Intro to Number Theory: Creating your own divisibility test

Dr. David M. Goulet

November 14, 2007

Suppose you have a prime number p and want to find a divisibility test for it that involves chopping off the last k digits. Suppose that the number you want to test can be written in decimal form as $d_1 d_2 \dots d_n$.

$$\begin{aligned} d_1 \dots d_n &= (d_1 \dots d_{n-k})10^k + d_{n-k+1} \dots d_n \\ &= (d_1 \dots d_{n-k})p + (d_1 \dots d_{n-k})(10^k - p) + d_{n-k+1} \dots d_n \end{aligned}$$

The first term is obviously divisible by p. So let's focus on the remaining terms.

$$(d_1 \dots d_{n-k})(10^k - p) + d_{n-k+1} \dots d_n =$$
$$(d_1 \dots d_{n-k} - \alpha(d_{n-k+1} \dots d_n))(10^k - p) + (d_{n-k+1} \dots d_n)(1 + \alpha(10^k - p))$$

So, if we can choose α so that p divides $\alpha 10^k + 1$ then our test method will be as follows.

1. Remove the last k digits from the number.
2. Subtract α times those digits from what remains.
3. If the result is divisible by p, then so was the original number.

Example: p=13

$$\begin{aligned} d_1 \dots d_n &= 100(d_1 \dots d_{n-2}) + d_{n-1}d_n \\ &= 13(d_1 \dots d_{n-2}) + 87(d_1 \dots d_{n-2}) + d_{n-1}d_n \\ &= 13(d_1 \dots d_{n-2}) + 87(d_1 \dots d_{n-2} - \alpha(d_{n-1}d_n)) + (d_{n-1}d_n)(1 + 87\alpha) \end{aligned}$$

We need to find an α so that 13 divides $87\alpha + 1$. The smallest choice is 10 $(87 * 10 - 1 = 869 = 13 * 67$. To see this test in action, let's find if 132431 is divisible by 13.

$$1324 - 10 * 31 = 1014$$
$$10 - 10 * 14 = -130 = -13 * 10$$

The test says that 132431 is divisible by 13 (132431=13*61*167).

The only loose end we need to address is the question of whether, for any prime p, there is an integer α, with $1 \leq \alpha \leq p$, so that p divides $\alpha(10^k - p) + 1$. The answer is yes, provided that $p \neq 2$ and $p \neq 5$. The proof is actually very simple.

Proof: Suppose that a and b are integers and that p does not divide a. Consider the p values of

$$ax + b\ (modp)$$

for $x = 1, 2, \ldots, p$. Suppose that two of these values are the same. That is, there is an integer $1 \leq x \leq p$ and an integer $1 \leq y \leq p$, with $x \neq y$, so that

$$(ax + b)(modp) - (ay + b)(modp) = 0$$

Simplifying this shows that

$$a(x - y) = 0\,(modp)$$

By hypothesis, p does not divide a. So, because x and y are both ≥ 1 and $\leq p$, $x = y$. This contradicts the hypothesis that x and y are different. Therefor, all of the values of $(ax + b)(modp)$ are different for $x = 1, 2, \ldots, p$. Notice also that these values must be in the range $[0, p-1]$. Therefor, because there are exactly p distinct values, they cover this range completely. So, for any given integer $c \in [0, p - 1]$ there is a unique integer $x \in [1, p]$ so that $ax + b = c\,(modp)$. $\Box$

Applying this to our problem with $a = 10^k - p$, $b = 1$, and $c = 0$ shows that there is a value of α so that $\alpha(10^k - p) + 1$ is divisible by p, provided that p does not divide 10^k. That is, provided that $p \neq 2$ and $p \neq 5$.

Comment: Notice that our proof does not tell you how to find α. It only tells you that there is an $\alpha \in [1, p]$.

Example: 103 We wish to find α so that 103 divides $897\alpha + 1$. In other words, find integer α so that $897\alpha + 1 = 103k$, for some integer k.

Notice that $897 = 3 * 13 * 23$. We might expedite this process by using some modular arithmetic. For example, using mod 3, we find k=3q+1 so that $299\alpha = 103q + 34$. Now, using mod 13, we find $q = 13m + 8$, so that $23\alpha = 103m + 66$. Finally, using mod 23, we find $m = 23n + 17$, so that $\alpha = 103n + 79$. Therefor, we choose $\alpha = 79$.

As a test we apply this to 11592740743.

$$11592740 - 79 * 743 = 11534043$$
$$11534 - 79 * 43 = 8137 = 103 * 79$$

Therefor 11592740743 is divisible by 103 (note $11592740743 = 103^5$). Note that we can also use a negative value for α. For $p = 13$ we can use $\alpha = 10$ or $\alpha = -3$ and for $p = 103$ we can use $\alpha = 79$ or $\alpha = 24$.

Table 1: Let k be the number of digits in p. We list here the smallest (in absolute value) α for each of the first 10 p's, excluding 2 and 5, so that $10^k\alpha + 1 \equiv 0$ (mod p). The most efficient choices are in bold.

p	3	7	11	13	17	19	23	29	31	37
k	1	1	2	2	2	2	2	2	2	2
	2	**2**	**10**	**10**	**9**	15	**20**	**20**	**22**	27
α	**-1**	-5	-1	-3	-8	**-4**	-3	-9	-9	**-10**
	7	3	91	77	53	79	87	69	71	73
$(10^k\alpha + 1)/p$	-3	-7	-9	-23	-47	-21	-13	-31	-29	-27

Notice that some of the divisibility tests use the same α values. This makes it possible to perform multiple tests simultaneously. For example, divisibility by 33 or 130 is can be checked with a single use of this method.