerging from the divisibility rules above?

4 General divisibility rules

The divisibility rules above suggest a unified framework for creating divisibility rules. I will focus on those divisors D which are coprime to 2 and 5 and thus also to 10. These divisors can be written as $D = 10c + d$ where $d = \pm 1, \pm 3$.

Divisibility rule for numbers of the form $D = 10c - 1$

Since $1 \equiv 10c \pmod{D}$, it follows that $N \equiv 10a + b \equiv 10a + 10cb \equiv 10(a + bc) \pmod{D}$. Therefore, any number N is divisible by D if and only if D divides the number obtained by adding N's last digit c times to the rest of N's digits.

For instance, $N = 319$ is divisible by $D = 29$ since $29 = 10c - 1$ for $c = 3$ and since 29 divides $31 + c \times 9 = 31 + 3 \times 9 = 58$.

Divisibility rule for numbers of the form $D = 10c + 1$

Since $1 \equiv -10c \pmod{D}$, it follows that $N \equiv 10a+b \equiv 10a-10cb \equiv 10(a-bc) \pmod{D}$. Therefore, a number N is divisible by D if and only if D divides the number obtained by subtracting N's last digit c times from the rest of N's digits.

For instance, $N = 441$ is divisible by $D = 21$ since $21 = 10c + 1$ for $c = 2$ and since 21 divides $44 - c \times 1 = 44 - 2 \times 1 = 42$.

Divisibility rule for numbers of the form $D = 10c - 3$

Since $3(10c - 3) \equiv 3 \times 0 \equiv 0 \pmod{D}$, we have $1 \equiv 1 - 3(10c - 3) \equiv 10(-3c + 1) \pmod{D}$. Therefore, $N \equiv 10a + b \equiv 10a + 10(-3c + 1)b \equiv 10(a - (3c - 1)b) \pmod{D}$. It follows that any number N is divisible by D if and only if D divides the number obtained by subtracting N's last digit $3c - 1$ times from the rest of N's digits.

For instance, $N = 323$ is divisible by $D = 17$ since $19 = 10c - 3$ for $c = 2$ and since 17 divides $32 - (3c - 1) \times 3 = 32 - 5 \times 3 = 17$.

Divisibility rule for numbers of the form $D = 10c + 3$

Since $3(10c+3) \equiv 3 \times 0 \equiv 0 \pmod{D}$, we have $1 \equiv 1+3(10c+3) \equiv 10(3c+1) \pmod{D}$. Therefore, $N \equiv 10a + b \equiv 10a + 10(3c + 1)b \equiv 10(a + (3c + 1)b) \pmod{D}$. It follows that any number N is divisible by D if and only if D divides the number obtained by adding N's last digit $3c + 1$ times to the rest of N's digits.

For instance, $N = 403$ is divisible by $D = 13$ since $13 = 10c + 3$ for $c = 1$ and since 13 divides $40 + (3c + 1) \times 3 = 40 + 4 \times 3 = 52$.

Example. I conclude this section with a fun composite number. To check whether N is divisible by $D = 99$, one could check whether N is divisible by both 9 and 11. However, a more exciting approach is to group the digits of N in pairs from right, and add them. If this sum is divisible by 99, then N is divisible by 99, since $100 \equiv 1 \pmod{99}$. More generally, $10^{2m} \equiv 1 \pmod{99}$ for $m \geq 1$. Does 99 divide 1234567818? To check this, add digit pairs as follows: $12 + 34 + 56 + 78 + 18 = 198 = 99 \times 2$. The answer is yes!

5 Divisibility rules for arbitrary bases

The divisibility rules above assume that the number N is written as a sequence of decimal ($q = 10$) digits. However, we can also find divisibility rules when N is written using base q digits, such as binary ($q = 2$) digits, for instance. Let $N = a_n \cdots a_1 a_0$ be an $n+1$ digit integer written using base q digits, and define $a = q^{n-1}a_n + \cdots + a_1$. Then

$$N = q^n a_n + \cdots + qa_1 + a_0 = qa + b$$

where $b = a_0$. Our main result is as follows.

Theorem. *Let $N = qa + b$ and $D = qc + d$ be integers with $a, b, c, d, q \in \mathbb{Z}$ and $\gcd(d, q) = 1$. Also, let k be an integer such that $kd \equiv -1 \pmod{q}$. Then N is divisible by D if and only if D divides the number*

$$a + \left(kc + \frac{kd+1}{q}\right)b\,.$$

Proof. Note that $kd + 1$ is divisible by q. Since $kD \equiv k \times 0 \equiv 0 \pmod{D}$,

$$1 \equiv 1 + kD \equiv 1 + k(qc + d) \equiv kqc + (kd + 1) \equiv q\left(kc + \frac{kd+1}{q}\right) \pmod{D}\,.$$

Therefore,

$$N \equiv qa + b \equiv qa + q\left(kc + \frac{kd+1}{q}\right)b \equiv q\left(a + \left(kc + \frac{kd+1}{q}\right)b\right) \pmod{D}\,.$$

Since d and q are coprime, it follows that $D = qc + d$ and q are also coprime. Therefore, $q(a + (kc + (kd+1)/q)b)$ is divisible by D if and only if D divides $a + (kc + (kd+1)/q)b$. The theorem now follows. $\square$

This theorem allows us to find divisibility rules over arbitrary bases.

Example. To derive the divisibility rule for 7 from Section 3 from the theorem above, let $q = 10$ and $D = 7$. To express D as $qc + d = 10c + d$, we could choose the numbers $c = 1$, $d = -3$ and $k = -3$, noting that $kd \equiv (-3)^2 \equiv 9 \equiv -1 \pmod{10}$. By the theorem, N is divisible by 7 if and only if 7 divides

$$a + \left(kc + \frac{kd+1}{q}\right)b = a + \left(-3 \times 1 + \frac{(-3) \times (-3) + 1}{10}\right)b = a - 2b\,,$$

which is the rule that we found previously.

Example. Let us now derive the divisibility rule for 7 with respect to the base $q = 2$. To express D as $qc + d = 2c + d$, we could choose the numbers $c = 3$, $d = 1$ and $k = 1$, noting that $kd \equiv 1^2 \equiv 1 \equiv -1 \pmod{2}$. By the theorem, any number $N = 2a + b$ is divisible by 7 if and only if 7 divides

$$a + \left(kc + \frac{kd+1}{q}\right)b = a + \left(1 \times 3 + \frac{1 \times 1 + 1}{2}\right)b = a + 4b\,,$$

which is a different rule than that found previously.

For instance, note that $N = 91 = 2a + b$ for $a = 45$ and $b = 1$. Therefore, $N = 91$ is divisible by 7 since 7 divides $a + 4b = 45 + 4 \times 1 = 49$.

Acknowledgements

The author is grateful to the Editor, Thomas Britz, for suggestions that considerably improved the article. The author also would like to express his heart-felt thanks to Sin Keong Tong for his contributions that raised this manuscript to a whole new level.

References

[1] R. Wilson, *Number Theory, A Very Short Introduction*, Oxford University Press, Oxford, UK, 2020.