1-28-2019

Divisibility Tests and Factoring

First, I'll discuss quick ways for deciding whether a number is divisible by various small integers. In what follows, I'll assume that numbers are represented as strings of decimal digits (i.e. in base 10) as usual.

Proposition. (a) An integer is divisible by 2 if and only if its last digit is divisible by 2.

(b) An integer is divisible by 5 if and only if its last digit is 0 or 5.

Proof. The proofs for these two tests are nearly identical; I'll do the one for divisibility by 2 as an example.

Suppose the decimal representation of x is

$$x_n x_{n-1} \dots x_2 x_1 x_0.$$

That is, x_0 is the units digit, x_1 is the tens digit, and so on. For 1728,

$$x_3 = 1, x_2 = 7, x_1 = 2, x_0 = 8.$$

Then

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_1 \cdot 10 + x_0.$$

Since $2 \mid 10$, it follows that $2 \mid 10^n$ for $n \geq 1$. Thus, $2 \mid x$ if and only if $2 \mid x_0$ — that is, x is even if and only if the units digit x_0 is even. □

Definition. The **digital sum** of an integer n is the sum of the digits in the decimal representation of n.

For instance, the digital sum of 1728 is 18:

$$1 + 7 + 2 + 8 = 18.$$

The digital sum of 278349 is 33:

$$2 + 7 + 8 + 3 + 4 + 9 = 33.$$

Proposition. (a) An integer is divisible by 3 if and only if its digital sum is divisible by 3.

(b) An integer is divisible by 9 if and only if its digital sum is divisible by 9.

Proof. Suppose the decimal representation of x is

$$x_n x_{n-1} \dots x_2 x_1 x_0.$$

Then

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_1 \cdot 10 + x_0.$$

The sum of the digits of x is

$$s = x_n + x_{n-1} + \cdots + x_1 + x_0.$$

Observe that

$$x - s = \left(x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_1 \cdot 10 + x_0\right) - (x_n + x_{n-1} + \cdots + x_1 + x_0) =$$

$$x_n(10^n - 1) + x_{n-1}(10^{n-1} - 1) + \cdots + x_1(10 - 1).$$

The right side is divisible by 3 and by 9, because

$$10 - 1 = 9, 10^2 - 1 = 99, 10^3 - 1 = 999, \quad \text{and so on.}$$

That is,

$$x - s = \text{(something divisible by 3 or 9)}.$$

Hence, if $3 \mid x$, then $3 \mid s$, and if $3 \mid s$, then $3 \mid x$. And if $9 \mid x$, then $9 \mid s$, and if $9 \mid s$, then $9 \mid x$. □

Note that you can continue to sum the digits of the numbers that you get until you get something that is obviously divisible by 3 or 9. For example, start with 893948083:

$$8 + 9 + 3 + 9 + 4 + 8 + 0 + 8 + 3 = 52, \quad 5 + 2 = 7.$$

Since 7 is not divisible by 3 or by 9, neither is 52. Since 52 is not divisible by 3 or by 9, neither is 893948083.

The next result can be proved by a method similar to that used to prove the test for divisibility by 9. Since the proof is a little more complicated, I'll merely state the result and give an example.

Proposition. To test divisibility by 7, remove the last (units) digit, double it, and subtract it from the remainder of the number. The original number is divisible by 7 if and only if the result is divisible by 7. □

Example. Use the test in the proposition to test 9423242 for divisibility by 7.

$$942324 - 2 \cdot 2 = 942320,$$

$$94232 - 2 \cdot 0 = 94232,$$

$$9423 - 2 \cdot 2 = 9419,$$

$$941 - 2 \cdot 9 = 923,$$

$$92 - 2 \cdot 3 = 86.$$

86 is not divisible by 7, so 9423242 is not divisible by 7. □

It is difficult to factor a large, arbitrary integer in a reasonable amount of time. You can use simple divisibility tests like those above to deal with "obvious" cases, but the general problem is difficult, and the object of current research.

I'll describe a simple factoring method called **Fermat factorization**.

Proposition. Let n be an odd integer. There is a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{factorizations} \\ \text{of } n \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{expressions of } n \text{ as the} \\ \text{difference of two squares} \end{array} \right\}$$

Proof. If $n = ab$, n is odd so a and b are odd. Then $a + b$ and $a - b$ are even, so $\dfrac{a+b}{2}$ and $\dfrac{a-b}{2}$ are integers. Now

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

This expresses n as a difference of two squares.

Conversely, suppose n is written as as difference of squares: $n = s^2 - t^2$. Then

$$n = (s - t)(s + t).$$

This is a factorization of n.

You can check that these two procedures — factors to difference and difference to factors — "undo" one another. □

Example. Use Fermat factorization to factor 4819.

The idea is to try to write 4819 as $s^2 - t^2$. I will form $s^2 - 4819$ and increase s till I get a perfect square. What s's do I need to use?

First, $\sqrt{4819} \approx 69.4$. Since $4819 = s^2 - t^2$, s must be at least as big as $69.4 \approx 70$.

On the other hand, the factorization with the biggest factor is $4819 = 1 \cdot 4819$. By the proof of the last result, this would produce an s of the form $\dfrac{4819+1}{2} = 2410$. So I need to try s for $70 \leq s \leq 2410$.

On the very first try,

$$70^2 - 4819 = 4900 - 4819 = 81 = 9^2.$$

Thus, $s = 70$ and $t = 9$. $s + t = 79$, $s - t = 61$, and $79 \cdot 61 = 4819$. □

Example. Use Fermat factorization to factor 779.

$\sqrt{779} \approx 27.91057$, so I need $s \geq 28$. $\dfrac{779+1}{2} = 390$, so $s \leq 390$.

s	$s^2 - 779$
28	$28^2 - 779 = 5$
29	$29^2 - 779 = 62$
30	$30^2 - 779 = 121 = 11^2$

The factors are $30 + 11 = 41$ and $30 - 11 = 19$: $779 = 41 \cdot 19$. □
