# Congruences of the First Degree

*Preliminary theorems about prime numbers, factors, etc.*

Art. 13

**Theorem 1.** *The product of two positive numbers, each of which is smaller than a given prime, cannot be divisible by this prime.*

Let $p$ be the prime, and let $a$ be a positive number $< p$. Then it will be shown that there is no positive number $b$ less than $p$, such that $ab \equiv 0 \pmod{p}$.

*Proof.* If anyone denies it, let us suppose that numbers $b$, $c$, $d$ etc. are given, all of which are $< p$, such that $ab \equiv 0$, $ac \equiv 0$, $ad \equiv 0$. Assume that $b$ is the smallest of these, so that all numbers smaller than $b$ are deprived of this property. Manifestly, $b > 1$, for if $b = 1$ then the product would be $ab = a < p$, so it would not be divisible by $p$. Being prime, $p$ cannot be divided by $b$, and instead must lie between two consecutive multiples of $b$, $mb$ and $(m+1)b$. Let $p - mb = b'$. Then $b'$ will be a positive number $< b$. Since we have assumed that $ab \equiv 0$, it is also true that $mab \equiv 0$ (Art. 7), and hence subtracting from $ap \equiv 0$, one has $a(p - mb) = ab' \equiv 0$; i.e. $b'$ is among the numbers $b$, $c$, $d$ etc., even though $b$ was supposed to be the smallest of them. □

Art. 14

**Proposition 1.** *If neither a nor b is divisible by a given prime number p, then the product ab will also not be divisible by p.*

*Proof.* Let $\alpha$ and $\beta$ be the minimal positive residues of $a$ and $b$. By hypothesis, neither of these is 0. Now if it were true that $ab \equiv 0 (\mathrm{mod}.p)$, then it would also be true that $\alpha\beta \equiv 0$. But this is impossible, by the previous theorem. □

The demonstration of this theorem was handed down by Euclid, *El. VII 32*. However, we did not want to omit it, both because several of the more recent treatments have either given vague reasoning for the demonstration, or have completely passed over the theorem, and also because the nature of the method used here, which we will use below to encode much more complex information, can be more easily understood from a simpler case.

Art. 15

**Proposition 2.** *If none of the numbers a, b, c, d etc. can be divided by a prime number p, then also the product abcd etc. cannot be divided by p.*

*Proof.* According to the preceding article, $ab$ cannot be divided by $p$, therefore also $abc$, hence $abcd$, etc. □

Art. 16

**Theorem 2.** *Any composite number can be resolved into prime factors in a unique way.*

*Proof.* It is evident from first principles that any composite number can be resolved into prime factors, but it is generally tacitly assumed that this cannot be done in several ways. Let us imagine a composite number $A = a^\alpha b^\beta c^\gamma$ etc., where $a$, $b$, $c$ etc. are unequal prime numbers, and suppose that $A$ can be resolved into prime factors in yet another way. First, it is clear that in this second system of factors, primes other than $a$, $b$, $c$ etc. cannot enter, since these are the only primes which divide $A$. Similarly in this second system of

factors, none of the prime numbers $a$, $b$, $c$ etc. can be missing, otherwise the missing prime would not divide $A$ (Art. 15). Therefore, these two factorizations can only differ in that, in one, a prime is repeated more times than in the other. Let $p$ be a prime that occurs $m$ times in one resolution and $n$ times in the other, and let $m > n$. Now let the factor $p$ be removed from each system $n$ times, so that it remains in one still $m - n$ times, while it is gone from the other. Now the number $\frac{A}{p^n}$ has two different factorizations, one of which is completely free of the factor $p$, while the other contains it $m - n$ times, contrary to what we have just shown. □

Art. 17

If, therefore, a composite number $A$ is the product of $B$, $C$, $D$, etc., then it is clear that among the prime factors of the numbers $B$, $C$, $D$, there cannot be others than those which are also among the factors of $A$, and any one of these factors occurs as many times in $B$, $C$, $D$, etc. as in $A$. From this is obtained a criterion for whether one number $B$ divides another number $A$, or not. This will happen if $B$ does not involve any prime more times than $A$; if this condition is lacking, then $B$ will not divide $A$.

It can easily be derived from this, with the help of the calculus of combinations, that if $A = a^\alpha b^\beta c^\gamma$ etc., where as above $a$, $b$, $c$, etc. denote distinct prime numbers, then $A$ has

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

distinct divisors, including 1 and $A$.

Art. 18

If, therefore, $A = a^\alpha b^\beta c^\gamma$ etc., $K = k^\alpha \ell^\lambda m^\mu$ etc., and the primes $a$,$b$,$c$ etc., $k$, $\ell$, $m$ etc. are all distinct from each other, then it is clear that $A$ and $K$ have no common divisor other than 1, or that they are relatively prime to each other.

Given several numbers $A$, $B$, $C$ etc. the *greatest common divisor* is thus determined. Let them all be resolved into their prime factors, and from these select those primes which are common to all the numbers $A$, $B$, $C$, etc. (if none are present, there will be no divisor common to all). Then it should be noted how often each of these prime factors is contained in $A$, $B$, $C$, etc., or how many dimensions they have in each of $A$, $B$, $C$, etc. Finally give to each prime factor the smallest dimension that it has in each of $A$, $B$, $C$, etc. Compute the product of all of these, and the result will be the required common divisor.

When the least common multiple of the numbers $A$, $B$, $C$ etc. is desired, proceed as follows. Collect all the prime numbers that divide the numbers $A$, $B$, $C$ etc., and assign to each prime factor the largest dimension that it has in each of $A$, $B$, $C$, etc. Compute the product of all of these, and the result will be the required common multiple.

*Example.* Let $A = 504 = 2^2 3^2 7$; $B = 2880 = 2^6 3^2 5$; $C = 864 = 2^5 3^3$. To find the greatest common divisor, the prime factors 2 and 3 are taken, to which the dimensions 3 and 2 are assigned; thus the greatest common divisor is $= 2^3 3^2 = 72$. The least common multiple will be $2^6 3^3 5.7 = 60480$.

For the sake of convenience, we omit the demonstrations. After all, it is known how to solve these problems in an elementary way, even when the resolution into factors of $A$, $B$, $C$, etc. is not given.

Art. 19

**Proposition 3.** *If the numbers a, b, c etc. are all relatively prime to another number k, then the product abc etc. is also relatively prime to k.*

*Proof.* Because no prime factor of any number $a$, $b$, $c$ etc. is common to $k$, and the product $abc$ etc. cannot have prime factors other than those which are the factors of $a$, $b$, $c$, the product will not have a common prime factor with $k$. Thus from the preceding article, $k$ is relatively prime to $abc$ etc. □

**Proposition 4.** *If the numbers a, b, c, etc. are all relatively prime to each other, and each of them divides a number k, then the product abc etc. also divides k.*

*Proof.* This is equally easy to derive from Art. 17, 18. For let the product *abc* have a prime divisor $p$, which it contains $\pi$ times. Then it is obvious that one of the numbers $a$, $b$, $c$ must contain this same prime divisor $\pi$ times. Thus $k$, which this number divides, also contains $p$ at least $\pi$ times. Similarly for the remaining divisors of the product *abc*. □

Hence if two numbers $m$, $n$ are congruent according to several relatively prime moduli $a$, $b$, $c$ etc., then they will also be congruent according to the product. For since $m - n$ is divisible by each of $a$, $b$, $c$, it must also be divisible by their product.

Finally, if $a$ is relatively prime to $b$, and $ak$ is divisible by $b$, then $k$ will also be divisible by $b$. Indeed, $ak$ can then be divided by $ab$, i.e. $\frac{ak}{ab} = \frac{k}{b}$ will be an integer.

Art. 20

**Proposition 5.** *If $A = a^\alpha b^\beta c^\gamma$ etc., where a, b, c etc. are distinct prime numbers, and A is also equal to a power $k^n$, then all of the exponents $\alpha$, $\beta$, $\gamma$ etc. must be divisible by n.*

*Proof.* The number $k$ does not involve prime factors other than $a$, $b$, $c$. Let it contain the factor $a$, $\alpha'$ times. Then $k^n$ or $A$ will contain this factor $n\alpha'$ times, therefore $n\alpha' = \alpha$, and $\frac{\alpha}{n}$ is an integer. In a similar way, $\frac{\beta}{n}$, $\frac{\gamma}{n}$ etc. can be shown to be integers. □

Art. 21

**Proposition 6.** *When numbers a, b, c etc. are relatively prime to each other, and their product abc etc. is an $n^{th}$ power, say $= k^n$, then each of the numbers a, b, c etc. will be $n^{th}$ powers.*

*Proof.* Let $a = \ell^\lambda m^\mu p^\pi$ etc., where $\ell$, $m$, $p$ etc. are distinct prime numbers, none of which (by hypothesis), is a factor of the numbers $b$, $c$, etc. Then the product *abc* etc. will include $\ell$ as a factor $\lambda$ times, $m$ as a factor $\mu$ times, etc. Hence $\lambda$, $\mu$, $\pi$ etc. will be divisible by $n$ and

$$\sqrt[n]{a} = \ell^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}}$$

will be an integer. Similarly for the other numbers $b$, $c$, etc. □

These facts about prime numbers having been put forth, we now turn to other things which are more closely related to our purpose.

Art. 22

**Proposition 7.** *If numbers a, b are divisible by k, and congruent according to a modulus m which is relatively prime to k, then $\frac{a}{k}$ and $\frac{b}{k}$ are congruent according to that same modulus.*

*Proof.* For it is clear that $a - b$ are divisible by $k$, and also by $m$ (hypothesis). Therefore (Art. 19) $\frac{a-b}{k}$ is divisible by $m$, i.e. $\frac{a}{k} \equiv \frac{b}{k} (\text{mod. } m)$. □

If the numbers $m$ and $k$ have a greatest common divisor $e$, then instead we will have $\frac{a}{k} \equiv \frac{b}{k} (\text{mod. } \frac{m}{e})$. For $\frac{k}{e}$ and $\frac{m}{e}$ are relatively prime, and $a - b$ is divisible by both $k$ and $m$. Hence also $\frac{a-b}{e}$ is divisible by both $\frac{k}{e}$ and $\frac{m}{e}$, and hence by $\frac{km}{ee}$, i.e. $\frac{a-b}{k}$ is divisible by $\frac{m}{e}$, or in other words $\frac{a}{k} \equiv \frac{b}{k} (\text{mod. } \frac{m}{e})$.

Art. 23

**Proposition 8.** *If numbers $a$ and $m$ are relatively prime, and numbers $e$ and $f$ are incongruent modulo $m$, then $ae$ and $af$ will be incongruent modulo $m$.*

This is just a restatement of the theorem in the preceding article.

From this it is clear that if all of the integers from 0 to $m-1$ are multiplied by $a$, and the products reduced to their minimal residues according to the modulus $m$, then all of the resulting residues will be distinct. But the number of such residues (none of which are $> m$) is $m$, and just as many numbers lie between 0 to $m-1$, so it is clear that among the residues, none of the numbers from 0 to $m-1$ can be missing.

Art. 24

**Proposition 9.** *The expression $ax+b$ , where $a$ and $b$ are arbitrary numbers, and $x$ is an indeterminate or variable number, can be made congruent to any number modulo $m$, provided that $m$ is relatively prime to $a$.*

*Proof.* Let $c$ be the number to which the expression must be congruent, and let $e$ be the minimum residue of $c-b$ according to the modulus $m$. From the preceding article, a value $x < m$ is necessarily given, such that the remainder of the product $ax$ has minimal residue $e$; let this be the value $v$. Then $av \equiv e \equiv c-b$, hence $av+b \equiv c \pmod{m}$. □

Art. 25

An expression representing two congruent quantities in the form of an equation, we call a congruence. A congruence involving an unknown is said to be solved when a value satisfying the congruence (a root) is found for it. Hence it is further understood what it means for a congruence to be solvable or unsolvable. Examples of transcendental congruences will be found below; the algebraic ones are distributed into congruences of the first, second, and higher degrees, according to the greatest power of the unknown. No less can congruences be proposed involving many unknowns, the elimination of which must be inquired into.

*Solution of congruences of the first degree*

Art. 26

It follows from Art. 24 that a congruence of the first degree $ax+b \equiv c$ is necessarily solvable, provided that the modulus is relatively prime to $a$. In this case, let $v$ be the appropriate value of $x$, or the root of the congruence. Then it is clear that all numbers congruent to $v$, according to the modulus of the proposed congruence, will also be roots (Art. 9). Nor is it less easily seen that all the roots must be congruent to $v$: for if another root be $t$, then $av+b \equiv at+b$, hence $av \equiv at$, and hence $v \equiv t$ (Art. 22). Hence it is concluded that the congruence $x \equiv v \pmod{m}$ is a complete solution of the congruence $ax+b \equiv c$.

Since the solutions of the congruence are obtained for values of $x$ which are themselves congruent, and, in this context, congruent numbers are to be considered equivalent, we shall consider such solutions of the congruence to be one and the same. Therefore, since our congruence $ax+b \equiv c$ does not admit of any other solutions, we will pronounce it to be solvable in only one way, or to have only one root. So e.g. the congruence $6x+5 \equiv 13 \pmod{11}$ admits no other roots than those which are $\equiv 5 \pmod{11}$. The situation is not the same for congruences of higher degrees, or even for congruences of the first degree in which the unknown is multiplied by a number which is not relatively prime to the modulus.

Art. 27

It remains for us to add some things about finding solutions of this kind of congruence. First, we observe that a congruence of the form $ax+t \equiv u$, the modulus of which we suppose is relatively prime to a, depends only on the solution of $ax \equiv \pm 1$. For if $x = r$ satisfies the latter, $x = \pm(u-t)r$ will satisfy the former. But the congruence $ax \equiv \pm 1$, with the modulus $b$, is equivalent to the indeterminate equation $ax = by \pm 1$, whose solution is indeed abundantly known at this time; therefore it will be sufficient for us to transcribe the algorithm by which the calculation is to be done.

If quantities $A$, $B$, $C$, $D$, $E$ etc. depend on others $\alpha$, $\beta$, $\gamma$, $\delta$ etc. in such a way that we have

$$A = \alpha,\ B = \beta A + 1,\ C = \gamma B + A,\ D = \delta C + B,\ E = \epsilon D + C,\ \text{etc.}$$

then for the sake of brevity we write[1]

$$A = [\alpha],\ B = [\alpha, \beta],\ C = [\alpha, \beta, \gamma],\ D = [\alpha, \beta, \gamma, \delta] \text{ etc.}$$

Let the indeterminate equation $ax = by \pm 1$ be proposed, where $a$, $b$ are positive. Let us suppose, which is permitted, that $a$ is not $< b$. Then, using the well-known algorithm according to which the greatest common divisor of two numbers is investigated, equations are formed by ordinary division,

$$a = \alpha b + c,\ b = \beta c + d,\ c = \gamma d + e,\ \text{ etc.}$$

so that $\alpha$, $\beta$, $\gamma$ etc. and $c$, $d$, $e$ etc. are positive integers, and $b$, $c$, $d$, $e$ are continuously decreasing, until one reaches $m = \mu n + 1$, which must eventually happen. So one will have

$$a = [n, \mu, \cdots, \gamma, \beta, \alpha]\ ,\ \ b = [n, \mu, \lambda, \cdots, \gamma, \beta]$$

Then let

$$x = [\mu, \cdots, \gamma, \beta]\ ,\ \ y = [\mu, \cdots, \gamma, \beta, \alpha]$$

and one will have $ax = by + 1$, when the number of $\alpha, \beta, \gamma, \cdots, \mu, n$ is even, and $ax = by - 1$, when it is odd.

Art. 28

The general solution of this kind of equation was first taught by Euler, *Comment. Petrop. T. VII. p. 46.* The method consists in the substitution of other unknowns instead of $x$ and $y$, and this is indeed sufficient. Lagrange approached the matter a little differently: namely, from the theory of continued fractions, it is clear that if the fraction $\frac{b}{a}$ is converted to a continued fraction

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cfrac{1}{\cdots + \cfrac{1}{\mu + \cfrac{x}{n}}}}}}$$

and this deleted last part $\frac{x}{n}$ is restored into a common fraction $\frac{x}{y}$, then $ax = by \pm 1$, since $a$ was relatively prime to $b$. Furthermore, the same algorithm is derived from the above method. The investigations of Lagrange can be found in *Hist. de l'Ac de Berlin Année 1767 p. 175* and *Supplementis versioni gallicae Algebrae Eulerianae adiectis.*

[1] This relation may be considered in a much more general way, which we shall perhaps undertake on another occasion. Here we add only two propositions, which have their use in the present investigation; of course

1. $[\alpha, \beta, \gamma, \cdots, \lambda, \mu] \cdot [\beta, \gamma, \cdots, \lambda] - [\alpha, \beta, \gamma, \cdots, \lambda][\beta, \gamma, \cdots, \lambda, \mu] = \pm 1$

where the positive sign is to be taken when the number of numbers $\alpha, \beta, \gamma, \ldots, \lambda, \mu$ is even, and negative when it is odd.

2. The order of the numbers $\alpha, \beta, \gamma$ etc. can be reversed,$[\alpha, \beta, \gamma, \cdots, \lambda, \mu] = [\mu, \lambda, \cdots, \gamma, \beta, \alpha]$

We suppress here the demonstrations, which are not difficult.

Art. 29

Congruences $ax + t = u$, for which the modulus is not relatively prime to $a$, can be easily reduced to the previous case. Let $m$ be the modulus, and let $\delta$ be the greatest common divisor of $a$ and $m$. First, it is clear that any value of $x$ which satisfies the congruence according to the modulus $m$ also satisfies the congruence according to the modulus $\delta$. But always $ax \equiv 0$ (mod. $\delta$), since $\delta$ itself is divisible by $a$. Therefore, unless $t \equiv u$ (mod. $\delta$), the proposed congruence is not solvable.

Let us therefore set $a = \delta e$, $m = \delta f$, $t - u = \delta k$, so that $e$ and $f$ will be relatively prime. Then the congruence proposed, $dex + dk = 0$ (mod. $df$), will be equivalent to $ex + k \equiv 0$ (mod.$f$), i.e. whichever value of $x$ satisfies one will also satisfy the other, and vice versa. For it is obvious that $ex + k$ can be divided by $f$, when $\delta ex + \delta k$ can be divided by $\delta f$, and vice versa. But we saw above how to solve the congruence $ex + k \equiv 0$ (mod.$f$), hence it is clear that if $v$ is one of the values of $x$, then $x \equiv v$ (mod.$f$) is the complete solution of the proposed congruence.

Art. 30

When the modulus is composite, it sometimes makes sense to use the following method.

Let the modulus $= mn$, and let the proposed congruence be $ax \equiv b$. Let us first solve this congruence according to the modulus $m$, and suppose that it is satisfied if $x \equiv v$ (mod. $\frac{m}{\delta}$), where $\delta$ is the greatest common divisor of the numbers $m$, $a$. It is already clear that any value of $x$ satisfying $ax \equiv b$ according to the modulus $mn$ must also satisfy the same according to the modulus $m$: therefore it must take the form $v + \frac{m}{\delta}x'$, where $x'$ is an indeterminate number, but not all numbers of this form satisfy the congruence (mod. $mn$). The values of $x'$ such that $v + \frac{m}{\delta}x'$ is a root of the congruence $ax \equiv b$ (mod. $mn$), can now be deduced by solving the congruence $\frac{am}{\delta}x' + av \equiv b$ (mod. $mn$), which is equivalent to $\frac{a}{\delta}x' \equiv \frac{b-av}{m}$ (mod. $n$). From this it is concluded that the solution of any congruence of the first degree according to the modulus $mn$ can be reduced to the solution of two congruences according to the moduli $m$ and $n$. It will be easily seen that if $n$ is again the product of two factors, the solution of the congruence according to the modulus $n$ depends on the solution of the two congruences whose moduli are those factors. In general, the solution of a congruence according to any composite modulus depends on the solution of other congruences, the moduli of which are the factors of that number; and these, if it seems convenient, may always be taken in such a way as to be prime numbers.

*Example.* If the congruence $19x \equiv 1$ (mod. 140) is proposed: solve it first modulo 2, which gives $x \equiv 1$ (mod. 2). Put $x = 1 + 2x'$, and it becomes $38x' \equiv -18$ (mod. 140), which is equivalent to $19x' \equiv -9$ (mod. 70). If this is solved again according to the modulus 2, it becomes $x' \equiv 1$ (mod. 2), and after setting $x' = 1 + 2x''$, it becomes $38x' \equiv -28$ (mod. 35). Solving modulo 5 gives $x'' \equiv 4$ (mod. 5), and substituting $x'' = 4 + 5x'''$ it becomes $95x'' \equiv -90$ (mod. 35), which is equivalent to $19x''' \equiv -18$ (mod. 7). From this it finally follows that $x''' \equiv 2$ (mod. 7), and putting $x''' = 2 + 7x'$ we get $x = 59 + 140x'''$, and therefore $x \equiv 59$ (mod. 140) is the complete solution of the proposed congruence.

Art. 31

In the same way that the root of the equation $ax = b$ is expressed by $\frac{b}{a}$, we can also denote the root of the congruence $ax \equiv b$ by $\frac{b}{a}$, including the modulus of the congruence for the sake of clarity. So e.g. $\frac{19}{17}$ (mod. 12) denotes any number that is $\equiv 11$ (mod. 12).[2] It is generally clear from the above that $\frac{b}{a}$ (mod. $c$) does not have any real significance in the case where $a$ and $c$ have a common divisor which does not divide $b$ (or, if one prefers, it is imaginary). But except in this case, the expression $\frac{b}{a}$ (mod. $c$) will always have real values, and indeed infinitely many, which will all be congruent modulo $c$ when $a$ is relatively prime to $c$, or more generally modulo $\frac{c}{\delta}$, where $\delta$ is the greatest common divisor of $c$ and $a$.

These expressions have almost the same arithmetic as ordinary fractions. Here we add some properties that can be easily deduced from what we have already shown.

[2] This could likewise be denoted by $\frac{11}{1}$ (mod. 12)

1. If $a \equiv \alpha$ and $b \equiv \beta$ modulo $c$, then the expressions $\frac{a}{b}$ (mod. $c$) and $\frac{\alpha}{\beta}$ (mod. $c$) are equivalent.
2. $\frac{a\delta}{b\delta}$ (mod. $c\delta$) and $\frac{a}{b}$ (mod. $c$) are equivalent.
3. $\frac{ak}{bk}$ (mod. $c$) and $\frac{a}{b}$ (mod. $c$) are equivalent if $k$ is relatively prime to $c$.

Many other similar propositions might be added here: but as they are not difficult, and unnecessary for what follows, let us move on to other things.

*On finding numbers with given remainders according to given moduli*

Art. 32

A problem which will be of great use in what follows is to find all the numbers which form given remainders according to several given moduli. First, let there be given two moduli $A$ and $B$, and a number $z$ must be found which is congruent to $a$ and $b$ according to these moduli respectively. Then all the values of $z$ are contained in the form $Ax+a$, where $x$ is indeterminate but also satisfies $Ax+a = b$ (mod. $B$). If the greatest common divisor of the numbers $A$ and $B$ is $\delta$, then the complete solution of this congruence will have the form $x = v$ (mod. $\frac{B}{\delta}$), or what amounts to the same thing, $x = v + \frac{kB}{\delta}$, where $k$ denotes an arbitrary integer. Hence the formula $Av + a + \frac{kAB}{\delta}$ includes all the values of $z$, i.e. $z \equiv Av + a$ (mod. $\frac{AB}{\delta}$) will be the complete solution of the problem. If to the moduli $A$, $B$ a third $C$ is added, according to which the number $z$ must be $\equiv c$, then it is obvious how to proceed in the same way, since the two previous conditions have already been fused into one. Namely, if the greatest common divisor of the numbers $\frac{AB}{\delta}, C$ is $= \epsilon$, and the congruence $\frac{AB}{\delta}x + Av + a \equiv c$ (mod. $C$) has the solution $x \equiv w$ (mod. $\frac{C}{\epsilon}$), then the problem will be solved by the congruence $z \equiv \frac{ABw}{\delta} + Av + a$ (mod. $\frac{ABC}{\delta\epsilon}$). One can proceed in the same way, no matter how many moduli are proposed. It can be observed that $\frac{AB}{\delta}$ and $\frac{ABC}{\delta\epsilon}$ are the greatest common divisors of $A$, $B$ and $A$, $B$, $C$ respectively, and it is easy to see from this that no matter how many moduli $A$, $B$, $C$ etc. are given, if their least common multiple is $M$, then the complete solution will be of the form $z \equiv r$ (mod. $M$).

*Example.* Let the numbers $A, B, C; a, b, c$ be $504, 35, 16; 17, -4, 33$. Here the first two conditions, $z \equiv 17$ (mod. 504) and $z \equiv -4$ (mod. 35), are equivalent to the single condition $z \equiv 521$ (mod. 2520). When combined with the condition $z \equiv 33$(mod. 16), it appears that $z \equiv 3041$ (mod. 5040).

Art. 33

When the numbers $A$, $B$, $C$ etc. are all prime to each other, it is clear that their product is equal to their least common multiple. In this case it is clear that the congruences $z \equiv a$ (mod. $A$), $z \equiv b$ (mod. $B$) etc. are together equivalent to a single congruence $z \equiv r$ (mod. $R$), where $R$ denotes the product of the numbers $A$, $B$, $C$ etc. Conversely, it follows from this that a single condition $z \equiv r(R)$ can be decomposed into several; that is, if $R$ is somehow resolved into mutually prime factors $A$, $B$, $C$, then the conditions $z \equiv r(A)$, $z \equiv r(B)$, $z \equiv r(C)$ together will be equivalent to the original one.

This observations leads us to a method of not only discovering an impossibility if it exists, but also arranging the calculations more conveniently and neatly.

Art. 34

Let the conditions proposed above be $z \equiv a$ (mod. $A$), $z \equiv b$ (mod. $B$), $z \equiv c$ (mod. $C$). Resolve all of the moduli into relatively prime factors, $A$ into $A'A''A'''$, $B$ into $B'B''B'''$ etc., so that the numbers $A'$,$A''$, etc. $B'$,$B''$, etc. etc. are either primes, or powers of primes. Of course, if one of the numbers $A$, $B$, $C$, etc. is already prime itself, or a power of a prime, then no resolution into factors is needed for it. Then it is clear from the preceding, that for the proposed conditions the following can be substituted: $z \equiv a$ (mod. $A'$), $z \equiv a$ (mod. $A''$), $z \equiv a$ (mod. $A'''$), etc., $z \equiv b$ (mod. $B'$),$z \equiv b$ (mod. $B''$),$z \equiv b$ (mod. $B'''$), etc. etc. The later conditions must be among the first; then we can be sure of the possibility of the problem and proceed according to the precepts given above.

Art. 35

*Example.* If as above we set $z \equiv 17$ (mod. 504, $\equiv -4$ (mod. 35), and $\equiv 33$ (mod. 16), then these conditions resolve into $z \equiv 17$ (mod. 8), $\equiv 17$ (mod. 9), $\equiv 17$ (mod. 7), $\equiv -4$ (mod. 5), $\equiv -4$ (mod. 7), $\equiv 33$ (mod. 16). From these conditions $z \equiv 17$ (mod. 8), $z \equiv 17$ (mod. 7) can be rejected, as the former is contained within $z \equiv 33$ (mod. 16), and the latter is identical to $z \equiv -4$ (mod. 7); so what remains is

$$z \equiv \begin{cases} 17 \text{ (mod. } 9) \\ -4 \text{ (mod. } 5) \\ -4 \text{ (mod. } 7) \\ 33 \text{ (mod. } 16) \end{cases}$$

from which it can be found that

$$z \equiv 3041 \text{ (mod. } 5040)$$

It is clear that it is generally more convenient if, of the remaining conditions, those which had been derived from one and the same condition were to be collected, since this can be done without much difficulty. That is, when some of the conditions $z \equiv a$ (mod. $A'$), $z \equiv a$ (mod. $A''$) etc. have been removed, the rest can be restored as $z \equiv a$ according to the modulus which is the product of the remaining moduli from the original $A'$, $A''$, $A'''$ etc. Thus in our example, the condition $z \equiv -4$ (mod. 35) is automatically restored from $z \equiv -4$ (mod. 5) and $z \equiv -4$ (mod. 7). Now, it does make some difference which of the superfluous conditions are rejected, as far as brevity of calculation is concerned. But these and other practical arts, which are learned from practice much more easily than from precepts, it is not our place to impart here.

Art. 36

When the moduli $A$, $B$, $C$, $D$ etc. are all prime to each other, it is often worth using the following method. Let $\alpha$ be a number which is unity according to $A$, and which is divisible by the product of the remaining moduli. To accomplish this, one can let $\alpha$ be any value (the minimum is generally acceptable) of the expression $\frac{1}{BCD \text{ etc.}}$ (mod. $A$), multiplied by $BCD$. Similarly, let $\beta \equiv 1$ (mod. $B$) and $\equiv 0$ (mod. $ACD$ etc.), $\gamma \equiv 1$ (mod. $C$) and $\equiv 0$ (mod. $ABD$ etc.). Then if a number $z$ is desired, which according to the moduli $A$, $B$, $C$, $D$ etc. is congruent to numbers $a$, $b$, $c$, $d$ etc. respectively, one can put

$$z \equiv \alpha a + \beta b + \gamma c + \delta d + \text{ etc. (mod. } ABCD \text{ etc.)}$$

Obviously, $\alpha a \equiv a$ (mod. $A$); and the other members $\beta b$, $\gamma c$ etc. are all $\equiv 0$ (mod. $A$), hence $z \equiv a$(mod. $A$). A similar demonstration applies to the other moduli.

This solution is preferable to the former when several such problems are to be solved, in which the moduli $A$, $B$, $C$ etc. retain their values; for then the values obtained for the numbers $\alpha$, $\beta$, $\gamma$ etc. remain constant. It comes into use in a chronological problem, where it is asked which Julian year has a given indiction, golden number, and solar cycle. Here $A = 15$, $B = 19$, $C = 28$; thus the value of $\frac{1}{19 \cdot 28}$ (mod. 15) or $\frac{1}{532}$ (mod. 15), is 13, and $\alpha = 6916$. Similar we find $\beta = 4200$, and $\gamma = 4845$, hence the number sought will be the minimum remainder of the number $6916a + 4200b + 4845c$, where $a$ is the indiction, $b$ is the golden number, and $c$ is the solar cycle.

*Linear congruences involving multiple unknowns*

Art. 37

Congruences of the first degree involving a single unknown have now been sufficiently dealt with. It remains to deal with congruences which involve several unknowns. But if we wished to explain each detail with all rigor, this chapter would become quite long. Since it is not our purpose here to exhaust everything, but only to discuss that which seems worthy of attention, we here restrict the investigation to a few observations, with a more abundant exposition of the matter being reserved for another time.

1) In a similar way, as in equations, it is seen that here too there must be as many congruences as there are unknowns to be determined.

2) Therefore, let these congruences be proposed,

$$ax + by + cz + \cdots \equiv f \text{ (mod. } m) \quad \text{(A)}$$
$$ax + by + cz + \cdots \equiv f \text{ (mod. } m) \quad \text{(A')}$$
$$ax + by + cz + \cdots \equiv f \text{ (mod. } m), \quad \text{(A")}$$

in the same number as there are unknowns $x$, $y$, $z$ etc.

Then determine numbers $\xi$, $\xi'$, $\xi''$ so that

$$b\xi + b'\xi' + b''\xi'' + \text{ etc. } = 0$$
$$c\xi + c'\xi' + c''\xi'' + \text{ etc. } = 0$$

and in such a way that they are all integers without common factors (which is possible, from the theory of linear equations). In a similar way determine $v$, $v'$, $v''$ etc., $\zeta$, $\zeta'$, $\zeta''$, etc. etc. so that

$$av + a'v' + a''v'' + \text{ etc. } = 0$$
$$cv + c'v' + c''v'' + \text{ etc. } = 0$$
$$\text{etc.}$$
$$a\zeta + a'\zeta' + a''\zeta'' + \text{ etc. } = 0$$
$$b\zeta + b'\zeta' + b''\zeta'' + \text{ etc. } = 0$$
$$\text{etc. etc.}$$

3) It is clear that if the congruences $A$, $A'$, $A''$ etc. are multiplied by $\xi$, $\xi'$, $\xi''$ etc., then by $v$, $v'$, $v''$ etc. etc., and then added, the following congruences will result:

$$(a\xi + a'\xi' + a''\xi'' + \text{ etc. })x \equiv f\xi + f'\xi' + f''\xi'' + \text{ etc.} \quad (1)$$
$$(bv + b'v' + b''v'' + \text{ etc. })y \equiv fv + f'v' + f''v'' + \text{ etc.} \quad (2)$$
$$(c\zeta + c'\zeta' + c''\zeta'' + \text{ etc. })z \equiv f\zeta + f'\zeta' + f''\zeta'' + \text{ etc.} \quad (3)$$

which for the sake of brevity we write as

$$\Sigma(a\xi)x \equiv \Sigma(f\xi), \quad \Sigma(bv)y \equiv \Sigma(fv), \quad \Sigma(c\zeta)z \equiv \Sigma(f\zeta) \quad \text{etc.}$$

4) Now there are several cases to distinguish.

*First*, when all of the congruences have coefficients $\Sigma(a\xi)$, $\Sigma(bv)$ etc. which are relatively prime to the modulus $m$, they can be solved according to the rules given before, and the complete solution of the problem will be given by congruences of the form $x \equiv p$ (mod. $m$), $y \equiv q$ (mod. $m$) etc.

*Example.* If the following congruences are proposed,

$$x + 3y + z \equiv 1\ , \quad 4x + y + 5z \equiv 7\ , \quad 2x + 2y + z \equiv 3 \text{ (mod. } 8)$$

then one finds $\xi = 9$, $\xi' = 1$, $\xi'' = -14$, from which one derives $-15x \equiv -26$, and therefore $x \equiv 6$ (mod. 8); in the same way it is found that $15y \equiv -4$, $15z \equiv 1$, and hence $y \equiv 4$, $z \equiv 7$ (mod. 8).

5) *Second*, when not all of the coefficients $\Sigma(a\xi)$, $\Sigma(bv)$ etc. are relatively prime to the modulus, let $\alpha$, $\beta$, $\gamma$ etc. be the greatest common divisors of $m$ with $\Sigma(a\xi)$, $\Sigma(bv)$, $\Sigma(c\zeta)$ etc. respectively. Then it is clear that the problem is impossible unless the numbers $\Sigma(f\xi)$, $\Sigma(fv)$, $\Sigma(f\zeta)$ etc. are divisible by $\alpha$, $\beta$, $\gamma$ etc. respectively. But when these conditions are in place, the congruences in (3) will be completely solved by $x \equiv p$ (mod. $\frac{m}{\alpha}$), $y \equiv q$ (mod. $\frac{m}{\beta}$), $z \equiv r$ (mod. $\frac{m}{\gamma}$) etc., or if you prefer will be given by $\alpha$

distinct values of $x$ (i.e. the values $p$, $p+\frac{m}{\alpha}$, ... , $p+\frac{(\alpha-1)m}{\alpha}$, which are incongruent modulo $m$ ), $\beta$ distinct values of $y$, etc. satisfying those congruences, and obviously all the solutions of the proposed congruences (if any are given at all) will be found among these. However, it is not permissible to reverse this conclusion; for generally not all combinations of all $\alpha$ values of $x$ with all of $y$ and all of $z$ etc. will satisfy the problem, but some of them may need to be connected by one or more conditional congruences. But since a complete resolution of this problem is not necessary for what follows, this argument will not be pursued more fully in this place, and we will content ourselves to give the idea with an example.

*Example.* Let the following congruences be proposed:

$$3x+5y+z\equiv 4\ ,\quad 2x+3y+2z\equiv 7\ ,\quad 5x+y+3z\equiv 6 \text{ (mod. 12)}.$$

Here one finds $\xi, \xi', \xi''$; $v, v', v''$ $\zeta, \zeta', \zeta''$; resp. $= 1, -2, 1; 1, 1, -2; -13, 22, -1$, hence $4x\equiv -4$, $7y\equiv 5$, $28z\equiv 96$. From this we get four values $x\equiv 2, 5, 8, 11$; one value $y\equiv 11$, and four values $z\equiv 0, 3, 6, 9$ (mod. 12). To find which combinations of the values of $x$ and $z$ it is permissible to use, we substitute in the given congruences for $x$, $y$, $z$ respectively $2+3t$, 11, $3u$, after which they become

$$57+9t+3u\equiv 0\ ,\quad 30+6t+6u\equiv 0\ ,\quad 15+15t+9u\equiv 0 \text{ (mod. 12)}$$

and these are easily understood to be equivalent to

$$19+3t+u\equiv 0\ ,\quad 10+2t+2u\equiv 0\ ,\quad 5+5t+3u\equiv 0 \text{ (mod. 4)}$$

The first congruence obviously requires that $u\equiv t+1$(mod. 4), and when this value is substituted it is found to satisfy the rest. From this it is concluded that the values $2, 5, 8, 11$ for $x$ (which are produced by substituting $t=0, 1, 2, 3$), necessarily result in the values $3, 6, 9, 0$ respectively for $z$, so that there are altogether four solutions

$$\begin{array}{lllll} x\equiv & 2, & 5, & 8, & 11 \quad \text{(mod. 12)} \\ y\equiv & 11, & 11, & 11, & 11 \\ z\equiv & 3, & 6, & 9, & 0 \end{array}$$

To these discussions, through which the purpose of the section has already been accomplished, we add here some propositions based on similar principles, which will be needed frequently in what follows.

*Various Theorems*

Art. 38

**Problem 1.** *Find how many positive numbers there are, which are less than and relatively prime to a given positive number A.*

For the sake of brevity, let us designate the multitude of positive numbers less than and relatively prime to a given number using the prefixed symbol $\phi$. So, the problem is to find $\phi A$.

I. When $A$ is prime, it is clear that all numbers from 1 to $A-1$ are relatively prime to $A$. Therefore in this case

$$\phi A = A-1$$

II. When $A$ is a power of a prime number, say $= p^m$, then all the numbers divisible by $p$ will not be relatively prime to $A$ and the rest will be. Therefore, of the numbers $p^m-1$ of these are to be rejected: $p, 2p, 3p, \ldots, (p^{m-1}-1)p$; so there remain $p^m-1-(p^{m-1}-1)=p^{m-1}(p-1)$. Hence

$$\phi p^m = p^{m-1}(p-1).$$

III. The remaining cases are easily reduced to these with the help of the following statement:

**Proposition 10.** *If $A$ is divided into relatively prime factors $M$, $N$, $P$, etc. then*

$$\phi A = \phi M.\phi N.\phi P \text{ etc.},$$

*Proof.* The proposition can be shown in this way. Let there be numbers $m$, $m'$, $m''$ etc. which are less than and relatively prime to $M$ and whose multitude is therefore $\phi M$. Similarly let the numbers less than and relatively prime to $N$, $P$, etc. be respectively $n$, $n'$, $n''$ etc.; $p$, $p'$, $p''$ etc. etc., whose multitude $= \phi N$, $\phi P$, etc. It is clear that all the numbers which are relatively prime to the product $A$ are also relatively prime to all of the individual factors $M$, $N$, $P$, etc., and conversely (Art. 19). Furthermore, any number which is congruent to one of the numbers $m$, $m'$, $m''$ etc. modulo $M$ will be relatively prime to $M$, and conversely, and similarly for $N$, $P$ etc. The question is therefore reduced to this: to determine how many of the numbers less than $A$ are congruent to one of $m$, $m'$, $m''$ etc. according to the modulus $M$, congruent to one of $n$, $n'$, $n''$ etc. according to the modulus $N$, etc. But from Art. 32 it follows that all numbers with fixed residues modulo $M$, $N$, $P$ are congruent according to $A$, so that below $A$ only one can be given which is congruent to the given residues modulo $M$, $N$, $P$. Therefore the number sought will be equal to the number of combinations of the individual numbers $m$,$m'$,$m''$ with the individual numbers $n$, $n'$, $n''$ etc. and $p$, $p'$, $p''$ etc. etc. That this is $= \phi M.\phi N.\phi P$ is evident from the theory of combinations. □

IV. Now it is easy to understand how this is to be applied in the general case. Let $A$ be resolved into its prime factors, or reduced to the form $a^\alpha b^\beta c^\gamma$ etc. with $a$,$b$,$c$ etc. being distinct prime numbers. Then one has

$$\phi A = \phi a^\alpha \phi b^\beta \phi c^\gamma = a^{\alpha-1}(a-1)b^{\beta-1}(b-1)c^{\gamma-1}(c-1) \text{ etc.}$$

or more nicely,

$$\phi A = A\frac{a-1}{a}\frac{b-1}{b}\frac{c-1}{c}\cdots.$$

*Example.* Let $A = 60 = 2^2.3.5$. Then $\phi A = \frac{1}{2}.\frac{2}{3}.\frac{4}{5}.60 = 16$. The numbers which are relatively prime to 60 are:

$$1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59$$

The first solution of this problem is found in the commentary of Euler, *theoremata arithmetica nova methoo demonstrata*, Comm. nov. Ac. Petrop. VIII p. 74. The demonstration was later repeated in another dissertation, *Speculationes circa quasdam insignes proprietates numerorum*, Acta Petrop. VIII p. 17.

Art. 39

If the meaning of the symbol $\phi$ is determined in such a way that $\phi A$ denotes the multitude of numbers relatively prime to $A$ and no greater than $A$, then it is clear that $\phi 1$ would no longer be $= 0$, but instead $= 1$. In all other cases, nothing would be changed. Adopting this definition, we have the following theorem:

**Theorem 3.** *If $a$, $a'$, $a''$ are all the divisors of $A$ (not excluding unity and $A$ itself), then*

$$\phi a + \phi a' + \phi a'' + \text{etc.} = A.$$

*Example.* Let $A = 30$. Then $\phi 1 + \phi 2 + \phi 3 + \phi 5 + \phi 6 + \phi 10 + \phi 15 + \phi 30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$.

*Proof.* Multiply all of the numbers relatively prime to $a$ and not greater than $A$ by $\frac{A}{a}$, likewise all those relatively prime to $a'$ by $\frac{A}{a'}$, etc. and we will have $\phi a + \phi a' +$ etc. numbers, all not greater than $A$ itself. But

1) All these numbers are distinct. Indeed, all those which are generated from the same divisor of $A$ would be distinct, which is self-evident. If however, numbers $\mu$ and $\nu$ had come from different divisors $M$ and $N$, then we would have $\frac{A}{M}\mu = \frac{A}{N}\nu$, and it would follow that $\mu N = \nu M$. Assume that $M > N$ (which is allowed). Then since $M$ is relatively prime to $\mu$, and divides the number $\mu N$, it would follow that $M$, the greater, divides $N$, the lesser, a contradiction.

2) Among these numbers all $1, 2, 3, \ldots, A$ will be found. Let $t$ be any number not exceeding $A$, and let $\delta$ be the greatest common divisor of $A$ and $t$. Then $\frac{A}{\delta}$ will be a divisor of $A$ to which $\frac{t}{\delta}$ is prime. Then obviously the number $t$ will be found among those that came out of the divisor $\frac{A}{\delta}$.

3) From this it is concluded that the multitude of these numbers is $A$, and hence

$$\phi a + \phi a' + \phi a'' + \text{ etc.} = A$$

□

Art. 40

**Proposition 11.** *If the greatest common divisor of the numbers A, B, C, D etc is* $= \mu$*, then numbers a, b, c, d can be determined so that*

$$aA + bB + cC + \text{ etc. } = \mu$$

*Proof.* Let us first consider only two numbers $A$, $B$, and let their greatest common divisor be $\lambda$. Then the congruence $Ax \equiv \lambda$ (mod. $B$) will be solvable (Art. 30). Let the root be $\alpha$, and set $\frac{\lambda - A\alpha}{B} = \beta$. Then we will have $\alpha A + \beta B = \lambda$ as desired.

Adding a third number $C$, let the greatest common divisor of $\lambda$ and $C$ be $\lambda'$. Note that $\lambda'$ will also be the greatest common divisor of the numbers $A$, $B$, $C$. Then let numbers $k$ and $\gamma$ be determined so that $k\lambda + \gamma C = \lambda'$, and we will have $k\alpha A + k\beta B + \gamma C = \lambda'$.

Adding a fourth number $D$, let the greatest common divisor of $\lambda'$ and $D$ be $\lambda''$ (which, it is easily seen, is also the greatest common divisor of $A$, $B$, $C$, $D$). Then let $k'\lambda' + \delta D = \lambda''$, and we will have $kk'\alpha A + kk'\beta B + k'\gamma C + \delta D = \lambda''$.

This can be done in a similar way, no matter how many more numbers are added. □

In particular, if the numbers $A$, $B$, $C$ etc. do not have a common divisor, then we can find $a$, $b$, $c$ etc. such that

$$aA + bB + cC + \text{etc.} = 1$$

Art. 41

**Proposition 12.** *If p is a prime number, and there are p things, among which any number may be equal (provided they are not all equal to each other), then the number of permutations of these things is divisible by p.*

*Example.* The five things $A$, $A$, $A$, $B$, $B$ can be permuted in ten different ways.

The demonstration of this theorem is easy indeed, if the well-known theory of permutations is assumed. For if among $p$ things there are first $a$ equal to $A$, $b$ equal to $B$, $c$ equal to $C$ etc. (where the numbers $a$, $b$, $c$ might be unity), so that

$$a + b + c + \text{etc.} = p,$$

then the number of permutations will be

$$= \frac{1.2.3.\ldots.p}{1.2.3\ldots a.1.2\ldots b.1.2\ldots c \text{ etc.}}$$

It is already clear in itself that the numerator of this fraction is divisible by the denominator, since the number of permutations must be an integer: but the numerator is divisible by $p$ and the denominator, which is composed of factors smaller than $p$ itself, is not divisible by $p$ (Art. 15). Therefore the number of permutations will be divisible by $p$ (Art. 19).

We hope however, that the following demonstration will not be unwelcome.

Suppose that in two permutations of things, the order only differs insofar as the thing which occupied the first place in one, occupies a different place in the other, while the rest progress in the same order, except that the thing which was last now comes immediately after that which was first. Then we will call the permutations *similar*[3]. So for example the permutations ABAAB and ABABA will be similar, since the things which in the former occupy the first place, second place, etc. occupy the third place, fourth place, etc. in the latter.

Now, since every permutation consists of $p$ things, it is clear to anyone that $p-1$ similar permutations can be found, in which the thing that was first is moved to the second place, third place, etc. If no two similar permutations can be found which are identical to each other, then it is clear that the number of all permutations will be $p$ times larger than the number of dissimilar permutations, and hence must be divisible by $p$.

Let us suppose, then that two permutations

$$PQ\dots TV\dots YZ; \qquad V\dots YZPQ\dots T,$$

one of which has arisen from the other by the promotion of terms, are identical, or P=V etc. Let the term $P$ which was first in the former be the $(n+1)^{st}$ in the latter. Then in the latter series, the $(n+1)^{st}$ term will be equal to the first, the $(n+2)^{nd}$ term to the second, etc., hence the $(2n+1)^{st}$ again becomes equal to the first, and likewise for the $(3n+1)^{st}$, etc., and in general the $(kn+m)^{th}$ term becomes equal to the $m^{th}$ term (where when $kn+m$ exceeds $p$, either the series $V\dots YZPQ\dots T$ must be repeated from the beginning, or a multiple of $p$ must be subtracted from $kn+m$. Therefore, if $k$ is determined in such a way that $kn \equiv 1 \pmod{p}$, which is possible because $p$ is prime, then it generally follows that the $m^{th}$ and $(m+1)^{st}$ terms are equal, i.e. all the terms are equal, contrary to the hypothesis.

Art. 42

**Proposition 13.** *If the coefficients $A, B, C, \dots, N; a, b, c \dots n$ of two functions of the form*

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \dots + N \qquad (P)$$

$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} + \dots + n \qquad (Q)$$

*are all rational, but not all integral, then in the product of $P$ and $Q$*

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{etc.} + \mathfrak{Z}$$

*not all of the coefficients $\mathfrak{A}$, $\mathfrak{B}$, …, $\mathfrak{Z}$ are integral.*

*Proof.* Let the fractions in the coefficients $A$,$B$ etc., $a$, $b$ etc. be expressed in terms of numbers which are as small as possible, and let $p$ be an arbitrary prime dividing one or more denominators of these fractions. Let us assume, as we may, that $p$ divides the denominator of some fractional coefficient in $(P)$. It is clear that if $(Q)$ is divided by $p$, then at least one fractional coefficient in $(Q)/p$ will have a denominator divisible by $p$ (in particular, the first coefficient will be $\frac{1}{p}$). Now it is easy to see that in $(P)$ there will be a single coefficient whose denominator is divisible by a larger power of $p$ than that of any preceding coefficient, and no less than that of any following coefficient. Let this term $= Gx^g$, and let the power of $p$ in its denominator be $t$. Let the analogous term in $\frac{(Q)}{p}$ be $= \Gamma x^\gamma$, and let the power of $p$ in the denominator of $\Gamma$ be $\tau$. Obviously $t+\tau$ will be at least 2. With this understood, the term $x^{g+\gamma}$ in the product of $(P)$ and $(Q)$ will have a fractional coefficient, whose denominator will be divisible by the $t+\tau-1$ power of $p$, as will now be shown.

Let the terms in $(P)$ which precede $Gx^g$ be denoted $'Gx^{g+1}$, $''Gx^{g+2}$ etc. and let those which follow it be $G'x^{g-1}$, $G''x^{g-2}$ etc. Similarly in $\frac{(Q)}{p}$ let the terms preceding $\Gamma x^\gamma$ be $'\Gamma x^{\gamma+1}$,$''\Gamma x^{\gamma+2}$ etc. and the terms

[3]If two similar permutations are conceived to be written in a circle in such a way that the last thing is adjacent to the first, then there will be no difference between them at all, since no place can be called first or last

following it be $\Gamma' x^{\gamma+1}$, $\Gamma'' x^{\gamma+2}$ etc. Then it is clear that in the product of $(P)$ and $\frac{(Q)}{p}$, the coefficient of the term $x^{g+\gamma}$ will be

$$= G\Gamma +' G\Gamma' +'' G\Gamma'' + etc. \quad (4)$$
$$+' \Gamma G' +'' \Gamma G'' + etc. \quad (5)$$

The term $G\Gamma$ will be a fraction which, if expressed in smallest terms, has a denominator divisible by precisely the $t+\tau$ power of $p$. But if the remaining terms are factored, they will each involve a smaller power of $p$ than $t+\tau$, since they are all products of two factors, such that one involves a power of $p$ no greater than $t$ (or $\tau$) and the other of which involves a power of $p$ which is strictly smaller than $\tau$ (or $t$). Hence $G\Gamma$ will be of the form $\frac{e}{fp^{t+\tau}}$ and the sum of the rest will be of the form $\frac{e'}{f'p^{t+\tau-\delta}}$ where $\delta$ is positive and $e$, $f$, $f'$ are all relatively prime to $p$. Therefore, the sum of these will be $= \frac{ef'+e'fp^{\delta}}{ff'p^{t+\tau}}$, whose numerator is not divisible by $p$. Hence this fraction cannot be reduced in any way so that the denominator obtains a smaller power of $p$ than $t+\tau$. This implies that the coefficient of the term $x^{g+\gamma}$ in the product of $(P)$, $(Q)$ will be

$$= \frac{ef' + e'fp^{\delta}}{ff'p^{t+\tau-1}}$$

i.e. a *fraction*, whose denominator is divisible by at least the $t+\tau-1$ power of $p$. □

Art. 43

**Proposition 14.** *A congruence of the $m^{th}$ degree*

$$Ax^m + Bx^{m-1} + Cx^{m-2} + etc. + Mx + N \equiv 0$$

*whose modulus is a prime number $p$ that does not divide $A$, cannot be solved in more than $m$ different ways, or does not have more than $m$ distinct roots modulo $p$ (See Art. 25, 26).*

If anyone denies it, let us suppose that congruences of different degrees $m$, $n$ etc. are given which have more than $m$, $n$ etc. roots, and let $m$ be the smallest degree of all of these, so that all similar congruences of lower degrees are consistent with our theorem. Since it has already been demonstrated above (Art. 26) that the theorem holds for the first degree, it is clear that $m$ would need to be $= 2$ or greater. Let the congruence

$$Ax^m + Bx^{m-1} + \text{etc.} + Mx + N \equiv 0$$

admit at least $m+1$ roots, which are $x \equiv \alpha$, $x \equiv \beta$, $x \equiv \gamma$ etc., and suppose that all of the numbers $\alpha$, $\beta$, $\gamma$, etc. are positive and less than $p$, with the smallest being $\alpha$. Now, in the congruence proposed, let $y+\alpha$ be substituted for $x$, with the result being

$$A'y^m + B'y^{m-1} + C'y^{m-2} + \cdots + M'y + N' \equiv 0$$

Then it is clear that this congruence is satisfied if we put $y \equiv 0$, or $\equiv \beta - \alpha$, or $\equiv \gamma - \alpha$ etc., and these roots will all be distinct, with their number being $= m+1$. But from the fact that $y \equiv 0$ is a root, it follows that $N'$ is divisible by $p$. From this we obtain

$$y(A'y^{m-1} + B'y^{m-2} + \text{etc.} + M') \equiv 0 \text{ (mod. } p).$$

If $y$ is given one of the $m$ values $\beta - \alpha$, $\gamma - \alpha$ etc. which are all $> 0$ or $< p$, then in these cases

$$A'y^{m-1} + B'y^{m-2} + \text{ etc. } + M' \equiv 0 \text{ (Art. 22)}$$

i.e. the congruence

$$A'y^{m-1} + B'y^{m-2} + \text{ etc. } + M' \equiv 0,$$

which has degree $m-1$, has $m$ roots, contrary to our theorem (for it is easy to see that $A' = A$, and therefore it is not divisible by $p$, as required), even though we have assumed that all congruences of a lower degree than $m$ agree with the theorem.

Art. 44

Although we have assumed here that the modulus $p$ does not divide the highest order coefficient, the theorem is not restricted to this case. For if the first coefficient and even some of the following ones were divisible by $p$, these terms could safely be rejected, and the congruence would be reduced to a degree where the first coefficient would no longer be divisible by $p$. For not all coefficients can be divided by $p$; in this case the congruence would be an identity, and the unknown would be completely indeterminate.

This theorem was first proposed and demonstrated by Lagrange (*Mem. de l'Ac de Berlin, Année 1768 p.192*). It can also be found in the dissertation of Legendre, *Recherches d'Analyse indéterminée, Hist. de l'Acad. de Paris 1785 p. 466*, which showed that the congruence $x^n - 1 \equiv 0$ cannot have more than $n$ different roots. Although this is a particular case, the method used by the great man can easily be adapted to all congruences. A still more limited case had already been completed before, *Comm. nov. Ac. Petr. V p.6*, but these methods cannot be used in general. In section 8 below we will prove the theorem in yet another way; but no matter how different all these methods may seem at first glance, experts who wish to compare them will easily be convinced that they are all based on the same principle.

Finally, since this theorem is to be considered here only as a lemma, a complete exposition does not belong here: we will treat the case of a composite modulus elsewhere.