way as to render the calculation difficult, and special functions have been invented for the graphing, to avoid these inconvenient figures and permit an accurate determination of the area.

Any advances which permit an increased accuracy in graphical calculations will be welcomed by the chemist.

18. Conclusion. It has been the purpose of this article to point out some of the mathematical needs of modern chemistry. It would be appreciated if courses in mathematics could emphasize some of these things, along with the calculations of volumes, lengths of curves, and moments of inertia and other calculations which are included for the benefit of the engineer. The present courses should not be changed, however, for mathematics is much more valuable to the student of chemistry as a mental training than as a source of technical methods. In physical chemistry the chief aim is to emphasize the research point of view and to interest the student in the mechanism of natural phenomena and there is no better way to develop the necessary originality in a student than to have him solve hundreds and thousands of problems in pure mathematics.

A SIMPLIFICATION OF CERTAIN PROBLEMS IN ARITHMETICAL DIVISION

By MORGAN WARD, California Institute of Technology

1. Like all inverse operations, the process of dividing one integer by another requires certain tentative steps irresolvable into the direct operations of addition and multiplication. Any method of division has then a three-fold aim: to reduce as far as possible (1) the number of these tentative steps, (2) the difficulty of each step, and (3) the amount of addition, multiplication and mere copying necessary to combine the results of the separate steps into the correct quotient. These aims conflict to a certain extent and our ordinary "long" division is a sort of compromise between them. It may in fact be considerably improved as regards the third requirement.[1]

The object of this paper is to exhibit a method of division satisfying the requirements above and applicable to a class of problems where solution by ordinary division is excessively laborious, if not impossible. Our main result is given in section 4; its proof, which rests upon the most elementary properties of congruences and power residues, is developed in sections 2 and 3. The concluding section is devoted to numerical examples.

---

[1] See a discussion of "long" division by L. S. Dederick in this Monthly, vol. 33 (1926), pp. 143–144.

2. In what follows small italic and Greek letters stand for positive integers or zero.

Denote the quotient obtained on dividing a by $b \neq 0$ by

$$(1) \qquad [a/b] = q \quad \text{so that} \quad a = qb + r \qquad 0 \leqq r < b.$$

Then $q = 0$ when $b > a$ and is otherwise a positive integer. It is to be understood that b is never zero in the symbol $[a/b]$. Let us develop some of the properties of the symbol.

First, if $b = b_1 \cdot b_2$, it is easily shown[1] that

$$(I) \qquad \left[\frac{a}{b_1 b_2}\right] = \left[\frac{\left[\frac{a}{b_1}\right]}{b_2}\right] = \left[\frac{\left[\frac{a}{b_2}\right]}{b_1}\right]$$

Suppose $a = a_1 \cdot a_2$. Let $[a_1/b] = q_1$ and $[a_2/b] = q_2$ so that $a_1 = bq_1 + r_1$ and $a_2 = bq_2 + r_2$ $(0 \leqq r_1, r_2 < b)$. Then $a_1 a_2 = (bq_1q_2 + q_1r_2 + q_2r_1)b + r_1r_2$. Hence

$$(II) \qquad \left[\frac{a_1a_2}{b}\right] = b\left[\frac{a_1}{b}\right]\left[\frac{a_2}{b}\right] + r_2\left[\frac{a_1}{b}\right] + r_1\left[\frac{a_2}{b}\right] + \left[\frac{r_1r_2}{b}\right].$$

The following special cases of II are to be noted:

First, if $r_2 = 0$,

$$(IIa) \qquad \left[\frac{a_1a_2}{b}\right] = b\left[\frac{a_1}{b}\right]\left[\frac{a_2}{b}\right] + r_1\left[\frac{a_2}{b}\right] = a_2\left[\frac{a_1}{b}\right] + r_1\left[\frac{a_2}{b}\right].$$

Secondly, if $q_2 = 0$, then $a_2 < b$, $[a_2/b] = 0$, $r_2 = a_2$, and

$$(IIb) \qquad \left[\frac{a_1a_2}{b}\right] = a_2\left[\frac{a_1}{b}\right] + \left[\frac{a_2r_1}{b}\right].$$

Also if $a = a_1 + a_2$,

$$(III) \qquad \left[\frac{a}{b}\right] = \left[\frac{a_1}{b}\right] + \left[\frac{a_2}{b}\right] + \left[\frac{(r_1 + r_2)}{b}\right], \quad \text{where}$$
$$0 \leqq \left[\frac{(r_1 + r_2)}{b}\right] \leqq 1.$$

3. Assume now that a is greater than b and prime to it,

$$(2) \qquad U_m = \left[\frac{a^m}{b}\right]. \qquad \text{Then} \quad (2a) \quad U_0 = U_1 = 0.$$

We seek the general expression for U_m.

---

[1] Reid: *Elements of the Theory of Algebraic Numbers*, p. 27.

Let r be the least positive integer for which

$$a^{r+1} \equiv a \pmod{b}. \tag{3}$$

That is, r is the exponent to which a belongs, modulo b, so that $a, a^2, a^3, \cdots, a^r$ are all distinct. Let $a^s \equiv a_s \pmod{b}$ $(0 \leqq a_s < b)$ and

$$V_s = [aa_s/b], \quad \text{so that} \quad V_0 = 0, \quad V_s < b. \tag{4}$$

Then by (3), (4), $V_s = V_t$ when and only when $s \equiv t \pmod{r}$.

By (IIb), $U_m = [a \cdot a^{m-1}/b] = a[a^{m-1}/b] + [a \cdot a_{m-1}/b]$, $m \geqq 1$; or, by (2) and (4),

$$U_m = aU_{m-1} + V_{m-1}. \tag{5}$$

Thus $U_2 = aU_1 + V_1 = V_1$; $U_3 = aU_2 + V_2 = aV_1 + V_2$. Assume for some $s \geqq 2$

$$U_s = a^{s-2}V_1 + a^{s-3}V_2 + \cdots + aV_{s-2} + V_{s-1} = \sum_{K=1}^{s-1} a^{s-1-K}V_K.$$

Then

$$U_{s+1} = aU_s + V_s = \sum_{K=1}^{s-1} a^{s-K}V_K + V_s = \sum_{K=1}^{s} a^{s-K}V_K$$

or

$$U_{s+1} = \sum_{K=1}^{(s+1)-1} a^{(s+1)-1-K}V_K,$$

so that, by induction, for any $m \geqq 1$

$$U_m = \sum_{K=1}^{m-1} a^{m-1-K}V_K. \tag{6}$$

Now suppose

$$m - 1 = kr + \alpha \qquad (0 \leqq \alpha < r, \ k \geqq 0). \tag{7}$$

Divide K in (6) by r and let the quotient be τ and the remainder σ $(0 \leqq \tau \leqq k, 0 \leqq \sigma < r)$. Set $K = \tau_1 r + \sigma_1$ $(0 \leqq \sigma \leqq \alpha)$ and $K = \tau_2 r + \sigma_2$ $(\alpha < \sigma \leqq r-1)$. Then (6) may be written

$$\begin{aligned} U_m &= \sum_{\tau_1=0}^{k} \sum_{\sigma_1=0}^{\alpha} a^{(k-\tau_1)r+\alpha-\sigma_1}V_{\tau_1 r+\sigma_1} + \sum_{\tau_2=0}^{k-1} \sum_{\sigma_2=\alpha_1}^{r-1} a^{(k-1-\tau_2)r+\alpha+r-\sigma_2}V_{\tau_2 r+\sigma_2} \\ &= \sum_{\tau_1=0}^{k} a^{(k-\tau_1)r} \sum_{\sigma_1=0}^{\alpha} a^{\alpha-\sigma_1}V_{\sigma_1} + \sum_{\tau_2=0}^{k-1} a^{(k-1-\tau_2)r} \sum_{\sigma_2=\alpha_1}^{r-1} a^{\alpha+r-\sigma_2}V_{\sigma_2} \\ &= \sum_{\tau_1=0}^{k} a^{(k-\tau_1)r} \sum_{\sigma_1=0}^{\alpha} a^{\alpha-\sigma_1}V_{\sigma_1} + \sum_{\tau_2=0}^{k-1} a^{(k-1-\tau_2)r} \sum_{\sigma_1=1}^{r-1-\alpha} a^{\alpha+\sigma_1}V_{\alpha+\sigma_1} \end{aligned}$$

on replacing in the second expression $r-\sigma_2$ by σ_1 and changing the order of summation. But

$$\sum_{\tau_1=0}^{k} a^{(k-\tau_1)r} = \frac{a^{(k+1)r}-1}{a^r-1}; \qquad \sum_{\tau_2=0}^{k-1} a^{(k-1-\tau_2)r} = \frac{a^{kr}-1}{a^r-1}.$$

Hence we obtain the following theorem.

4. THEOREM: "Let b be any integer greater than a but not a power of a, and let m be any positive integer. Let k and α denote the quotient and remainder obtained on dividing $m-1$ by the least positive integer r for which $a^{r+1}-a$ is divisible by b. Then the quotient on dividing a^m by b is given by

$$\text{(IV)} \qquad \left[\frac{a^m}{b}\right] = \frac{a^{(k+1)r}-1}{a^r-1}(a^{\alpha-1}V_1 + a^{\alpha-2}V_2 + \cdots + aV_{\alpha-1} + V_\alpha) + \frac{a^{kr}-1}{a^r-1}a^\alpha(aV_{\alpha+1} + a^2V_{\alpha+2} + \cdots + a^{r-\alpha-1}V_{r-1}),$$

where $V_i=[a\cdot a_i/b]$ $(1\leqq i\leqq r-1)$ and a_i is the least positive residue of a^i modulo b."

The numbers V_i must be found by trial. They are always less than b and can be readily computed in conjunction with the a_i's; for from (4) we have $V_s=[a\cdot a_s/b]$, $a_{s+1}\equiv a^{s+1}\equiv a\cdot a^s\equiv a\cdot a_s \pmod b$, $0\leqq a_{s+1}<b$, or $a\cdot a_s = b\cdot V_s + a_{s+1}$, so that V_s is the quotient and a_{s+1} the remainder on dividing $a\cdot a_s$ by b. We can thus determine $V_1, V_2, \cdots, V_{r-1}$ step by step. If we have found by any means the residue system $a_1, a_2, \cdots, a_s, \cdots, a_{r-1}$, say by a table of indices modulo $b/(b, a)$, we have

$$V_s = (a\cdot a_s - a_{s+1})/b \tag{8}$$

which for small b's gives V_s by inspection.

The expressions in brackets in IV are indeed numbers in the scale a.

If the V's are assumed known, IV involves only additions and multiplications, for the first terms in each line are merely the sums of geometric progressions. Hence we have here a *formula* for the quotient of a^m by b.

There are several special cases of IV. First $\alpha=0$ if $m-1$ is exactly divisible by r, and IV becomes

$$\left[\frac{a^m}{b}\right] = \frac{a^{kr}-1}{a^r-1}(aV_1 + a^2V_2 + \cdots + a^{r-1}V_{r-1}) = \frac{a^m-1}{a^r-1}(a^{r-1}V_{r-1} + a^{r-2}V_{r-2} + \cdots + aV_1)$$

so that we have the result:

(IVa) $$\left[\frac{a^m}{b}\right] \equiv 0 (\text{mod } a) \qquad \text{if} \quad m \equiv 0 (\text{mod } r).$$

If $b = a^r - 1$, $V_1 = V_2 = V_3 = \cdots = V_{r-2} = 0$, $V_{r-1} = 1$, and

(IVb) $$\left[\frac{a^m}{b}\right] = \frac{a^{kr} - 1}{a^r - 1} a^{r-1}.$$

If $a = 10$, the expressions in round brackets in IV become ordinary numbers with digits $V_1 \cdots V_\alpha$; $V_{r-1} \cdots V_{\alpha+1}$, and the geometric progressions are numbers of the form

(IVc) $$100 \cdots 0100 \cdots 0100 \cdots 01 \cdots$$

where the 1's are separated by $r-1$ zeros.

The formulas I–IV enable us to solve any problem in division by separating a and b into sums and products in suitable ways. But IV is the only result essentially novel. Let us apply it to some numerical examples.

5. Example 1. To find the quotient when 10^{11} is divided by 13.

Here

$$a = 10, \quad b = 13, \quad m = 11, \quad a_1 = 10, \quad a \cdot a_1 = 100 = 7 \cdot 13 + 9.$$

$$\therefore v_1 = 7, \quad a_2 = 9, \quad a \cdot a_2 = 90 = 6 \cdot 13 + 12; \quad \therefore v_2 = 6, \quad a_3 = 12,$$

$$a \cdot a_3 = 120 = 9 \cdot 13 + 3;$$

$$\therefore v_3 = 9, \quad a_4 = 3, \quad a \cdot a_4 = 30 = 2 \cdot 13 + 4; \quad \therefore v_4 = 2, \quad a_5 = 4,$$

$$a \cdot a_5 = 40 = 3 \cdot 13 + 1;$$

$$\therefore v_5 = 3, \quad a_6 = 1, \quad r = 6, \quad m - 1 = 6 + 4. \quad \therefore k = 1, \quad \alpha = 4.$$

$$\left[\frac{10^{11}}{13}\right] = \left[\frac{10^{12} - 1}{10^6 - 1}\right] \cdot 7692 + \frac{10^6 - 1}{10^6 - 1} \cdot 10^4 \cdot 32$$

$$= (10^6 + 1) \cdot 7692 + 10^4 \cdot 32 = 7692307692.$$

The work here is exactly the same as in the ordinary process of short division:

$$13\overline{)100000000000}$$
$$7692307692.$$

Example 2. To find the quotient when 9^μ, where $\mu = (9^9)$, is divided by 19. Here $a = 9$, $b = 19$, $m = 9^9$, and 9, 5, 7, 6, 16, 11, 4, 17, 1 are the residues of $a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9$, so that $r = 9$.

$$m - 1 = 9^9 - 1 = (9^8 - 1)9 + 8, \quad \text{so that} \quad k = 9^8 - 1, \quad \alpha = 8.$$

Using (8), we readily find 4, 2, 3, 2, 7, 5, 1, 8 for $V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8$. Therefore if $\mu = (9^9)$ and $\nu = 9^8$,

$$\left[\frac{9^\mu}{19}\right] = \left(\frac{9^\nu - 1}{9^9 - 1}\right)(4 \cdot 9^7 + 2 \cdot 9^6 + 3 \cdot 9^5 + 2 \cdot 9^4 + 7 \cdot 9^3 + 5 \cdot 9^2 + 1 \cdot 9 + 8)$$

Example 3. To find the quotient when $2^{257} - 1$ is divided by 1023.

Here $a = 2$, $b = a^{10} - 1$, $r = 10$, and IVb is applicable. Since $2^{257} \equiv 2^7 \pmod{1023}$,

$$\left[\frac{2^{257} - 1}{1023}\right] = \left[\frac{2^{257}}{1023}\right] = \frac{2^{250} - 1}{2^{10} - 1} \cdot 2^9 = 2^9 + 2^{19} + 2^{29} + \cdots + 2^{249}.$$

FORMAL UNIFICATION OF GRADIENT, DIVERGENCE, AND CURL, BY MEANS OF AN INFINITESIMAL OPERATIONAL VOLUME

By VLADIMIR KARAPETOFF, Cornell University

In vector analysis, the results of the three differential operations known as taking the gradient, the divergence, and the curl of a function are radically different from each other, both from a mathematical and from a physical point of view. Nevertheless there is some formal connection among the operations themselves in that the same Hamiltonian operator "nabla" or "del" (∇) is used in all three.[1] This permits to denote the three operations as ∇, $\nabla\cdot$, and $\nabla\times$, respectively. In elementary text-books on vector analysis, the three operations and the Hamiltonian operator itself are introduced in Cartesian coördinates, thus perhaps leaving in the mind of the reader an unconscious impression that it is absolutely necessary to begin a problem by using the projections of both the operator and the operand.

On the other hand, the very purpose of vector analysis being to do away with resolving directed quantities into their components, as much as possible, a direct and unified interpretation of the foregoing differential operators in space is quite desirable. [In some advanced German works[2] this unification has been obtained by defining the gradient, the divergence, and the curl as follows:

$$\text{(A)} \qquad \nabla P = \lim_{\Delta \doteq 0} (1/\Delta v) \int_S ds P\,; \qquad \text{(B)} \qquad \nabla \cdot \boldsymbol{F} = \lim_{\Delta \doteq 0} (1/\Delta v) \int_S d\boldsymbol{s} \cdot \boldsymbol{F}\,;$$

$$\text{(C)} \qquad \nabla \times \boldsymbol{F} = \lim_{\Delta \doteq 0} (1/\Delta v) \int_S d\boldsymbol{s} \times F.$$

---

[1] In this article, by the Hamiltonian operator is meant the operator ∇ expressed in orthogonal coordinates, that is, $\nabla = i(\partial/\partial x) + j(\partial/\partial y) + k(\partial/\partial z)$

[2] C. Runge, *Vector Analysis* (English Translation), p. 95; W. von Ignatowsky, *Die Vektoranalysis*, vol. 1, p. 16; J. Spielrein, *Lehrbuch der Vektorrechnung*, p. 111.