SOLUTION OF THE ARITHMETICAL PROBLEM CONCERNED WITH FINDING THE NUMBER WHICH DIVIDED BY A KNOWN NUMBER SHALL LEAVE A GIVEN REMAINDER

E 36 : Commentarii academiae scientiarum Petropolitanae 7 (1734/5), 1740, p. 46-66

1. In common arithmetic books there are found problems of this kind here and there, for which more study and skill is required to be resolved fully than indeed may be considered necessary, with the aid of which a solution may be able to be obtained, but that yet either is insufficient and agrees only with the proposed case so that with the circumstances of the case changed a little it shall be of no further use, or usually instead at once it may be found to be false. Thus the construction of magic squares has been treated previously by arithmetic; but which since that may be insufficient, it has required the greater ingenuity Lahire and Sauveur for being perfected. Also in a similar manner that same problem occurs almost everywhere, in order that a number may be found, which may be divided by 2, 3, 4, 5 and 6 and may leave one as the remainder, indeed it may be able to be divided by 7 without a remainder. Truly a suitable method for solving a problem of this kind has never been shown ; indeed the solution added there agrees in this case and is resolved by being required to be tested further.

2. Indeed if the numbers are small, by which the number sought must be divided, just as in this example, on being tested the number sought can be found without difficulty ; but a solution of this kind may become a little difficult, if the divisors proposed shall be extremely large. And thus since even now no true method may be had, required for solving problems of this kind, which may be applied equally both for large and small divisors, I am confidant my arrangement to be a useful work, while I have investigated a method of this kind, from which without a trial it may be extended to the largest also, so that such problems may be able to be resolved from the division.

3. Therefore so that I may set out distinctly what I have considered here about this matter, I shall begin from the simplest case, from which only as single divisor of some number may be sought, and the number may be sought, which by that division will leave the given remainder. Clearly the number z may be sought, which divided by the number a may leave p for the residue. Certainly the solution of this question is the most easy; indeed there shall be $z = ma + p$, with m denoting some whole number ; yet meanwhile it is agreed to be observed that this solution to be universal and all the satisfying numbers to be included. Besides it is understood from this also, if one satisfying number may be had, from that innumerable other satisfying numbers also can be found, while that number either may be increased by some multiple of a itself, or may be diminished, if it can be done. Moreover p or $0a + p$ will be the minimum satisfying number, this is followed by $a + p$, which again is followed by $2a + p,\ 3a + p,\ 4a + p$ etc., numbers which constitute an arithmetical progression having the constant difference a.

4. With this established the case follows, where two divisors with their remainders are proposed, which is a special case, and all the following is included in it. For whatever divisors will have been proposed, the question always can be reduced to this case, where only two divisors are proposed, just as I will show in the following. Therefore it shall be required to search for a number *z*, which divided by *a* may leave the remainder *p*, truly divided by *b* may leave the remainder *q*, and the number *a* shall be greater than the number *b*. Therefore since the number sought *z* must be able to be compared thus, so that on division by *a* there may remain *p*, by necessity it will be contained in this form $ma + p$ and therefore $z = ma + p$. Then from the other condition, where *z* divided by *b* it must leave the remainder *q*, there will become $z = nb + q$. On account of which, since there shall become $ma + p = nb + q$, whole numbers are required to be substituted in place of *m* and *n*, so that $ma + p = nb + q$; from which it will be found that $ma + p$ or $nb + q$, to be the number sought *z*.

5. Therefore since there is $ma + p = nb + q$, there will be $n = \frac{ma+p-q}{b}$, or on putting $p - q = v$ there will become $n = \frac{ma+v}{b}$. On this account it will be required to define the number *m*, so that $ma + v$ shall be able to be divided by *b* without a remainder. Since we have defined $a > b$ above, there may be put $a = \alpha b + c$; there will become $n = m\alpha + \frac{mc+v}{b}$; it will be required therefore, that $mc + v$ may be allowed to be divided by b ; but α and *c* are known numbers, which are found from the division of *a* by *b*; indeed α is the quotient and *c* the remainder. Again there may be put $\frac{mc+v}{b} = A$; there will become $m = \frac{Ab-v}{c}$; whereby the number *A* will be required to be found, so that $Ab - v$ may be able to be divided by *c*. If it may eventuate, that *v* may be divisible by *c*, the operation now will be able to be finished; for on taking $A = 0$ there will become $m = -\frac{v}{c}$ and $z = -\frac{\alpha v}{c} + p$, which expression, even if it may emerge negative, is yet suitable for finding infinitely many positive numbers for *z*.

6. But if v cannot be divided by *c*, so that $\frac{Ab-v}{c}$ may become as whole number, I put $b = \beta c + d$ or, b divided by *c*, and I call the quotient $= \beta$ and the remainder $= d$. With which done there will be $\frac{Ab-v}{c} = A\beta + \frac{Ad-v}{c} = m$ and $\frac{Ab-v}{c}$ must become a whole number; this shall be $= B$; there will become $A = \frac{Bc+v}{d}$. Now if v can be divided by *d*, I make $B = 0$, and there will become $A = \frac{v}{d}$, and $m = \frac{\beta v}{d}$.

But if *v* is not divisible by *d*, again I put $c = \gamma d + e$ and there will become $A = B\gamma + \frac{Be+v}{d}$. And I put $\frac{Be+v}{d} = C$, so that there shall become $B = \frac{Cd-v}{e}$. Now if *v* will be able to be divided by *e*, I put $C = 0$ and there will become $B = -\frac{v}{e}$, $A = -\frac{\gamma v}{e}$ and $m = -\frac{\beta\gamma v}{e} - \frac{v}{c}$.

But if at no time were $\frac{v}{e}$ a whole number, I put $d = \delta e + f$ and there will become $B = C\delta + \frac{Cf - v}{e}$; and I make $\frac{Cf - v}{e} = D$, so that there shall become $C = \frac{De + v}{f}$, where it is required to be seen, whether *v* may be divided by *f* or otherwise, and in each case so that the above operation may be put in place.

7. Moreover, since $a > b$, $b > c$ and $c > d$ etc., this series *a, b, c, d, e, f* etc. on being continued will always arrive at smaller numbers, thus so that finally it ought to arrive at so small a number, that shall be some part of, or a divisor of *v*. But *c, d, e, f* etc. are the continued remainders of the ordinary operation, by which the greatest common divisor of *a* and *b* themselves is accustomed to be found, which operation I may put in place here :

$n = \frac{ma+v}{b}$	b	a	α								$a = \alpha b + c$
$m = \frac{Ab-v}{c}$		c	b	β							$b = \beta c + d$
$A = \frac{Bc+v}{d}$			d	c	γ						$c = \gamma d + e$
$B = \frac{Cd-v}{e}$				e	d	δ					$d = \delta e + f$
$C = \frac{De+v}{f}$					f	e	ε				$e = \varepsilon f + g$
$D = \frac{Ef-v}{g}$						g	f	ζ			$f = \zeta g + h$
$E = \frac{Fg+v}{h}$							h	g	η		$g = \eta h + i$
$F = \frac{Gh-v}{i}$								i	h	θ	$h = \theta i + k$
$G = \frac{Hi+v}{k}$									k		

8. Therefore this operation, which we are accustomed to use for the greatest common divisor of the numbers *a* and *b,* is required to be continued to that point, until it may arrive at a remainder, which may divide *v*. With which found, we may investigate the number *m* in the following manner. If *v* now may be divided by *b*, there will become $m = 0$. If *v* may allow division by *c*, there will become $A = 0$ and $m = \frac{-v}{c}$. If *v* may be divided by *d* , there will become $B = 0$, $A = \frac{v}{d}$ and $m = \frac{bv}{cd} - \frac{v}{c} = \frac{bv}{d}$, on account of $b = \beta c + d$. But where the values of *m* may be found easier, the first value of *A* by *B,* and then the value of *B* thus again must be expressed by *C,* from which this table arises :

1. $m = \frac{Ab-v}{c}$,
2. $m = \frac{Bb+\beta v}{d}$,
3. $m = \frac{Cb-v(1+\beta\gamma)}{e}$,
4. $m = \frac{Db+v(\delta+\beta\gamma\delta+\beta)}{f}$,
5. $m = \frac{Eb-v(\delta\varepsilon+\beta\gamma\delta\varepsilon+\beta\varepsilon+\beta\gamma+1)}{g}$,
6. $m = \frac{Fb+v(\delta\varepsilon\zeta+\beta\gamma\delta\varepsilon\zeta+\beta\varepsilon\zeta+\beta\gamma\zeta+\zeta+\delta+\beta\gamma\delta+\beta)}{h}$,

etc.

With regard to these values it is required to note the signs of v to alternate in this manner $-+-+-+$ etc.
From which, the coefficients of v maintain this rule:

β	γ	δ	ε	ζ	
1,	$\beta\beta$,	$\beta\gamma+1$,	$\beta\gamma\delta+\delta+\beta$,	$\beta\gamma\delta\varepsilon+\beta\varepsilon+\delta\varepsilon+\beta\gamma+1$	etc.,

and for which the term of each progression is the sum of the preceding term multiplied by the index itself written above and with the term preceding this.

9. Therefore if v will be able to be divided by b, there will become $m = 0$; if v can be divided by c, there will become $m = \frac{-v}{c}$ on account of $A = 0$; if v will be divided by d, there shall become $B = 0$ and there will become $m = \frac{v}{d}\beta$. From which the following rule emerges:

If the following number is whole:	there will become
$\frac{v}{b}$	$m = 0$
$\frac{v}{c}$	$m = -\frac{v}{c}$
$\frac{v}{d}$	$m = +\frac{v}{d}\beta$
$\frac{v}{e}$	$m = -\frac{v}{e}(\beta\gamma+1)$
$\frac{v}{f}$	$m = +\frac{v}{f}(\beta\gamma\delta+\delta+\beta)$
$\frac{v}{g}$	$m = -\frac{v}{g}(\beta\gamma\delta\varepsilon+\delta\varepsilon+\beta\varepsilon+\beta\gamma+1)$
$\frac{v}{h}$	$m = +\frac{v}{h}(\beta\gamma\delta\varepsilon\zeta+\delta\varepsilon\zeta+\beta\varepsilon\zeta+\beta\gamma\zeta+\beta\gamma\delta+\zeta+\delta+\beta)$

etc.

If now these values of m may be substituted into the equation $z = ma + p$, there will be found as follows:

If the following number is whole:	there will become
$\frac{v}{b}$	$z = q + \frac{bv}{b}1 = q + v$
$\frac{v}{c}$	$z = q - \frac{bv}{c}\alpha$
$\frac{v}{d}$	$z = q + \frac{bv}{d}(\alpha\beta + 1)$
$\frac{v}{e}$	$z = q - \frac{bv}{e}(\alpha\beta\gamma + \alpha + \gamma)$
$\frac{v}{f}$	$z = q + \frac{bv}{f}(\alpha\beta\gamma\delta + \alpha\beta + \alpha\delta + \gamma\delta + 1)$
$\frac{v}{g}$	$z = q - \frac{bv}{g}(\alpha\beta\gamma\delta\varepsilon + \alpha\beta\varepsilon + \alpha\delta\varepsilon + \gamma\delta\varepsilon + \alpha + \gamma + \varepsilon)$
	etc.

10. Therefore in order to find the number *z,* which divided by *a* may leave the remainder *p* and which divided by *b* may leave the remainder q, on putting $p - q = v$, we will have the following rule:

The procedure may be put in place for finding the greatest common divisor between *a* and *b* as far as that may be produced, until it may arrive at a remainder, which shall be a divisor of *v,* and the quotient resulting from the division of *v* by that remainder, which shall be *Q,* [*i.e.* $Q = \frac{p-q}{final\ remainder}$], where the procedure may be interrupted. From which the quotients in the series arising from this division may be written α, β, γ etc. and from these the series may be constructed

$$1,\ \alpha,\ \alpha\beta + 1,\ \alpha\beta\gamma + \alpha + \gamma \text{ etc.},$$

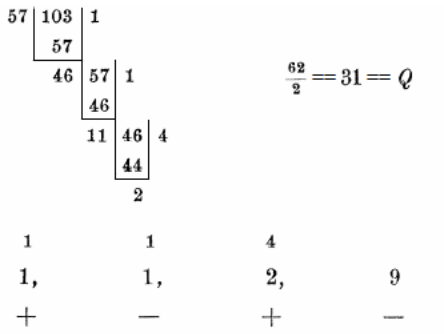
which from that a series of quotients may be formed and must be continued to that point, so that a series can be composed. The alternating signs $+ - + -$ etc. must be written under this new series as far as the final term with its sign multiplied by *Q* and also by its smaller divisor proposed *b;* to the product the remainder *q* may be added corresponding to the divisor *b*. With which accomplished the sum will be the number sought.

11. From this one satisfying number *z* found in this manner, at once innumerable other satisfying numbers will be found. For if *z* divided by *a* leaves the remainder *p* and divided by *b* leaves q, some numbers having that same property will be had $ab + z$, $2ab + z$ and $mab + z$. Indeed a multiple of the product *ab* may be able to be continually added or taken away, if a and b were relatively prime numbers ; but if *a* and *b* were composite numbers, then also it will suffice to have taken the smallest common divisor of these, of which some multiple either added or taken from *z* will give satisfying numbers; so that if the smallest common divisor were *M,* it will be understood that $mM + z$ will give all the satisfying numbers sought entirely. Whereby even if in this

manner often negative numbers may be found for z , yet by adding M to these or some multiple of this positive numbers will be obtained. Therefore by this operation the smallest satisfying number will always be found, if indeed the smallest common divisor M may be subtracted, as many times as it can be able to do so.

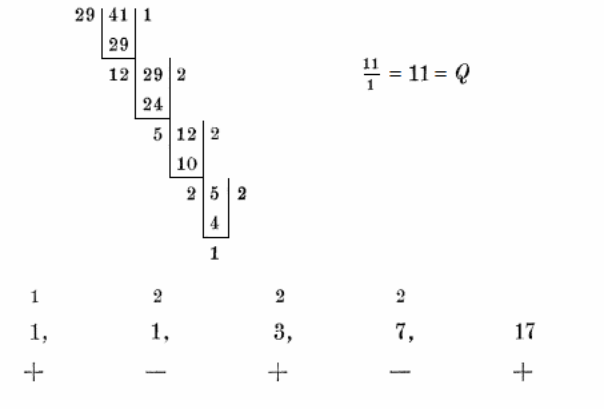
12. Since this operation will be illustrated best by examples, we may enquire about the number which divided by 103 may leave the remainder 87 and divided by 57 may leave 25. Therefore there will be

$a=103,\ b=57,\ p=87\ ;\ q=25$ and $v=62$; whereby the operation thus may be put in place :



Now there becomes $-9\cdot 31=-279$ and the number sought $25-57\cdot 279$; which since it shall be negative, by adding to that $3\cdot 57\cdot 103$ or $57\cdot 309$, from which there is found $25\cdot 57\cdot 30=1735$, which is the minimum number sought; indeed all the satisfying numbers are contained in this form $m\cdot 103\cdot 57+1735$.

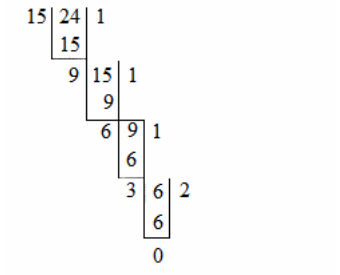
13. Again we may seek the number, which divided by 41 may leave the remainder 10, and divided by 29 may leave the remainder 28. In this example I will use a shorthand method, which will have a great use in all similar computations; for since in the division by 29 the remainder shall be 28, also in the same division -1 will be able to remain, if some quotient greater than unity may be taken. Therefore I take -1 for the remainder of the division by 29 and there will become $a=41,\ b=29,\ p=10$ and $q=-1,$ from which there will become $v=11$. Thus with the procedure put in place as before :



Therefore there will become $+17\cdot 11 = 187$ and the number sought $= -1+29\cdot 187$. $29\cdot 4\cdot 41$ may be subtracted; this will become $= -1+29\cdot 23 = 666$. Therefore all the numbers present in this form $m\cdot 41\cdot 29+666$ will satisfy the question.

14. Hence the shortcut produced will itself be required to be added to the rule given above, so that it may be in agreement with this, after the number Q $[= \frac{p-q}{\textit{final remainder}}]$ is multiplied by the final term of the series formed, the product may be divided by the greater divisor a and the remainder if this product may be used in place of this. Clearly this remainder multiplied by the smaller divisor b and with the remainder q increased will give the number sought. And this same number found with this agreed on will be the smallest which it satisfies. Besides by this division it can be effected, so that it may produce a positive remainder, even if the dividend were negative. Thus in the first example § 12 there will be had $[-9\cdot 31 =]\ -279$, which number divided by 103 with the quotient taken $= 3$ will leave +30. From which the smallest number sought $= 25+57\cdot 30 = 1735$.

15. Thereupon it can also be done, so that examples of this kind may be proposed, which may not allow any solution, as if a number may be sought, which divided by 24 may leave the remainder 13, and divided by 15 may leave the remainder 9; for such a number by this other condition must also be divisible by 3, in accordance with the other rule. Truly this will be shown by this same rule; for at no time will such remainder other than 0 arise, since it shall divide v or 4, as is to be seen from this operation:



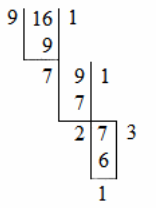
Truly examples of this kind cannot be shown, unless the divisors *a* and *b* shall be composite between themselves ; for if they were relatively prime, the numbers sought always will be able to be shown . But if the divisors *a* and *b* were composite numbers and *v* will not have been able to be divided by the maximum divisor of *a* and *b* themselves, then the problem always will be reduced to being absurd. And this is the criterion, from which it can be judged, whether or not a problem may allow a solution, before the operation may be put into place.

16. With this method set out generally, by which all the problems of this kind can be resolved easily, from these another rule can be formed, which indeed is not so easy to use, but is had more simply. Moreover this arises, if in the above values of *z* found (§ 9) in place of $\alpha,\ \beta,\ \gamma$ etc. the values of these from the equations $a = \alpha b + c,\ b = \beta c + d$ etc. may be substituted. For if the operation for the greatest common divisor between *a* and *b* requiring to be found, and from that the continued remainders *c*, *d*, *e* etc. may become known, I say the number *z* to become :

$$z = q + abv\left(\frac{1}{ab} - \frac{1}{bc} + \frac{1}{cd} - \frac{1}{de} + \frac{1}{ef} - \text{etc.}\right)$$

and that this series by being continued as far, until *v* may be able to be divided by some factor of the denominator.

As if the number may be sought, which shall leave the remainder 1 on division by 16 and may leave 7 on division by 9, there will become $a = 16,\ b = 9,\ p = 1,\ q = 7$ and $v = -6$. Whereby :



Hence therefore there will become

$$z = 7 - 6\cdot 9\cdot 16\left(\frac{1}{16\cdot 9} - \frac{1}{9\cdot 7} + \frac{1}{7\cdot 2}\right) = 7 - 6 + \frac{6\cdot 16}{7} - \frac{3\cdot 9\cdot 16}{7} = 1 - 3\cdot 16 = -47.$$

Therefore all the numbers are satisfactory $m\cdot 144 - 47$ or $m\cdot 144 + 97$ and the smallest of these is 97.

The above general formula of *z* also can be expressed in this manner

$$z = p - abv\left(\frac{1}{bc} - \frac{1}{cd} + \frac{1}{de} - \frac{1}{ef} + \text{etc.}\right),$$

which series of fractions must be continued to that extent, until the value of *z* may become a whole number.

17. Now I will consider certain particular cases, in which *a* may have a given relation to *b* ; and initially indeed there shall be $b = a - 1$ or $a = b + 1$, truly the remainders sought from the division of the number sought by *a* and *b* shall come about as before as *p* and *q*. Therefore there will be $c = 1$ [*i.e.* from $a = \alpha b + c$] and thus by the last rule:

$$z = p - av = ap + aq.$$

Which expression, if $aq + p > ap$, gives the minimum satisfying number sought ; but if $aq + p < ap$, then the minimum satisfying number will be $a^2 - a + p - ap + aq$. Truly all the satisfying numbers are held in this general formula $ma^2 - ma + p - ap + aq$, or also in this $mb^2 + mb - bp + bq + q$. However much m shall be now, if this quantity may be divided by $b^2 + b$, the remainder will be the smallest satisfying number sought.

18. Just as by this account with the help of the given remainders, which remain after the division of the unknown number by the divisors *b* and $b + 1$, from which the unknown number shall be known, Stifel has shown in his *Commentary on the Cossic art of Rudolf* , the rule of this is itself found thus: If the remainder of an unknown number divided by $b + 1$ were *p* and the remainder of the same number divided by *b* were *q*, the sum of these factors *q* multiplied by *b* + 1 and *p* by b^2 is ordered to be divided by $b^2 + b$; what may result after the division may be said to be the number sought. Moreover this rule flows from our general formula, if there may be put $m = p$; for then there will be had $b^2 p + (b + 1)q$, which divided by $b^2 + b$ will leave the minimum number sought.
[For $mb^2 + mb - bp + bq + q$ becomes $pb^2 + pb - bp + bq + q = pb^2 + q(b + 1)$.]

19. Yet meanwhile the satisfying number may be found in the following manner with less work: The remainder *q*, which arises from the division of the number sought by *b*, will be multiplied by $b + 1$ and the product made from *b* by the adjoining number may be added, considered as $b^2 + b$, hence the product may be subtracted from the remainder *p*, which remains from the division of the number sought by $b + 1$, times by *b;* if that which remains, were $< b^2 + b$, that itself will be the number sought, but if truly it were $> b^2 + b$, $b^2 + b$ may be subtracted and the remainder will be the number sought. So that if the number may be sought, which divided by 100 may leave 75 and divided by 101 may leave 37 ; then 10100 may be added to the product from 75 by 101 or 7575 , so that there may be had 17675, hence the product from 37 by 100 or 3700 may be subtracted ; 13975 will remain ; from which if 10100 may be taken away, 3875 will be produced, which is the minimum number sought.
[Here $b = 100$ & $q = 75$, while $b + 1 = 101$ & $p = 37$, hence $b^2 p + (b + 1)q$ with $b^2 + b$ taken away becomes
$b(b + 1) + (b + 1)q - pb - b(b + 1) = (b + 1)q - pb = 7575 - 3700 = 3875.$

Here $b^2 p+(b+1)q = 370000+7575 = 377575$ divided by $b^2+b = 10100$]

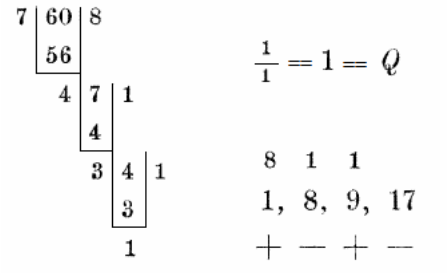
20. If the number may be sought, which divided by *b* shall leave *q* and *p* divided by $nb+1$, again there will be $c = 1$ and the number sought

$$z = p - av = p - ap + aq = (nb+1)q - nbp \text{ , on account of } a = nb+1 .$$

And all the satisfying numbers will be contained in this expression $mnb^2 + mb+(nb+1)q - nbp$, from which with some minimum satisfying number found for *m*, if this expression may be divided by nb^2+b ; indeed the remainder will be the minimum satisfying number.

21. Again the case is noteworthy, where the remainders p and *q*, which arise from the division of the number sought by the given divisors *a* and *b*, are equal to each other, or $p = q$. For in this case there becomes $v = 0$ and thus the number sought $z = p$. Therefore if *M* shall be the smallest common divisor of the numbers *a* and *b*, all the satisfying numbers will be contained in this formula $mM + p$. Clearly also it will satisfy the same formula, if however many divisors there were *a*, *b*, *c*, *d* etc., by which an individual number sought divided may leave the remainder p, if indeed *M* may denote the least common divisor of all the divisors. Therefore all the numbers of this kind satisfying the questions thus have been prepared, so that on division by *M* shall leave the remainder p.

22. Hence the well-tried problem can be solved, where the number is sought, which divided by 2, 3,4, 5, 6 shall leave the remainder 1, but truly by 7 shall leave nothing. For all the numbers, which divided by 2, 3, 4, 5, 6 will leave the remainder 1, have this property, just as divided by 60, which number is the least common divisor of the numbers 2, 3, 4, 5 and 6, to be divided will leave the remainder 1. Therefore the problem is reduced to this, so that we may find a number which divided by 60 shall leave the remainder 1, but shall be divisible by 7 ; therefore there will become $a = 60,\ b = 7,\ p = 1,\ q = 0$ and $v = 1$. Therefore with the procedure put in place



there will become $z = 0-119+420m$, and if $m = 1$, there will become $z = 301$.

23. A greater difficulty is seen to be had with this problem, where the number is sought, which divided respectively by the numbers 2, 3, 4, 5, 6 shall leave the remainders 1, 2, 3,

4, 5, but shall be divisible by 7, on account of the proposed remainder inequality. But this question agrees with this one: to find the number, which divided by 2, 3, 4, 5, 6 may leave the remainder -1, and nothing on division by 7. Now for that condition to be satisfied by the form $60m-1$; whereby the number sought, which the division by 60 leaves -1, but shall leave nothing on division by 7 ; and there become $a=60,\ b=7,\ p=-1,\ q=0$ and $v=-1$ and by the procedure put in place before there is $Q=-1$, which multiplied into -17 gives +17; and this multiplied by *b* gives 119, the number sought.

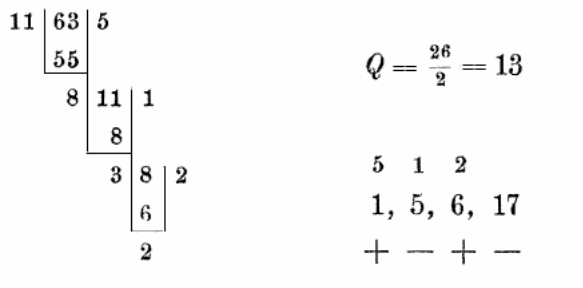
24. It is evident from these two examples, how questions of this kind, in which some number of divisors are proposed, but in which only two remainders correspond, may be able to be solved by the rules given above ; for at once the question is reduced to the question of division by two divisors ; as if all the remainders are equal, the question likewise is solved, as if a single divisor were proposed. But if the remainders are not equal, then likewise the solution will be obtained by repeating these operations, which we have used for two divisors. For initially it must be satisfied by two divisions, then the third is taken, then the fourth, then it will be satisfied by everything. This indeed we will explain most conveniently by examples.

25. Therefore we shall seek the number, which divided by 7 shall leave the number 6, and 7 shall be left on dividing by 9, 8 by 11 and 1 by 17. Now from these four conditions we may take any two, as the two first, and investigate all the numbers satisfied by these. Therefore there will be $a=9,\ b=7,\ p=7,\ q=6$ and $v=1$, whereby the procedure may be put in place, as follows:

7	9	1	$Q=1$
	7		
	2	7 | 3	1 3
		6	1, 1, 4
		1	+ − +

and there will become $z=6+1\cdot 4\cdot 7=34$.
Therefore all the numbers satisfying these two conditions will be contained in this formula $63m+34$ or thus will be able to be prepared, so that the may be divided by 63 with the remainder 34.

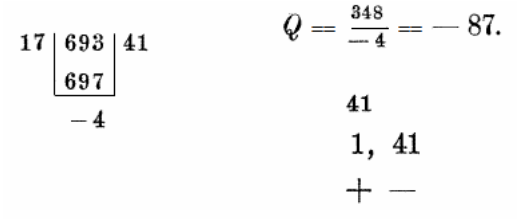
26. Therefore the problem is reduced to this, so that the number may be found, which divided by 63 may leave the remainder 34, by 11 it shall leave 8 and by 17 it shall leave 1. The first two of these three conditions may be taken, and there will become $a=63,\ b=11,\ p=34,\ q=8$ and $v=26,$ from which the following procedure arises:



therefore $z = m \cdot 63 \cdot 11 + 8 - 13 \cdot 17 \cdot 11$.

So that a minimum satisfying number may be found, there may be put $m = 4$; there will become $z = 8 + 31 \cdot 11 = 349$.
Therefore all the satisfying numbers will be contained in this form $693m + 349$ or hence they will have the property, that being divided by 693 they will leave the remainder 349.

27. Therefore the problem finally is reduced to this, so that the number may be defined, which divided by 693 may leave the remainder 349 and divided by 17 may leave the remainder 1. Therefore I make $a = 693$, $b = 17$, $p = 349$, $q = 1$ and $v = 348$ and I put in place the following given adjoining precepts :



$$z = 693 \cdot 17 \cdot m + 1 + 41 \cdot 87 \cdot 17.$$

So that the smallest satisfying number may be produced, I put $m = -5$ and there will become :

$$z = 1 + 102 \cdot 17 = 1735,$$

which is the smallest number satisfying the four prescribed conditions. Moreover everything, which shall be satisfactory, will be present in this formula $11781m + 1735$.
Therefore from this example it is abundantly clear, how all the questions of this kind shall be required to be resolved.

28. The solution of a well-known problem pertains to this, as from these rules found, I may establish approximately in what year the birth of Christ may have arisen from the given cycles of the sun and moon together with the imposition on that of the Roman year [*i.e.* finding the year of the event according to the Julian Calendar or previous]. Indeed since the solar cycle shall be the remainder, which arises from the number of years divided by 9 and increased by 28, truly the lunar cycle shall be the remainder, which arises from the division of the number of years by 1 and increased by 19, truly the Roman year shall be the remainder which arises, if the number of years may be divided by 15 and increased by 3, from which the following solution has emerged.

The solar cycle shall be *p*, the lunar cycle *q* and *r* the indicated Roman year; *p* is multiplied by 4845, *q* by 4200 and *r* by 6916, these three products may be combined with 3267 into one sum, and that may be divided by 7980; so that the remainder left is the number of the year sought. If the period in terms of the Julian year may be required, then the procedure may be established in the same way, except that the number 3267 must be ignored; which is the rule now generally treated.

$\left[\textit{solar cycle } \left(\textit{days in month} \right) : \frac{N}{9} + 28; \ \textit{lunar cycle} : \frac{N}{1} + 19; \ \textit{Julian calender} : \frac{N}{15} + 3; \right.$

$4845 \cdot \left(\frac{N}{9} + 28 \right) = 4200 \cdot \left(N + 19 \right) \therefore 538N + 135660 = 4200N + 79800$

$\left. \therefore 3662N \approx 55860 \quad \therefore N \approx 15 \text{ ; giving the date to be around the year } 3 \sim 4 \text{ in the Julian calender.} \right]$

29. Indeed the solution for several divisors will require much work to be reduced, if indeed the problem may be continued to the case, where the number of the divisions may be decreased by one, as we have done in the preceding example; but from that same operation a much easier and shorter way itself arises, from which at once the question proposed, also however many divisors there were, can be reduced to the case of two divisors ; which rule thus will itself be had:

The number is required to be found, which for the divisors *a, b, c, d, e,* which numbers I put to be relatively prime amongst themselves, the division may leave these numbers with respect to the remainders *p, q, r, s, t.* This number

$$Ap+Bq+Cr+Ds+Et+mabcde,$$

satisfies the equation in which expression *A* is the number, which divided by the product *bcde* may leave zero, truly division by *a* may leave unity ;
B is the number, which divided by *acde* may leave zero, truly by *b* unity;
C is the number, which divided by *abde* may leave zero, truly by *c* unity;
D is the number, which divided by *abce* may leave zero, truly by *d* unity; and
E is the number, which divided by *abcd* may leave zero, truly by *e* unity; therefore which numbers can be found for the two divisors given.

SOLUTIO PROBLEMATIS ARITHMETICI DE INVENIENDO NUMERO QUI PER DATOS NUMEROS DIVISUS RELINQUAT DATA RESIDUA

Commentatio 36 indicis ENESTROEMIANI

Commentarii academiae scientiarum Petropolitanae 7 (1734/5), 1740, p. 46-66

1. Reperiuntur in vulgaribus arithmeticorum libris passim huiusmodi problemata, ad quae perfecte resolvenda plus studii et sollertiae requiritur, quam quidem videatur. Quamvis enim plerumque regula sit adiecta, cuius ope solutio obtineri queat, tamen ea vel est insufficiens solique casui proposito convenit, ita ut circumstantiis quaestionis parum immutatis ea nullius amplius sit usus, vel subinde etiam solet esse falsa. Ita quadratorum magicorum constructio iam pridem ab arithmeticis est tradita; quae autem cum esset insufficiens, maiora ingenia LAHIRII et SAUWERII ad perficiendum requisivit. Simili quoque modo ubique fere occurrit istud problema, ut inveniatur numerus, qui per 2, 3, 4, 5 et 6 divisus relinquat unitatem, per 7 vero dividi queat sine residuo. Methodus vero idonea ad huiusmodi problemata solvenda nusquam exhibetur; solutio enim ibi adiecta in hunc tantum casum competit atque tentando potius absolvitur.

2. Si quidem numeri, per quos quaesitus numerus dividi debet, sunt parvi, prout in hoc exemplo, tentando non difficulter quaesitus numerus invenitur; difficillima autem foret istiusmodi solutio, si divisores propositi essent valde magni. Cum itaque ad huius generis problemata solvenda methodus etiamnum habeatur nulla genuina, quae ad magnos divisores aeque pateat ac ad parvos, non inutiliter operam meam collocatam esse confido, dum in huiusmodi methodum inquisivi, qua sine tentatione pro maximis etiam divisoribus talia problemata resolvi queant.

3. Quo igitur, quae hac de re sum meditatus, distincte exponam, a casu incipio simplicissimo, quo unicus tantum datur divisor numerusque quaeritur, qui per illum divisus datum relinquat residuum. Requiratur scilicet numerus z, qui per numerum a divisus relinquat p pro residuo. Huius quidem quaestionis solutio est facillima; erit enim $z = ma + p$, denotante m numerum quemcunque integrum; interim tamen observari convenit hanc solutionem esse universalem omnesque numeros satisfacientes complecti. Praeterea ex ea quoque intelligitur, si unus habeatur numerus satisfaciens, ex eo innumerabiles alios satisfacientes quoque posse inveniri, dum ille numerus quocunque

multiplo ipsius *a* vel augeatur vel, si fieri potest, minuatur. Erit autem *p* seu $0a+p$ minimus numerus satisfaciens, hunc excipit $a+p$, quem porro sequuntur $2a+p,\ 3a+p,\ 4a+p$ etc., qui numeri omnes constituunt progressionem arithmeticam differentiam constantem habentem *a.*

4. Hoc exposito sequitur casus, quo duo divisores cum suis residuis proponuntur, qui est praecipuus et sequentes omnes in se complectitur. Nam quotcunque propositi fuerint divisores, quaestio semper ad hunc casum, quo duo tantum proponuntur, reduci poterit, quemadmodum in sequentibus monstrabo. Quaeri igitur oporteat numerum *z,* qui per *a* divisus relinquat *p,* per *b* vero divisus relinquat *q,* sitque numerus *a* maior numero *b.* Cum ergo numerus quaesitus *z* ita debeat esse comparatus, ut per *a* divisus relinquat *p,* necessaria in hac forma $ma+p$ continebitur eritque idcirco $z=ma+p$. Deinde ex altera conditione, qua *z* per *b* divisus relinquere debeat *q,* erit $z=nb+q$. Quamobrem, cum sit $ma+p=nb+q$, determinari debebunt numeri integri loco *m* et *n* substituendi, ut sit $ma+p=nb+q$ *;* quibus inventis erit $ma+p$ seu $nb+q$ numerus quaesitus *z.*

5. Quia ergo est $ma+p=nb+q$, erit $n=\frac{ma+p-q}{b}$ seu posito $p-q=v$ erit $n=\frac{ma+v}{b}$. Hanc ob rem definiri oportet numerum *m,* ut $ma+v$ divide possit sine residuo per *b.* Quia est $a>b$, ponatur $a=\alpha b+c$ *;* erit $n=m\alpha+\frac{mc+v}{b}$; oportet ergo, ut $mc+v$ divisionem per *b* admittat; sunt autem α et *c* numeri cogniti, qui reperiuntur ex divisione ipsius *a* per *b*; erit enim α quotus et *c* residium. Ponatur porro $\frac{mc+v}{b}=A$; erit $m=\frac{Ab-v}{c}$; quare numerum *A* inveniri oportet, ut $Ab-v$ dividi queat per *c.* Si eveniat, ut *v* per *c* dividi possit, operatio iam poterit finiri; sumto enim $A=0$ erit $m=-\frac{v}{c}$ et $z=-\frac{\alpha v}{c}+p$, quae expressio, etiamsi evadat negativa, tamen ad infinitos numeros affirmativos pro *z* inveniendos est idonea.

6. Sin autem *v* per *c* non potest dividi, quo $\frac{Ab-v}{c}$ fiat numerus integer, pono $b=\beta c+d$ seu divido *b* per *c* dicoque quotum β et residuum $=d$. Quo facto erit $\frac{Ab-v}{c}=A\beta+\frac{Ad-v}{c}=m$ debebetque $\frac{Ab-v}{c}$ esse numerus integer; sit is $=B$ *;* fiet $A=\frac{Bc+v}{d}$. Si nunc *v* per *d* dividi poterit, facio $B=0$,eritque $A=\frac{v}{d}$, et $m=\frac{\beta v}{d}$.

Sin autem *v* per *d* non est divisibile, pono porro $c=\gamma d+e$ eritque $A=B\gamma+\frac{Be+v}{d}$. Atque pono $\frac{Be+v}{d}=C$, ut sit $B=\frac{Cd-v}{e}$. Si nunc *v* per *e* dividi poterit, pono $C=0$ eritque $B=-\frac{v}{e}$ et $A=-\frac{\gamma v}{e}$ atque $m=-\frac{\beta\gamma v}{e}-\frac{v}{c}$.

Sin $\frac{v}{e}$; nondum fuerit integer numerus, pono $d=\delta e+f$ eritque $B=C\delta+\frac{Cf-v}{e}$; atque facio $\frac{Cf-v}{e}=D$, ut sit $C=\frac{De+v}{f}$, ubi videndum est, utrum *v* per *f* dividi possit an secus, atque in utroque casu ut supra operatio debet institui.

7. Quia autem $a > b$ atque $b > c$ et $c > d$ etc., hac serie *a, b, c, d, e, f* etc. continuanda perpetuo ad minores numeros devenitur, ita ut tandem ad tam parvum perveniri oporteat, qui sit pars aliquota seu divisor ipsius *v.* Sunt autem *c, d, e, f* etc. continua residua ordinariae operationis, qua maximus communis divisor ipsorum *a* et *b* investigari solet, quam operationem hic appono:

$n = \frac{ma+v}{b}$	b	a	α							$a = \alpha b + c$
$m = \frac{Ab-v}{c}$		c	b	β						$b = \beta c + d$
$A = \frac{Bc+v}{d}$			d	c	γ					$c = \gamma d + e$
$B = \frac{Cd-v}{e}$				e	d	δ				$d = \delta e + f$
$C = \frac{De+v}{f}$					f	e	ε			$e = \varepsilon f + g$
$D = \frac{Ef-v}{g}$						g	f	ζ		$f = \zeta g + h$
$E = \frac{Fg+v}{h}$							h	g	η	$g = \eta h + i$
$F = \frac{Gh-v}{i}$								i	h	θ $h = \theta i + k$
$G = \frac{Hi+v}{k}$									k	

8. Haec ergo operatio, qua ad maximum communem divisorem numerorum *a* et *b* uti solemus, eousque est continuanda, donec ad residuum perveniatur, quod dividat *v.* Quo invento sequenti modo investigabimus numerum *m.* Si *v* iam per *b* dividi poterit, fiet $m = 0$. Si *v* per *c* divisionem admittat, fiet $A = 0$ et $m = \frac{-v}{c}$. Si *v* per *d* dividatur, fiet $B = 0$ et $A = \frac{v}{d}$ atque $m = \frac{bv}{cd} - \frac{v}{c} = \frac{bv}{d}$ ob $b = \beta c + d$. Quo autem valores ipsius *m* facilius reperiantur, primo valor ipsius *A* per *B,* tum valor ipsius *B* per *C* et ita porro exprimi debet, unde nata est ista tabula:

1. $m = \frac{Ab-v}{c}$,
2. $m = \frac{Bb+\beta v}{d}$,
3. $m = \frac{Cb-v(1+\beta\gamma)}{e}$,
4. $m = \frac{Db+v(\delta+\beta\gamma\delta+\beta)}{f}$,
5. $m = \frac{Eb-v(\delta\varepsilon+\beta\gamma\delta\varepsilon+\beta\varepsilon+\beta\gamma+1)}{g}$,
6. $m = \frac{Fb+v(\delta\varepsilon\zeta+\beta\gamma\delta\varepsilon\zeta+\beta\varepsilon\zeta+\beta\gamma\zeta+\zeta+\delta+\beta\gamma\delta+\beta)}{h}$,

etc.

De his valoribus est notandum signa ipsius *v* alternari hoc modo $-+-+-+$ etc.
Deinde coefficientes ipsius *v* hanc tenent legem

β	γ	δ	ε	ζ	
1,	$\beta\beta$,	$\beta\gamma+1$,	$\beta\gamma\delta+\delta+\beta$,	$\beta\gamma\delta\varepsilon+\beta\varepsilon+\delta\varepsilon+\beta\gamma+1$	etc.,

cuius progressionis quisque terminus est aggregatum ex termino praecedente in indicem supra se scriptum multiplicato et termino hunc praecedente.

9. Si igitur *v* per *b* dividi poterit, erit $m = 0$; si *v* per *c* dividi potest, erit $m = \frac{-v}{c}$ propter $A = 0$; si *v* per *d* dividi poterit, fiat $B = 0$ eritque $m = \frac{v}{d}\beta$. Unde sequens oritur lex:

Si est numerus integer	erit
$\frac{v}{b}$	$m = 0$
$\frac{v}{c}$	$m = -\frac{v}{c}$
$\frac{v}{d}$	$m = +\frac{v}{d}\beta$
$\frac{v}{e}$	$m = -\frac{v}{e}(\beta\gamma+1)$
$\frac{v}{f}$	$m = +\frac{v}{f}(\beta\gamma\delta+\delta+\beta)$
$\frac{v}{g}$	$m = -\frac{v}{g}(\beta\gamma\delta\varepsilon+\delta\varepsilon+\beta\varepsilon+\beta\gamma+1)$
$\frac{v}{h}$	$m = +\frac{v}{h}(\beta\gamma\delta\varepsilon\zeta+\delta\varepsilon\zeta+\beta\varepsilon\zeta+\beta\gamma\zeta+\beta\gamma\delta+\zeta+\delta+\beta)$

etc.

Si _nunc hi ipsius *m* valores in aequatione $z = ma + p$ substituantur, reperietur,

ut sequitur:

Si est integer

Si est integer	erit
$\frac{v}{b}$	$z = q + \frac{bv}{b}1 = q+v$
$\frac{v}{c}$	$z = q - \frac{bv}{c}\alpha$
$\frac{v}{d}$	$z = q + \frac{bv}{d}(\alpha\beta+1)$
$\frac{v}{e}$	$z = q - \frac{bv}{e}(\alpha\beta\gamma+\alpha+\gamma)$
$\frac{v}{f}$	$z = q + \frac{bv}{f}(\alpha\beta\gamma\delta+\alpha\beta+\alpha\delta+\gamma\delta+1)$
$\frac{v}{g}$	$z = q - \frac{bv}{g}(\alpha\beta\gamma\delta\varepsilon+\alpha\beta\varepsilon+\alpha\delta\varepsilon+\gamma\delta\varepsilon+\alpha+\gamma+\varepsilon)$
	etc.

10. Ad inveniendum ergo numerum *z*, qui per *a* divisus relinquat *p* et per *b* divisus relinquat *q*, posito $p - q = v$ sequentem habebimus regulam:

Instituatur operatio ad maximum communem divisorem inter *a* et *b* inveniendum eaque eousque producatur, donec ad residuum perveniatur, quod sit divisor ipsius *v*, teneaturque quotus ex divisione ipsius *v* per illud residuum resultans, qui sit *Q*, ubi operatio abrumpatur. Deinde in serie scribantur quoti α, β, γ etc. in hac divisione orti ex iisque construatur nova series

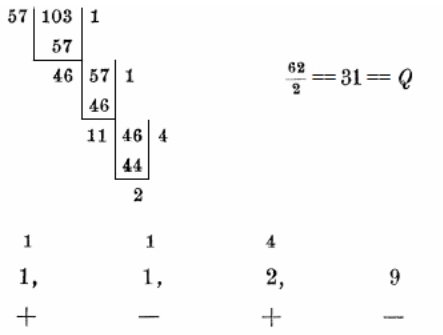
$$1,\ \alpha,\ \alpha\beta+1,\ \alpha\beta\gamma+\alpha+\gamma \text{ etc.},$$

quae ex illa quotorum serie formatur atque eousque continuari debet, quousque per illam seriem fieri potest. Sub hac nova serie scribantur signa alternantia $+-+-$ etc. ultimusque terminus cum suo signo multiplicetur per *Q* atque etiam per minorem divisorem propositum *b;* ad factum addatur residuum *q* divisori *b* respondens. Quo facto erit aggregatum numerus quaesitus.

11. Invento hoc modo uno numero satisfaciente *z* ex eo statim innumerabiles alii numeri satisfacientes reperiuntur. Nam si *z* per *a* divisum *p* relinquit et per *b* divisum *q*, eandem proprietatem habebunt quoque numeri $ab + z$, $2ab+z$ et $mab + z$. Multiplum quidem facti *ab* continuo adiici vel auferri potest, si *a* et *b* fuerint inter se numeri primi; at si *a* et *b* fuerint numeri compositi, tum etiam sufficit eorum minimum communem dividuum sumsisse, cuius multiplum quodque adiectum vel ablatum a *z* dabit numeros satisfacientes; ut si minimus communis dividuus fuerit *M*, comprehendet $mM + z$ omnes omnino numeros quaestioni satisfacientes. Quare etiamsi hoc modo saepe numeri negativi pro *z* inveniantur, tamen adiiciendo ad eos *M* vel eius multiplum obtinebuntur numeri affirmativi. Hac ergo operatione semper minimus numerus satisfaciens invenietur, siquidem minimus communis dividuus *M* toties subtrahatur, quoties fieri potest.

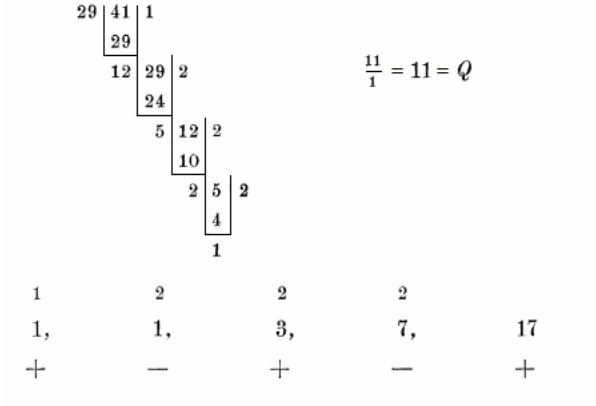
12. Quia exemplis haec operatio maxime illustrabitur, quaeramus numerum, qui per 103 divisus relinquat 87 et per 57 divisus relinquat 25. Erit ergo

$a=103,\ b=57,\ p=87$ et $q=25$ atque $v=62$; quare operationem ita instituo:



Nunc est $-9\cdot 31=-279$ atque numerus quaesitus $25-57\cdot 279$; qui cum fiat negativus, addo ad eum $3\cdot 57\cdot 103$ seu $57\cdot 309$, unde invenitur $25\cdot 57\cdot 30=1735$, qui est minimus numerus quaesitus; omnes vero satisfacientes continentur in hac forma $m\cdot 103\cdot 57+1735$.

13. Quaeramus porro numerum, qui per 41 divisus relinquat 10 et per 29 divisus relinquat 28. In hoc exemplo compendium adhibebo, quod in aliis similibus computationibus magnam habebit utilitatem; nam cum in divisione per 29 residuum sit 28, restare quoque poterit in eadem divisione -1, si quotus unitate maior accipiatur. Sumo ergo -1 pro residuo divisoris 29 eritque $a=41,\ b=29,\ p=10$ et $q=-1,$ unde erit $v=11$. Operationem ergo ut ante instituo ita:

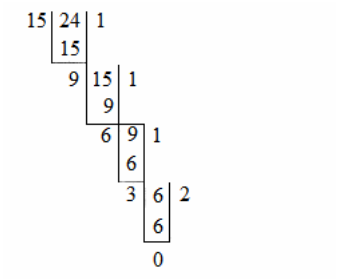


Erit ergo $+17\cdot 11=187$ atque numerus quaesitus $=-1+29\cdot 187$. Subtrahatur $29\cdot 4\cdot 41$; erit is $=-1\cdot 29\cdot 23=666$. Satisfacient ergo quaestioni omnes numeri in hac forma $m\cdot 41\cdot 29+666$ contenti.

14. Compendium hinc se prodit ad supra datam regulam adiiciendum, quod in hoc constat, ut, postquam numerus *Q* per ultimum seriei formatae terminum est multiplicatus, factum per maiorem divisorem *a* dividatur atque residuum loco ipsius facti adhibeatur. Scilicet hoc residuum per minorem divisorem *b* multiplicatum atque residuo *q* auctum dabit numerum quaesitum. Atque iste numerus hoc pacto inventus erit minimus, qui satisfacit. Praeterea hac divisione effici potest, ut residuum prodeat affirmativum, etiamsi

dividendus fuerit negativus. Ita in primo exemplo § 12 habebatur -279, qui numerus per 103 divisus sumto quota $=3$ relinquit +30. Ex quo numerus quaesitus minimus est $=25+57\cdot 30=1735$.

15. Fieri deinde etiam potest, ut huiusmodi exempla proponantur, quae solutionem omnino non admittant, uti si quaeratur numerus, qui per 24 divisus relinquat 13, per 15 vero divisus relinquat 9; talis enim numerus per alteram conditionem deberet esse per 3 divisibilis, per alteram secus. Idem vero etiam ipsa regula ostendit; nunquam enim ad tale residuum excepto 0 devenietur, quod dividat *v* seu 4, uti ex ipsa operatione videre est:



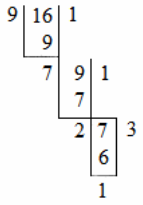
Huiusmodi vero exempla exhiberi non possunt, nisi divisores *a* et *b* sint numeri compositi inter se; nam si fuerint inter se primi, semper numeri quaesiti exhiberi possunt. Sin autem divisores *a* et *b* fuerint numeri compositi atque *v* non dividi potuerit per maximum ipsorum *a* et *b* divisorem, tum semper problema ad absurdum deducit. Hocque est criterium, ex quo, num problema solutionem admittat, diiudicari potest, antequam operatio instituatur.

16. Exposita hac methodo universali, qua omnis generis huius problemata facile resolvi possunt, ex ea alia regula potest formari, quae quidem ad usum non est tam facilis, at simplicitatis plus in se habet. Oritur ea autem, si in valoribus supra inventis ipsius *z* (§ 9) loco $\alpha,\ \beta,\ \gamma$ etc. eorum valores ex aequationibus $a=\alpha b+c,\ b=\beta c+d$ etc. substituantur. Nam si instituatur operatio ad maximum communem divisorem inter *a* et *b* inveniendum ex eaque innotescant continua residua *c*, *d*, *e* etc., dico fore numerum

$$z=q+abv\left(\frac{1}{ab}-\frac{1}{bc}+\frac{1}{cd}-\frac{1}{de}+\frac{1}{ef}-\text{etc.}\right)$$

eousque hac serie continuanda, donec *v* per factorem aliquem denominatoris dividi queat.

Uti si quaeratur numerus, qui per 16 divisus relinquat 1 et per 9 divisus relinquat 7, erit $a=16,\ b=9,\ p=1,\ q=7$ et $v=-6$. Quare



Hinc ergo erit

$$z = 7 - 6\cdot 9\cdot 16\left(\tfrac{1}{16\cdot 9} - \tfrac{1}{9\cdot 7} + \tfrac{1}{7\cdot 2}\right) = 7 - 6 + \tfrac{6\cdot 16}{7} - \tfrac{3\cdot 9\cdot 16}{7} = 1 - 3\cdot 16 = -47.$$

Satisfaciunt ergo omnes numeri $m\cdot 144 - 47$ seu $m\cdot 144+97$ eorumque minimus est 97.
Superior formula generalis ipsius *z* etiam in hunc modum potest exprimi

$$z = p - abv\left(\tfrac{1}{bc} - \tfrac{1}{cd} + \tfrac{1}{de} - \tfrac{1}{ef} + \text{etc.}\right),$$

quae series fractionum eousque continuari debet, donec valor ipsius *z* fiat numerus integer.

17. Considerabo nunc quosdam casus particulares, in quibus *a* ad *b* datam habeat relationem; et primo quidem sit $b = a - 1$ seu $a = b + 1$, residua vero ex divisione numeri quaesiti per *a* et *b* orta sint ut ante *p* et *q*. Erit ergo $c = 1$ ideoque per regulam postremam

$$z = p - av = ap + aq.$$

Quae expressio, si $aq + p > ap$, dat minimum numerum quaesito satisfacientem; at si $aq+p < ap$, tum minimus numerus satisfaciens erit $a^2 - a + p - ap+aq$. Omnes vero numeri satisfacientes in hac formula generali $ma^2 - ma + p - ap + aq$ comprehenduntur, seu etiam in ista $mb^2 + mb - bp + bq + q$. Quicquid nunc sit *m*, si haec quantitas dividatur per $b^2 + b$, residuum erit minimus numerus quaesito satisfaciens.

18. Quemadmodum hac ratione ope residuorum datorum, quae post divisionem numeri incogniti per divisores *b* et $b+1$ remanent, ipse numerus incognitus sit inveniendus, docuit Stifilius in Commentario ad Rudolfi artem Cossicam. Regula eius ita se habet: Si fuerit residuum numeri incogniti per $b+1$ divisi *p* et residuum eiusdem per *b* divisi *q*, iubet *q* multiplicare per *b* + 1 et *p* per b^2 horumque factorum aggregatum per $b^2 + b$ dividere; quod restat post divisionem, id pronunciat esse numerum quaesitum. Fluit autem haec regula ex nostra generali formula, si ponatur $m = p$; tum enim habetur $b^2 p + (b+1)q$, quod per $b^2 + b$ divisum relinquit minimum numerum quaesitum.

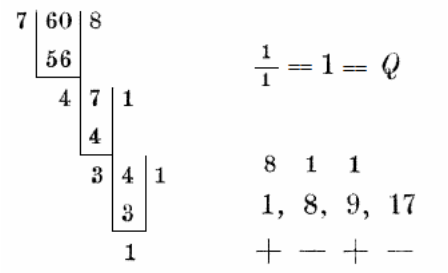
19. Interim tamen minori opera minimus numerus satisfaciens reperietur sequenti modo: Residuum *q*, quod ex divisione quaesiti numeri per *b* oritur, multiplicetur per $b+1$ factumque addatur ad numerum proni cum ipsius *b*, puta ad $b^2 + b$, hinc subtrahatur factum ex residuo *p*, quod ex divisione numeri quaesiti per $b+1$ remanet, ducto in *b;* si id, quod restat, fuerit $< b^2 + b$, erit id ipse numerus quaesitus, sin vero fuerit $> b^2 + b$, subtrahatur $b^2 + b$ eritque residuum numerus quaesitus. Ut si quaeratur numerus, qui per

100 divisus relinquat 75 et per 101 divisus 37; tum addatur 10100 ad factum ex 75 in 101 seu 7575, ut habeatur 17675, hinc subtrahatur factum ex 37 in 100 seu 3700; remanebit 13975; a quo si 10100 auferantur, prodibit 3875, qui est minimus numerus quaesitus.

20. Si quaeratur numerus, qui per *b* divisus relinquat *q* et per $nb+1$ divisus *p*, erit iterum $c=1$ atque numerus quaesitus $z=p-av=p-ap+aq=(nb+1)q-nbp$ ob $a=nb+1$. Atque omnes numeri satisfacientes continebuntur in hac expressione $mnb^2+mb+(nb+1)q-nbp$, ex qua sumto pro *m* numero quocunque invenietur minimus numerus satisfaciens, si ea expressio dividatur per nb^2+b ; residuum enim erit minimus numerus satisfaciens.

21. Casus porro notari meretur, quo residua *p* et *q*, quae oriuntur ex divisione quaesiti numeri per datos divisores *a* et *b*, sunt inter se aequalia seu $p=q$. Hoc enim casu fit $v=0$ ideoque invenitur numerus quaesitus $z=p$. Si igitur sit *M* minimus communis dividuus numerorum *a* et *b*, omnes numeri satisfacientes continebuntur in hac formula $mM+p$. Eadem plane formula quoque satisfacit, si quotcunque fuerint divisores *a, b, c, d* etc., per quos singulos numerus quaesitus divisus relinquat *p*, si quidem *M* denotet omnium divisorum minimum communem dividuum. Omnes ergo numeri huiusmodi quaestionibus satisfacientes ita sunt comparati, ut per *M* divisi relinquant *p.*

22. Hinc satis tritum problema, quo quaeritur numerus, qui per 2, 3,4, 5, 6 divisus relinquat 1, per 7 vero nihil relinquat, solvi potest. Omnes enim numeri, qui per 2, 3, 4, 5, 6 divisi relinquunt 1, hanc habent proprietatem, ut per 60, qui numerus est minimus communis dividuus numerorum 2, 3, 4, 5 et 6, divisi relinquant 1. Problema ergo huc redit, ut inveniatur numerus, qui per 60 divisus relinquat 1, per 7 vero sit divisibilis; erit ergo $a=60,\ b=7,\ p=1,\ q=0$ et $v=1$. Facta ergo operatione



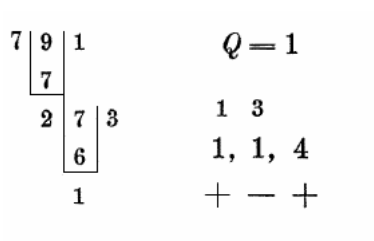
erit $z=0-119+420m$, et si $m=1$, erit $z=301$.

23. Maiorem difficultatem habere videtur hoc problema, quo quaeritur numerus, qui per numeros 2, 3, 4, 5, 6 divisus respective relinquat numeros 1, 2, 3, 4, 5, at per 7 dividi queat, propter residua proposita inaequalia. Sed haec quaestio congruit cum hac: Invenire numerum, qui per 2, 3, 4, 5, 6 divisus relinquat -1 et per 7 nihil. Illi iam conditioni satisfacit forma $60m-1$; quare numerus quaeritur, qui per 60 divisus -1, at per 7 nihil relinquat; fit itaque $a=60,\ b=7,\ p=-1,\ q=0$ et $v=-1$ atque operatione ut ante

instituta est $Q=-1$, quod in -17 ductum dat +17; hocque per *b* multiplicatum dat 119, numerum quaesitum.

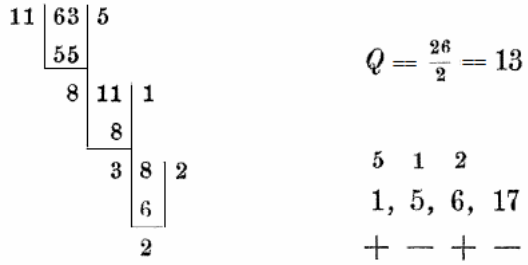
24. Ex his duobus exemplis apparet, quomodo huiusmodi quaestiones, in quibus quotcunque divisores proponuntur, quibus autem duo tantum residua respondent, per supra datas regulas solvi queant; statim enim quaestio ad quaestionem duorum divisorum reducitur; uti si omnia residua sunt aequalia, quaestio perinde solvitur, ac si unicus divisor fuisset propositus. At si residua sunt inaequalia, tum nihilominus repetendis his operationibus, quibus pro duobus divisoribus usi sumus, solutio poterit obtineri. Primo enim duobus divisoribus satisfieri debet, tum tertius assumitur, deinde quartus, donec omnibus erit satisfactum. Hoc vero commodissime exemplis explicabitur.

25. Quaeramus igitur numerum, qui per 7 divisus relinquat 6, per 9 relinquat 7, per 11 relinquat 8 et per 17 relinquat 1. Ex his iam quatuor conditionibus sumamus duas quasque, ut duas priores, et investigemus omnes numeros iis satisfacientes. Erit ergo $a=9,\ b=7,\ p=7,\ q=6$ et $v=1$, quare operatio instituetur, uti sequitur:



fietque $z=6+1\cdot 4\cdot 7=34$.
Omnes ergo numeri his duabus conditionibus satisfacientes continentur in hac forma $63m+34$ seu ita erunt comparati, ut per 63 divisi relinquant 34.

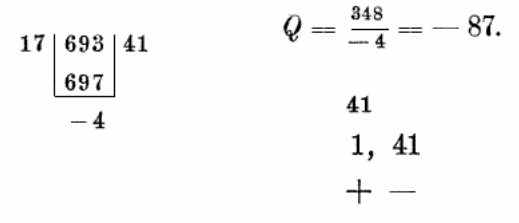
26. Problema ergo huc est reductum, ut inveniatur numerus, qui divisus per 63 relinquat 34, per 11 relinquat 8 et per 17 relinquat 1. Harum trium conditionum sumantur duae priores eritque $a=63,\ b=11,\ p=34,\ q=8$ et $v=26,$ unde fluit sequens operatio:



ergo $z=m\cdot 63\cdot 11+8-13\cdot 17\cdot 11$.

Quo minimus numerus satisfaciens reperiatur, ponatur $m=4$; erit $z=8+31\cdot 11=349$.
Omnes ergo numeri satisfacientes in hac continentur forma $693m+349$ seu hanc habebunt proprietatem, ut per 693 divisi relinquant 349.

27. Problema ergo tandem huc est reductum, ut definiatur numerus, qui per 693 divisus relinquat 349 et per 17 divisus relinquat 1. Facio ergo $a = 693,\ b = 17,\ p = 349,\ q = 1$ et $v = 348$ sequentemque iuxta data praecepta instituo operationem:



$$z = 693 \cdot 17 \cdot m + 1 + 41 \cdot 87 \cdot 17.$$

Quo minimus numerus satisfaciens prodeat, pono $m = -5$ eritque

$$z = 1 + 102 \cdot 17 = 1735,$$

qui est minimus numerus quatuor praescriptis conditionibus satisfaciens. Omnes autem, qui satisfaciunt, hac continentur formula 11781*m*+1735. Ex hoc exemplo ergo abunde intelligitur, quomodo omnes huiusmodi quaestiones sint resolvendae.

28. Pertinet huc solutio problematis chronologici satis cogniti, quam, prout ex his regulis inveni, apponam, in quo annus a Christo nato quaeritur ex datis cyclis solis et lunae una cum indictione Romana illius anni. Cum enim cyclus solis sit residuum, quod oritur divisione numeri anni novenario aucti per 28, cyclus vero lunae sit residuum, quod oritur divisione numeri anni unitate aucti per 19, indictio vero Romana sit residuum, quod oritur, si numerus anni ternario auctus per 15 dividatur, sequens prodiit solutio.
Sit *p* cyclus solis, *q* cyclus lunae et *r* indictio Romana; multiplicetur *p* per 4845, *q* per 4200 et *r* per 6916, haec tria producta cum numero 3267 in unam summam coniiciantur eaque dividatur per 7980; quod remanebit residuum, erit numerus anni quaesiti. Si annus periodi Iulianae requiratur, tum operatio eodem modo instituatur, nisi quod numerus 3267 negligi debet; quae est regula iam passim tradita.

29. Multam quidem operam requirit solutio pro pluribus divisoribus, si quidem problema continuo ad casum, quo divisorum numerus unitate minuitur, ut in praecedente exemplo fecimus, reducitur; at ex ea ipsa operatione facilior multoque brevior via sese prodit, qua statim proposita quaestio, quotcunque etiam fuerint divisores, ad casum duorum divisorum reduci potest; quae regula ita se habet:
Inveniendus sit numerus, qui per divisores *a, b, c, d, e,* quos numeros inter se primos esse pono, divisus relinquat respective haec residua *p, q,r, s, t.* Huic quaestioni satisfacit iste numerus

$$Ap + Bq + Cr + Ds + Et + mabcde,$$

in qua expressione *A* est numerus, qui per factum *bcde* divisus nihil relinquat, per *a* vero divisus relinquat unitatem; *B* est numerus, qui per *acde*
divisus relinquat nihil, per *b* vero unitatem; *C* est numerus, qui per *abde*
divisus nihil relinquat, per *c* vero unitatem; *D* est numerus, qui per *abce*
divisus nihil relinquat, per *d* vero unitatem; atque *E* est numerus, qui per
abed divisus nihil relinquat, per *e* vero unitatum; qui ergo numeri per regulam pro duobus divisoribus datam inveniri possunt.