A New Demonstration of an Arithmetic Theorem

Art. 1

Questions in higher arithmetic lead frequently to singular phenomena, much more so than in analysis, and this contributes a great deal to their allure. In analytical investigations it is evidently impossible to discover new truths, unless the way to them has been revealed by our mastery of their underlying principles. On the other hand, in arithmetic it is very often the case that, through induction and by some unexpected fortune, the most elegant new truths spring up, the demonstrations of which are so deeply hidden and shrouded in so much darkness, that they elude all efforts, and deny access to the keenest investigations. Furthermore, there are so many surprising connections between arithmetic truths, which are at first sight most heterogeneous, that we not infrequently arrive at a demonstration much desired and sought after through long meditations by a path very different from that which had been expected, while we are looking for something quite different. Generally speaking, truths of this kind are of such a nature that they can be approached by several very different paths, and it is not always the shortest paths that present themselves at first. With such a truth, which has been demonstrated through the most abstruse detours, it is certainly valuable if one happens to discover a simpler and more genuine explanation.

Art. 2

Among the questions mentioned in the preceding article, a prominent place is held by the theorem containing almost all the theory of quadratic residues, which in *Disquisitionibus Arithmeticis* (Section IV) is distinguished by the name of the *fundamental theorem*. LEGENDRE is undoubtedly to be regarded as the discoverer of this most elegant theorem, although the great geometers EULER and LAGRANGE had long before discovered several of its special cases by induction. I will not dwell here on enumerating the efforts of these men to find a demonstration; the reader is referred to their extensive work which has just been mentioned. However it is permissible to add, in confirmation of what has been stated in the previous article, an account of my own efforts. I had fallen upon the theorem itself on my own in 1795, at a time when I was completely ignorant of all that had already been discovered in higher arithmetic, and was completely shut out from literary resources. For a whole year it tortured me, and eluded me despite my most strenuous efforts, until at last I received the demonstration that I have delivered in the fourth Section of the aforementioned work. Afterwards, three others presented themselves to me, based on entirely different principles, one of which I delivered in the fifth Section. But all these demonstrations, even if they seem to leave nothing to be desired with regard to rigor, are derived from very heterogeneous principles, except perhaps the first, which nevertheless proceeded by more laborious reasoning, and was burdened by more extensive operations. Therefore, I have no doubt that until now a genuine demonstration has not been given; let it now be up to the experts to judge whether that which has lately been successfully discovered, and which the following pages present, deserves to be decorated with this name.

Art. 3

Theorem. *Let p be an odd positive prime number, and let k be any integer which is not divisible by p. Let A be the complex of numbers*

$$1, 2, 3, \ldots, \tfrac{1}{2}(p-1)$$

and let B be the complex

$$\tfrac{1}{2}(p+1), \tfrac{1}{2}(p+3), \ldots, p-1.$$

Let us consider the minimal positive residues modulo p of the product of k with each of the numbers in A. These will obviously all be different, and will belong partly to A and partly to B. If it is now assumed that, among the resulting residues, μ of them belong to B, then k will be either a quadratic residue or non-residue according as μ is even or odd.

Proof. Let the residues belonging to A be a, a', a'', ..., and let the rest belonging to B be b, b', b'', ... It is clear that the complements of the latter, $p-b$, $p-b'$, $p-b''$, ... are all distinct from the numbers a, a', a'', ..., and that, taken together, these complete the complex A. Thus we have

$$1.2.3\ldots\tfrac{1}{2}(p-1) = aa'a''\ldots(p-b)(p-b')(p-b'')\ldots,$$

and this product clearly becomes

$$\begin{aligned}&\equiv(-1)^{\mu}aa'a''\ldots bb'b''\cdots\equiv(-1)^{\mu}k.2k.3k\ldots\tfrac{1}{2}(p-1)k\\&\equiv(-1)^{\mu}k^{\frac{1}{2}(p-1)}1.2.3\ldots\tfrac{1}{2}(p-1)\pmod{p}\end{aligned}$$

It follows that

$$1\equiv(-1)^{\mu}k^{\frac{1}{2}(p-1)}$$

or equivalently $k^{\frac{1}{2}(p-1)}\equiv\pm1$, according as μ is even or odd, from which our theorem immediately follows. □

Art. 4

The following considerations will be greatly shortened by the introduction of certain notation. We therefore denote by the symbol (k,p) the multitude of products from

$$k, 2k, 3k, \ldots, (p-1)k$$

whose minimal positive residues exceed half of the modulus p. Moreover, for any non-integral quantity x, we will denote by the symbol $[x]$ the integer which is just smaller than x, so that $x-[x]$ is always a positive quantity between 0 and 1. It is easy to verify the following relations:

I. $[x]+[-x]=-1$

II. $[x]+h=[x+h]$, whenever h is an integer.

III. $[x]+[h-x]=h-1$

IV. If $x-[x]$ is a fraction less than $\frac{1}{2}$, then $[2x]-2[x]=0$; if it is greater than $\frac{1}{2}$ then $[2x]-2[x]=1$.

V. If the minimum positive residue of an integer h modulo p is less than $\frac{1}{2}p$, then $\left[\frac{2h}{p}\right]-2\left[\frac{h}{p}\right]=0$; if it is greater than $\frac{1}{2}p$, then $\left[\frac{2h}{p}\right]-2\left[\frac{h}{p}\right]=1$.

VI. From this it immediately follows that

$$\begin{aligned}(k,p)=&\left[\frac{2k}{p}\right]+\left[\frac{4k}{p}\right]+\left[\frac{6k}{p}\right]+\cdots+\left[\frac{(p-1)k}{p}\right]\\&-2\left[\frac{k}{p}\right]-2\left[\frac{2k}{p}\right]-2\left[\frac{3k}{p}\right]-\cdots-2\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\end{aligned}$$

VII. From VI. and I. one easily derives

$$(k,p)+(-k,p)=\tfrac{1}{2}(p-1)$$

Hence it follows that $-k$ either has the same or opposite relation to p (insofar as it is a quadratic residue or non-residue) as does $+k$, according as p is either of the form $4n+1$ or of the form $4n+3$. In the former case it is obvious that -1 will be a quadratic residue, and in the latter case it will be a quadratic non-residue modulo p.

VIII. We now transform the formula given in VI., in the following way. By III. we have

$$\left[\frac{(p-1)k}{p}\right] = k-1-\left[\frac{k}{p}\right], \left[\frac{(p-3)k}{p}\right] = k-1-\left[\frac{3k}{p}\right], \left[\frac{(p-5)k}{p}\right] = k-1-\left[\frac{5k}{p}\right], \ldots$$

Applying these substitutions to the last $\frac{p\mp 1}{4}$ members of the above expression, we will have

first, whenever p is of the form $4n+1$,

$$\begin{aligned}(k,p) =& \tfrac{1}{4}(k-1)(p-1)\\ &-2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-3)k}{p}\right]\right\}\\ &-\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{4k}{p}\right]-\cdots-\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}\end{aligned}$$

second, whenever p is of the form $4n+3$,

$$\begin{aligned}(k,p) =& \tfrac{1}{4}(k-1)(p+1)\\ &-2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}\\ &-\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{4k}{p}\right]-\cdots-\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}\end{aligned}$$

IX. For the special case $k=2$ it follows from the formulas just given that $(2,p)=\frac{1}{4}(p\mp 1)$, where the sign is taken to be plus or minus according as p is of the form $4n+1$ or $4n+3$. Therefore, $(2,p)$ will be even, and therefore $2Rp$, whenever p is of the form $8n+1$ or $8n+7$; on the other hand $(2,p)$ will be odd and $2Np$ whenever p is of the form $8n+3$ or $8n+5$.

Theorem. *Let x be a positive, non-integer quantity, such that among the multiples x, $2x$, $3x$, ... up to nx, no integer can be found. Setting $[nx]=h$, it is easily concluded that likewise among the reciprocal quantities $\frac{1}{x}$, $\frac{2}{x}$, $\frac{3}{x}$, ... up to $\frac{h}{x}$ no integer can be found. Then I claim*

$$\left.\begin{aligned}&[x]+[2x]+[3x]+\cdots+[nx]\\ &+\left[\tfrac{1}{x}\right]+\left[\tfrac{2}{x}\right]+\left[\tfrac{3}{x}\right]+\cdots+\left[\tfrac{h}{x}\right]\end{aligned}\right\} = nh.$$

Proof. For the series $[x]+[2x]+[3x]+\cdots+[nx]$, which we will set $=\Omega$, the first members up to the $\left[\frac{1}{x}\right]^{th}$ inclusive will obviously all be $=0$; the following up to the $\left[\frac{2}{x}\right]$ will be $=1$, all up to the $[\frac{3}{x}]^{th}$ will be $=2$ and so on. Hence

$$\left.\begin{aligned}\Omega = \quad & 0\times\left[\tfrac{1}{x}\right]\\ &+1\times\left\{\left[\tfrac{2}{x}\right]-\left[\tfrac{1}{x}\right]\right\}\\ &+2\times\left\{\left[\tfrac{3}{x}\right]-\left[\tfrac{2}{x}\right]\right\}\\ &+3\times\left\{\left[\tfrac{4}{x}\right]-\left[\tfrac{3}{x}\right]\right\}\\ &\textit{etc.}\\ &+(h-1)\times\left\{\left[\tfrac{h}{x}\right]-\left[\tfrac{h-1}{x}\right]\right\}\\ &+h\times\left\{n-\left[\tfrac{h}{x}\right]\right\}\end{aligned}\right\} = hn-\left[\frac{1}{x}\right]-\left[\frac{2}{x}\right]-\left[\frac{3}{x}\right]\cdots-\left[\frac{h}{x}\right]$$

□

Theorem. *Let k, p be positive odd numbers which are relatively prime to each other. Then*

$$\left.\begin{aligned}&\left[\tfrac{k}{p}\right]+\left[\tfrac{2k}{p}\right]+\left[\tfrac{3k}{p}\right]+\cdots+\left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\\ &+\left[\tfrac{p}{k}\right]+\left[\tfrac{2p}{k}\right]+\left[\tfrac{3p}{k}\right]\cdots+\left[\tfrac{\frac{1}{2}(k-1)p}{k}\right]\end{aligned}\right\} = \tfrac{1}{4}(k-1)(p-1)$$

Proof. Suppose, which is allowed, that $k < p$. Then $\frac{\frac{1}{2}(p-1)k}{p}$ will be less than $\frac{1}{2}k$, and greater than $\frac{1}{2}(k-1)$, and therefore $\left[\frac{\frac{1}{2}(p-1)k}{p}\right] = \frac{1}{2}(k-1)$. From this it is clear that the present theorem follows directly from the one above, if we take $\frac{k}{p} = x$, $\frac{1}{2}(p-1) = n$, and therefore $\frac{1}{2}(k-1) = h$. □

It can be shown in a similar way that if k is an *even* number relatively prime to p, that

$$\left.\begin{array}{l}\left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-1)k}{p}\right] \\ + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] \cdots + \left[\frac{\frac{1}{2}kp}{k}\right]\end{array}\right\} = \frac{1}{4}k(p-1)$$

But we do not dwell on this proposition, which is not necessary for our purposes.

Art. 7

The fundamental theorem now follows immediately from the combination of the preceding theorem with proposition VIII of Art. 4, 9. Namely, let k, p be two distinct positive primes, and set

$$(k,p) + \left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-1)k}{p}\right] = L$$

$$(p,k) + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] \cdots + \left[\frac{\frac{1}{2}(k-1)p}{k}\right] = M.$$

Then by VIII. Art. 4 it is clear that L and M are always even numbers. But by the theorem of Art. 6 one has

$$L + M = (k,p) + (p,k) + \tfrac{1}{4}(k-1)(p-1)$$

Therefore, every time $\frac{1}{4}(k-1)(p-1)$ turns out to be even, which happens if either k or p is of the form $4n+1$, necessarily (k,p) and (p,k) are both even or both odd. And whenever $\frac{1}{4}(k-1)(p-1)$ is odd, which happens if both k and p are of the form $4n+3$, then necessarily one of the numbers (k,p) and (p,k) is even and the other is odd. In the former case, then, the relation of k and p and the relation of p and k (insofar as one is a quadratic residue or non-residue of the other) will be identical. In the latter case, they are opposite.

Q. E. D.