

Final Review Comments for ‘Finding Remainder on Dividing Numbers’

Date: July 23, 2015

The results of this manuscript are elementary but may be useful for computation purpose. The following are suggestions for improvement.

In the abstract, it was mentioned that ‘In this paper, we **also** prove an interesting ...’, meaning that the divisibility results are basically byproducts of the main result which, as the title suggests, is about finding remainder on dividing numbers. Since the authors of the manuscript are mainly interested in the case of dividing numbers by a prime number, the reviewer thinks that a theorem of the following type (see the Theorem below) should be the main result of the manuscript whereas the divisibility results may serve as corollaries of the main result. Moreover, it is ambiguous to write $N = a_m a_{m-1} \cdots a_0$ which may mean the product of the numbers $a_m, \cdots, a_0$. A quick way to fix this is to add ‘(in the decimal system)’ as parenthetical explanation.

Fact 1. Let p be a prime number. Then there is a ring homomorphism $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$, where $\phi(a) = \bar{a}$ is the congruent class modulo p . If $f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0$ with $x, a_m, \cdots, a_0 \in \mathbb{Z}$, then

$$\overline{f(x)} = \overline{a_m} \cdot \bar{x}^m + \overline{a_{m-1}} \cdot \bar{x}^{m-1} + \cdots + \overline{a_0}.$$

Fact 2. Let $a \in \mathbb{Z}$ and p be a prime number. Fermat’s Little Theorem says that if $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fact 3. Let p be a prime number and $\gcd(a, p) = 1$. Then the order d of $\bar{a}$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \cdots, \overline{p-1}\}$ satisfies $d \mid p-1$ by Fact 2 and Lagrange’s Theorem.

Definition. Let p be a prime not equal to 2 or 5. Let d be the order of $\alpha := \overline{10}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Then by Fact 3, one has $\alpha^{i+d} = \alpha$. This shows that the powers $\overline{10}^i$ exhibit periodic pattern of period d . If one writes $\overline{10}^i := \mu_i$, then $\mu_{i+d} = \mu_i$ (for convenience, we always represents μ_0 by 1).

Example 1.

- For $p = 3$, one has $d = 1$:

namely $\overline{10}^i, i \geq 0$ has the pattern $(\mu_0) = (1)$.

- For $p = 7$, $d = 6$, and $(\mu_0, \dots, \mu_5) = (1, 3, 2, -1, -3, -2)$ (which is $(1, -4, 2, -1, 4, -2)$ as in the article).
- For $p = 11$, $d = 2$, and $(\mu_0, \mu_1) = (1, -1)$.
- For $p = 13$, $d = 6$, and $(\mu_0, \dots, \mu_5) = (1, -3, -4, -1, 3, 4)$ (which is $(1, -3, 9, -1, 3, -9)$ as in the article).

Example 2. Since $10 = 2 \cdot 5$, the divisibility by $p = 2$ or $p = 5$ is very obvious. It is easy to see that the remainder for dividing N by 2 or by 5 is given by the last digit (i.e. a_0) of N .

Theorem. Let $p \neq 2, 5$ be a prime number and $N = a_m a_{m-1} \dots a_0$ be a positive integer in the decimal system, i.e.

$$N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \dots + a_0,$$

where $0 \leq a_0, \dots, a_m \leq 9$ are integers. Then the remainder for dividing N by p is the same as that of dividing

$$\sum_{i=0}^m \mu_i \cdot a_i = a_0 + \mu_1 a_1 + \dots + \mu_m a_m,$$

where μ_i has periodic pattern which is defined and explained above.

Proof. Writing

$$N = 10^0 \cdot a_0 + 10^1 \cdot a_1 + \dots + 10^{m-1} \cdot a_{m-1} + 10^m \cdot a_m$$

and taking congruence modulo p , it follows from Fact 1 that

$$\begin{aligned} \overline{N} &\equiv \overline{10}^0 \cdot a_0 + \overline{10}^1 \cdot a_1 + \dots + \overline{10}^{m-1} \cdot a_{m-1} + \overline{10}^m \cdot a_m \\ &\equiv a_0 + \mu_1 a_1 + \dots + \mu_{m-1} a_{m-1} + \mu_m a_m \pmod{p}. \end{aligned}$$

□

Corollary. Let p and N be given as in the above theorem. Then p divides N if and only if p divides

$$a_0 + \mu_1 a_1 + \cdots + \mu_{m-1} a_{m-1} + \mu_m a_m.$$

Proof. Immediately.

□

Example 3. Consider $N = 29397499 = 37 \cdot 97 \cdot 8191$ and $p = 37$. By direct computation, 10 is of order $d = 3$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, thus $(\mu_0, \mu_1, \mu_2) = (1, 10, -11)$. Then the number

$$1 \cdot 9 + 10 \cdot 9 + (-11) \cdot 4 + 1 \cdot 7 + 10 \cdot 9 + (-11) \cdot 3 + 1 \cdot 9 + 10 \cdot 2 = 148$$

must be divisible by 37. This is true, since $148 = 4 \cdot 37$.