Annexe 1 : Extrait de la section première des Recherches Arithmétiques de Gauss

1. Si un nombre a divise la différence des nombres b et c, b et c sont dits *congrus* suivant a, sinon *incongrus*. a s'appellera le module ; chacun des nombres b et c, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est à dire, sans aucun signe.

Ainsi -9 et $+16$ sont *congrus* par rapport au module 5 ; -7 est *résidu* de 15 par rapport au module 11, et *non résidu* par rapport au module 3.

Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque.

2. Tous les résidus d'un nombre donné a suivant le module m sont compris dans la formule $a + km$, k étant un entier indéterminé. Les plus faciles des propositions que nous allons exposer peuvent sans peine se démontrer par là ; mais chacun en sentira la vérité au premier aspect.

Nous désignons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses ; ainsi $-16 \equiv 9\ (mod\ 5)$, $-7 \equiv 15\ (mod\ 11)$[2].

3. THEOREME : *Soient m nombres entiers successifs a, a+1, a+2, ..., a+m-1 et un autre A, un des premiers sera congru avec A, suivant le module m, et il n'y en aura qu'un.*
[*Démonstration*]

4. Il suit de là que chaque nombre aura un résidu, tant dans la suite $0, 1, 2, ..., (m-1)$, que dans celle-ci $0, -1, -2, ..., -(m-1)$; nous les appellerons résidus minima ; et il est clair qu'à moins que 0 ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif. S'ils sont inégaux, l'un d'eux sera $< \frac{m}{2}$; s'ils sont égaux, chacun d'eux $= \frac{m}{2}$ sans avoir égard au signe ; d'où il suit qu'un nombre quelconque a un résidu qui ne surpasse pas la moitié du module, et que nous appellerons résidu minimum absolu.

Par exemple -13 suivant le module 5, a pour résidu minimum positif 2, qui est en même temps minimum absolu, et -3 pour résidu minimum négatif ; $+5$ suivant le module 7, est lui-même son résidu minimum positif ; -2 est le résidu minimum négatif et en même temps le minimum absolu.

Annexe 2 : une citation extraite des Recherches Arithmétiques de Gauss (p.416)

Le problème où l'on se propose de distinguer les nombres premiers des nombres composés, [...], est connu comme un des plus importants et des plus utiles de toute l'Arithmétique ; [...]. En outre, la dignité de la science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre.

[2]Nous avons adopté ce signe à cause de la grande analogie qui existe entre l'égalité et la congruence. C'est pour la même raison que Legendre, dans des mémoires que nous aurons souvent occasion de citer, a employé le signe même de l'égalité, pour désigner la congruence ; nous en avons préféré un autre, pour prévenir toute ambiguité.

Annexe 2 : Extraits de la section Quatrième *"Des Congruences du second degré"* des Recherches Arithmétiques

On ne fait ici que recopier des extraits de la section Quatrième des Recherches Arithmétiques qu'il faudrait bien maîtriser pour pouvoir démontrer que l'existence d'un décomposant de Goldbach pour chaque nombre pair découle de l'existence d'au moins une solution pour un certain système de congruences (ou incongruences, c'est quasiment l'opposé) quadratiques, cette dernière existence découlant quant à elle du théorème d'or appliqué aux nombres adéquats. Les articles les plus difficiles, mais peut-être les plus utiles pour notre problème sont **les articles** 104 **et** 105 puis 147**,** 148 **et** 149.

page 69, article 94 : THÉORÈME. Un nombre quelconque m étant pris pour module, il ne peut y avoir dans la suite $1, 2, 3 \ldots m-1$, plus de $\frac{1}{2}m+1$ nombres, quand m est pair, et plus de $\frac{1}{2}m+\frac{1}{2}$, quand m est impair, qui soient congrus à un carré.

page 70, article 96 : Le nombre premier p étant pris pour module, la moitié des nombres $1, 2, 3 \ldots p-1$, sera composée de résidus quadratiques, et l'autre moitié de non-résidus, c'est-à-dire qu'il y aura $\dfrac{1}{2}(p-1)$ résidus, et autant de non-résidus.

page 72, article 98 : THÉORÈME. Le produit de deux résidus quadratiques d'un nombre premier p est un résidu ; le produit d'un résidu et d'un non-résidu est non-résidu ; enfin le produit de deux non-résidus est résidu.
1°. Soient A et B les résidus qui proviennent des carrés a^2, b^2, ou soient $A \equiv a^2 \ (mod\ p)$ et $B \equiv b^2$, on aura $AB \equiv a^2b^2$, c'est-à-dire qu'il sera un résidu.
2°. Quand A est résidu, ou que $A \equiv a^2$, mais que B est non-résidu, AB est non-résidu. Soit en effet, s'il se peut $AB \equiv k^2$ et $\frac{k}{a} \ (mod\ p) \equiv b$, on aura $a^2B \equiv a^2b^2$ et partant $B \equiv b^2$, contre l'hypothèse.
Autrement. Si l'on multiplie par A les $\frac{p-1}{2}$ nombres de la suite $1, 2, 3 \ldots p-1$, qui sont résidus, tous les produits seront des résidus quadratiques, et ils seront tous incongrus. Or si l'on multiplie par A un nombre B non-résidu, le produit ne sera congru à aucun des précédents : donc, s'il était résidu, il y aurait $\frac{1}{2}(p+1)$ résidus incongrus, parmi lesquels ne serait pas 0, ce qui est impossible (n^o 96).
3°. Soient A et B deux nombres non-résidus, en multipliant par A tous les nombres qui sont résidus dans la suite $1, 2, 3, \ldots p-1$, on aura $\frac{p-1}{2}$ non-résidus, incongrus entr'eux (2°). Or le produit AB ne peut être congru à aucun de ceux-là ; donc s'il était non-résidu, on aurait $\frac{p+1}{2}$ non-résidus incongrus entr'eux ; ce qui est impossible (n^o 96).
Ces théorèmes se déduisent encore plus facilement des principes de la section précédente. En effet, puisque l'indice d'un résidu est toujours pair, et celui d'un non-résidu toujours impair, l'indice du produit de deux résidus ou non-résidus sera pair, et partant, le produit sera lui-même un résidu. Au contraire, si l'un des facteurs est non-résidu, et l'autre résidu, l'indice sera impair, et le produit non-résidu.
On peut aussi faire usage des deux méthodes pour démontrer ce THÉORÈME[9] : *la valeur de l'expression* $\frac{a}{b} \ (mod\ p)$*, sera un résidu, quand les nombres a et b seront tous les deux résidus ou non-résidus. Elle sera un non-résidu, quand l'un des nombres a et b sera résidu et l'autre non-résidu.* On le démontrerait encore en renversant les théorèmes précédents.

page 73, article 99 : Généralement, le produit de tant de facteurs qu'on voudra est un résidu, soit lorsque tous les facteurs en sont eux-mêmes, soit lorsque le nombre de facteurs non-résidus est pair ; mais quand le nombre des facteurs non-résidus est impair, le produit est non-résidu. On peut donc juger facilement si un nombre composé est résidu ou non ; pourvu qu'on sache ce que sont ses différents facteurs. Aussi dans la Table II, nous n'avons admis que les nombres premiers. Quant à sa disposition, les modules sont en marge[10], en tête les nombres premiers successifs ; quand l'un de ces derniers est résidu, on a placé un trait dans l'espace qui correspond au module et à ce nombre ; quand il est non-résidu, on a laissé l'espace vide.

page 73, article 100 : Si l'on prend pour module la puissance p^n d'un nombre premier, p étant > 2, une moitié des nombres non-divisibles par p et $< p^n$ seront des résidus, et l'autre des non-résidus ; c'est-à-dire

[9] Ici, je mets les petites capitales à ce mot bien qu'elles ne soient pas présentes dans les Recherches Arithmétiques dans la mesure où la démonstration de ce théorème n'est pas fournie.
[10] On verra bientôt comment on peut se passer des modules composés.

qu'il y en aura $\frac{p-1}{2}.p^{n-1}$ de chaque espèce.
En effet, si r est un résidu, il sera congru à un carré dont la racine ne surpasse pas la moitié du module (n^o 94) ; et l'on voit facilement qu'il y a $\frac{1}{2}p^{n-1}(p-1)$ nombres $< \frac{p^n}{2}$ et non-divisibles par p. Ainsi il reste à démontrer que les carrés de tous ces nombres sont incongrus, ou qu'ils donnent des résidus différents. Or si deux nombres a et b non-divisibles par p et plus petits que la moitié du module, avaient leurs carrés congrus, on aurait $a^2 - b^2$ ou $(a+b)(a-b)$ divisible par p^n, en supposant $a > b$, ce qui est permis. Mais cette condition ne peut avoir lieu, à moins que l'un des deux nombres $(a-b)$, $(a+b)$ ne soit divisible par p^n, ce qui est impossible, puisque chacun d'eux est plus petit que p^n, ou bien que l'un étant divisible par p^μ, l'autre le soit par $p^{\nu-\mu}$ ou chacun d'eux par p ; ce qui est encore impossible, puisqu'il s'ensuivrait que la somme $2a$ et la différence $2b$, et partant a et b eux-mêmes seraient divisibles par p, contre l'hypothèse. Donc enfin parmi les nombres non-divisibles par p et moindres que le module, il y a $\frac{p-1}{2}p^{n-1}$ résidus, et les autres, en même nombre, sont non-résidus.

page 74, article 101 : Tout nombre non-divisible par p, qui est résidu de p, sera aussi résidu de p^n ; celui qui ne sera pas résidu de p ne le sera pas non plus de p^n.
La seconde partie de cette proposition est évidente par elle-même ; ainsi si la première n'était pas vraie, parmi les nombres plus petits que p^n et non-divisibles par p, il y en aurait plus qui fussent résidus de p qu'il n'y en aurait qui le fussent de p^n, c'est-à-dire plus de $\frac{1}{2}p^{n-1}(p-1)$. Mais on peut voir sans peine que le nombre des résidus de p qui se trouvent entre 1 et p^n, est précisément $\frac{1}{2}p^{n-1}(p-1)$.
Il est tout aussi facile de trouver effectivement un carré qui soit congru à un résidu donné, suivant le module p^n, si l'on connaît un carré congru à ce résidu suivant le module p.
Soit en effet a^2 un carré congru au résidu donné A, suivant le module p^μ, on en déduira, de la manière suivante, un carré $\equiv A$, suivant le module p^ν, ν étant $> \mu$ et non plus grand que 2μ. Supposons que la racine du carré cherché soit $\pm a + xp^\mu$; et il est aisé de s'assurer que c'est là la forme qu'elle doit avoir. Il faut donc qu'on ait $a^2 \pm 2axp^\mu + x^2p^{2\mu} \equiv A \ (mod\ p^\nu)$, ou comme $2\mu > \nu$, on aura $\pm 2axp^\mu \equiv A - a^2 \ (mod\ p^\nu)$. Soit $A - a^2 = p^\mu.d$, on aura $\pm 2ax \equiv d \ (mod\ p^{\nu-\mu})$; donc x sera la valeur de l'expression $\pm\frac{d}{2a} \ (mod\ p^{\nu-\mu})$. Ainsi étant donné un carré congru à A, suivant le module p, on en déduira un carré congru à A, suivant le module p^2 ; de là au module p^4, au module p^8, etc.
Exemple. Etant proposé le résidu 6 congru au carré 1, suivant le module 5, on trouve le carré 9^2 auquel il est congru suivant le module 25, 16^2 auquel il est congru suivant le module 125, etc.

page 75, article 102 : Quant à ce qui regarde les nombres divisibles par p, il est clair que leurs carrés seront divisibles par p^2, et que partant tous les nombres qui seront divisibles par p et non par p^2, seront non-résidus de p^n. Et en général, si l'on propose le nombre p^kA, A n'étant pas divisible par p, il y aura trois cas à distinguer :
1°. Si $k \geq n$, on aura $p^kA \equiv 0 \ (mod\ p^n)$, c'est-à-dire qu'il sera résidu.
2°. Si $k < n$ et impair, p^kA sera non-résidu.
3°. Si $k < n$ et pair, p^kA sera résidu ou non-résidu de p^n suivant que A sera résidu ou non-résidu de p.

page 76, article 103 : Comme nous avons commencé (n^o 100) par exclure le cas où $p = 2$, il faut ajouter quelque chose à ce sujet. Quand 2 est module, tous les nombres sont résidus, et il n'y en a point de non-résidus. Quand le module est 4, tous les nombres impairs de la forme $4k+1$ sont résidus, et tous ceux de la forme $4k+3$ sont non-résidus. Enfin, quand le module est 8 ou une plus haute puissance de 2, tous les nombres impairs de la forme $8k+1$ sont résidus, et les autres, ou ceux de la forme $8k+3$, $8k+5$, $8k+7$ sont non-résidus ;

page 77, article 104 : Pour ce qui regarde le nombre de valeurs différentes, c'est-à-dire incongrues suivant le module, que peut admettre l'expression $V = \sqrt{A} \ (mod\ p^n)$, pourvu que A soit un résidu de p^n, on déduit facilement de ce qui précède, les conclusions suivantes. Nous supposons toujours que p est un nombre premier et, pour abréger, nous considérons en même temps le cas où $n = 1$.
1^o. Si A n'est pas divisible par p, V n'a qu'une seule valeur pour $p = 2$ et $n = 1$; ce sera $V \equiv 1$; il en a deux quand p est impair, ou bien quand on a $p = 2$ et $n = 2$; et, si l'une est $\equiv \nu$, l'autre sera $\equiv -\nu$; il en a quatre pour $p = 2$ et $n > 2$; et si l'une est $\equiv \nu$, les autres seront $\equiv \nu + 2^{n-1}, -\nu + 2^{n-1}, -\nu$.
2^o. Si A est divisible par p, mais non par p^n, soit $p^{2\mu}$ la plus haute puissance de p qui divise A, car

cette puissance doit être paire (n^o 102), et $A = ap^{2\mu}$; il est clair que toutes les valeurs de V doivent être divisibles par p^μ, et que tous les quotients donnés par ces divisions seront les valeurs de l'expression $V' = \sqrt{a}\ (mod\ p^{n-2\mu})$; on aura donc toutes les valeurs différentes de V, en multipliant par p^μ, toutes celles de V' contenues entre 0 et $p^{n-\mu}$. Elles seront, par conséquent,
$\nu p^\mu, \nu p^\mu + p^{n-\mu}, \nu p^\mu + 2p^{n-\mu}, \ldots \nu p^\mu + (p^\mu - 1)p^{n-\mu}$,
ν étant une valeur quelconque de V : suivant donc que V' aura 1, ou 2, ou [11] valeurs, V en aura p^μ, ou $2p^\mu$ ou $4p^\mu$ (1^o).
3^o. Si A est divisible par p^n, on voit facilement, en posant $n = 2m$ ou $= 2m - 1$, suivant que n est pair ou impair, que tous les nombres divisibles par p^m sont des valeurs de V, et qu'il n'y en a pas d'autres ; mais les nombres divisibles par p^m sont $0, p^m, 2p^m \ldots (p^{n-m} - 1)p^m$, dont le nombre est p^{n-m}.

page 78, article 105 : Il reste à examiner le cas où le module m est composé de plusieurs modules premiers. Soit $m = abc\ etc.$, a, b, c, *etc.* étant des nombres premiers différents. Il est clair d'abord que si n est résidu de m, il le sera aussi des différents nombres, a, b, c, *etc.*, et que partant il sera non-résidu de m, s'il est non-résidu de quelqu'un de ces nombres. Réciproquement, si n est résidu des différents nombres a, b, c, *etc.*, il le sera de leur produit m ; en effet, si l'on a $n \equiv A^2, B^2, C^2, etc.$, suivant les modules a, b, c, *etc.*, respectivement (n^o 32), on aura $n \equiv N^2$, suivant tous ces modules, et conséquemment suivant leur produit.
Comme on voit facilement que la valeur de N résulte de la combinaison d'une valeur quelconque de A, ou de l'expression $\sqrt{n}\ (mod\ a)$, avec une valeur quelconque de B, avec une valeur quelconque de C, *etc*, que les différentes combinaisons donneront des valeurs différentes, et qu'elles les donneront toutes ; le nombre des valeurs de N sera égal au produit des nombres de valeurs de A, B, C, *etc.* que nous avons appris à déterminer dans l'article précédent.

page 78, article 106 : On voit par ce qui précède, qu'il suffit de reconnaître si un nombre donné est résidu ou non-résidu d'un nombre premier donné, et que tous les cas reviennent à celui-là.
Un nombre quelconque A, non divisible par un nombre premier $2m + 1$, est résidu ou non-résidu de ce nombre premier suivant que $A^m \equiv +1 ou \equiv -1\ (mod\ 2m + 1)$.

page 80, article 109 : en effet, il est évident que si r est un résidu, $\dfrac{1}{r}\ (mod\ p)$ en sera un aussi.

(Les **articles** 108 **à** 124 **des pages** 79 **à** 91 traitent des cas particuliers 1, -1, 2, -2, 3, -3, 5, -5, 7 et -7.)

page 81, article 111 : Si donc r est résidu d'un nombre premier de la forme $4n + 1$, $-r$ le sera aussi, et tous les non-résidus seront encore non-résidus en changeant les signes[12]. Le contraire arrive pour les nombres premiers de la forme $4n + 3$, dont les résidus deviennent non-résidus, et réciproquement quand on change le signe (n^o 98).
Au reste on déduit facilement de ce qui précède cette règle générale : -1 est résidu de tous les nombres qui ne sont divisibles ni par 4, ni par aucun nombre de la forme $4n + 3$. Il est non-résidu de tous les autres.(N^{os} 103 *et* 105).

page 81, article 112 : Passons maintenant aux résidus $+2$ et -2.
Si dans la table II on prend tous les nombres premiers dont le module est $+2$, on trouvera $7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97$. Or on remarque facilement qu'aucun d'eux n'est de la forme $8n + 3$ ou $8n + 5$.
Voyons donc si cette induction peut devenir une certitude.
Observons d'abord que tout nombre composé de la forme $8n + 3$ ou $8n + 5$ renferme nécessairement un facteur premier de l'une ou l'autre forme ; en effet les nombres premiers de la forme $8n + 1$ et $8n + 7$ ne peuvent former que des nombres de la forme $8n + 1$ ou $8n + 7$. Si donc notre induction est généralement vraie, il n'y aura aucun nombre de la forme $8n + 3$, $8n + 5$, dont le résidu soit $+2$. Or il est bien certain qu'il n'existe aucun nombre de cette forme et au-dessous de 100, dont le résidu soit $+2$; mais s'il y en avait au-dessus de cette limite, supposons que t soit le plus petit de tous ; t sera de la forme $8n + 3$ ou $8n + 5$, et $+2$ sera son résidu ; mais il sera non-résidu de tous les nombres semblables plus petits. Soit $a^2 \equiv 2\ (mod\ t)$, on pourra toujours prendre a impair et $< t$, car a a au moins deux valeurs positives plus

[11] ici, je crois qu'il manque un mot, le chiffre 4 ?
[12] Ainsi quand nous parlerons d'un nombre, en tant qu'il sera résidu ou non-résidu d'un nombre de la forme $4n + 1$, nous pouvons ne faire aucune attention à son signe, ou lui donner le signe $\pm$.

petites que t, dont la somme $= t$, et dont par conséquent l'une est paire et l'autre impaire (N^{os} 104, 105). Cela posé, soit $a^2 = 2 + ut$ ou $ut = a^2 - 2$, a^2 sera de la forme $8n + 1$, et par-conséquent ut de la forme $8n - 1$; donc u sera de la forme $8n + 3$ ou $8n + 5$ suivant que t sera de la forme $8n + 5$ ou $8n + 3$; mais de l'équation $a^2 = 2 + tu$, on tire la congruence $a^2 \equiv 2(mod\ u)$, c'est-à-dire que $+2$ serait aussi résidu de u. Il est aisé de voir qu'on a $u < t$; il s'ensuivrait que t ne serait pas le plus petit nombre qui eût $+2$ pour résidu, ce qui est contre l'hypothèse ; d'où suit enfin une démonstration rigoureuse de cette proposition que nous avions déduite de l'induction.
En combinant cette proposition avec celles du n^o 111, on en déduit les théorèmes suivants :
I. $+2$ est non-résidu, et -2 est résidu de tous les nombres premiers de la forme $8n + 3$.
II. $+2$ et -2 sont non-résidus de tous les nombres premiers de la forme $8n + 5$.

page 82, article 113 : Par une semblable induction on tirera de la Table II, pour les nombres premiers dont le résidu est -2, ceux-ci : $3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97$[13]. Parmi ces nombres il ne s'en trouve aucun de la forme $8n + 5$ ou $8n + 7$; cherchons donc si de cette induction nous pouvons tirer un théorème général. On fera voir de la même manière que dans l'article précédent, qu'un nombre composé de la forme $8n + 5$ ou $8n + 7$, doit renfermer un facteur premier de la forme $8n + 5$ ou de la forme $8n + 7$; de sorte que si notre induction est généralement vraie, -2 ne peut être résidu d'aucun nombre de la forme $8n + 5$ ou $8n + 7$; or s'il peut y en avoir de tels, soit t le plus petit de tous, et qu'on ait $-2 = a^2 - tu$. Si l'on prend, comme plus haut, a impair et $< t$, u sera de la forme $8n + 5$ ou $8n + 7$ suivant que t sera de la forme $8n + 7$ ou $8n + 5$; mais de ce qu'on a $a < t$ et $ut = a^2 + 2$, il est facile de déduire que u est $< t$; et comme -2 serait aussi résidu de u, il s'ensuivrait que t ne serait pas le plus petit nombre dont -2 est le résidu, ce qui est contre l'hypothèse. Donc -2 sera nécessairement non-résidu de tous les nombres de la forme $8n + 5$ ou $8n + 7$.
En combinant cette proposition avec celles du n^o 111, on en déduit les théorèmes suivants :
I. -2 et $+2$ sont non-résidus de tous les nombres premiers de la forme $8n + 5$; comme nous l'avons déjà trouvé.
II.-2 est non-résidu et $+2$ résidu de tous les nombres premiers de la forme $8n + 7$.
Au reste, nous aurions pu prendre a pair dans les deux démonstrations ; mais alors il eût fallu distinguer le cas où a est de la forme $4n + 2$, de celui où il est de la forme $4n$; d'ailleurs la marche est absolument la même et n'est sujette à aucune difficulté.

page 83, article 114 : Il nous reste encore à traiter le cas où le nombre premier est de la forme $8n + 1$; mais il échappe à la méthode précédente et demande des artifices tout-à-fait particuliers.
Soit, pour le module premier $8n+1$, une racine primitive quelconque a, on aura (n^o 62) $a^{4n} \equiv -1\ (mod\ 8n+1)$; cette congruence peut se mettre sous la forme $(a^{2n} + 1)^2 \equiv 2a^{2n}\ (mod\ 8n + 1)$, ou $(a^{2n} - 1)^2 \equiv -2a^{2n}$; d'où il suit que $2a^{2n}$ et $-2a^{2n}$ sont résidus de $8n + 1$; mais comme a^{2n} est un carré non-divisible par le module, $+2$ et -2 seront aussi résidus (n^o 98).

page 84, article 116 : Au reste on tire facilement de ce qui précède la règle générale suivante : $+2$ est résidu de tout nombre qui n'est divisible ni par 4 ni par aucun nombre premier de la forme $8n + 3$ ou $8n+5$, et non-résidu de tous les autres, par exemple, de tous ceux de la forme $8n+3$, $8n+5$, tant premiers que composés.

page 91, article 125 : Tout nombre premier de la forme $4n + 1$ soit positif, soit négatif, est non-résidu de quelques nombres premiers, et même de nombres premiers plus petits que lui (il est évident qu'il faut éviter $+1$).

page 95, article 129 : Théorème. Si a est un nombre premier de la forme $8n+1$, il y aura nécessairement au-dessous de $2\sqrt{a}$ un nombre premier dont a est non-résidu.

page 95, article 130 : Maintenant que nous avons démontré que tout nombre premier de la forme $4n+1$ positif ou négatif, est toujours non-résidu d'un nombre premier au moins plus petit que lui...

page 98, au milieu du article 132 : mais, avant tout, il faut observer que tout nombre de la forme $4n + 1$ ne renfermera aucun facteur de la forme $4n + 3$, ou en renfermera un nombre pair parmi lesquels

[13]En considérant -2 comme le produit de $+2$ par -1 ; voyez n^o 111.

il pourra y en avoir d'égaux ; tandis que tout nombre de la forme $4n+3$ doit en renfermer un nombre impair. Le nombre des facteurs de la forme $4n+1$ reste indéterminé.

pages 108 et suiv., articles 146 à 150 : Au moyen du théorème fondamental [14] et des propositions relatives à -1, ± 2, on peut toujours déterminer si un nombre donné quelconque est résidu ou non-résidu d'un nombre premier donné.

Ensuite, dans l'**article 146**, Gauss généralise et explique la méthode permettant, étant donnés deux nombres quelconques P et Q, de trouver si l'un d'eux est résidu ou non-résidu de l'autre. Pour cela, il étudie la relation qui lie Q à chaque puissance de premier qui intervient dans la factorisation de P. Ce qui retient l'attention, c'est le début du point III de cet article 146, qui explique comment s'effectue le passage du second degré au premier degré :
On cherchera de la manière suivante la relation d'un nombre quelconque Q à un nombre premier a impair : quand $Q > a$, on substituera à Q son *résidu minimum positif* suivant le module a, ou, ce qui est quelquefois avantageux, son *résidu minimum absolu*, qui aura avec a la même relation que Q.
Or si l'on résoud Q, ou le nombre pris à sa place, en facteurs premiers p, p', p'', *etc.*, auxquels il faut joindre le facteur -1, quand Q est négatif, il est évident que la relation de Q à a dépendra de la relation des facteurs p, p', p'', *etc.* à a : de sorte que, si parmi eux il y en a $2m$ non-résidus de a, on aura QRa[15] ; mais s'il y en a $2m+1$, on aura QNa. Au reste, on voit facilement que si parmi les facteurs p, p', p'', *etc.*, il y en a un nombre pair d'égaux entre eux, on peut les rejeter, puisqu'ils n'influent en rien sur la relation de Q à a.

Dans les **articles** 147**,** 148 **et** 149, Gauss résoud le problème suivant : Etant proposé un nombre quelconque A, on peut trouver certaines formules qui contiennent tous les nombres premiers à A dont A est résidu, ou tous ceux qui sont diviseurs des nombres de la forme $x^2 - A$, x^2 étant un carré indéterminé. Nous appellerons simplement ces nombres *diviseurs* de $x^2 - A$; l'on voit facilement ce que sont les *non-diviseurs*. Mais pour abréger nous ne considérerons que les diviseurs qui sont impairs et premiers à A, les autres cas se ramenant sans peine à celui-là.

On recopie intégralement ces trois articles qui nous semblent très liés à l'idée que l'on cherche à développer.

Suite de l'article 147, page 110 : Soit d'abord A un nombre premier positif de la forme $4n+1$, ou négatif de la forme $4n-1$. Suivant le théorème fondamental, tous les nombres premiers qui, pris positivement, sont résidus de A, seront diviseurs de $x^2 - A$; mais tous les nombres premiers non-résidus de A seront non-diviseurs de $x^2 - A$, si pourtant on en excepte 2, qui est toujours diviseur. Soient r, r', r'', *etc.*, tous les résidus de A qui sont plus petits que lui, et n, n', n'', *etc.*, tous les non-résidus ; alors tout nombre premier contenu dans une des formes $Ak+r$, $Ak+r'$, $Ak+r''$, *etc.*, sera diviseur de $x^2 - A$; mais tout nombre premier contenu dans une des formes $Ak+n$, $Ak+n'$, *etc.*, sera non-diviseur de $x^2 - A$, k étant un nombre entier indéterminé. Nous appellerons les premières *formes des diviseurs* de $x^2 - A$ et les dernières *formes des non-diviseurs*. Le nombre de chacune d'elles sera égal au nombre de résidus r, r', *etc.* ou de non-résidus n, n', *etc.*, et partant, $(n^o\ 96) = \frac{1}{2}(A-1)$. Or si B est un nombre composé impair et que l'on ait ARB, tous les facteurs premiers de B seront contenus dans une des premières formes, et par conséquent, B lui-même ; donc tout nombre composé impair qui sera contenu dans la forme des non-diviseurs sera non-diviseur de $x^2 - A$; mais on ne peut pas dire que les non-diviseurs de $x^2 - A$ sont tous compris dans la forme des non-diviseurs, car en supposant B non-diviseur de $x^2 - A$, et si le nombre de ces facteurs est pair, B sera compris dans quelque forme de diviseurs (n^o 93).
Ainsi, soit $A = -11$; on trouvera que les formes des diviseurs de $x^2 + 11$ sont $11k+1$, 2, 3, 4, 5, 9, et que celles des non-diviseurs sont $11k+2$, 6, 7, 8, 10. Ainsi -11 sera résidu de tous les nombres premiers contenus dans une des premières formes et non-résidu de ceux qui sont contenus dans une des dernières.
On peut trouver des formes semblables pour les diviseurs et les non-diviseurs de $x^2 - A$, quel que soit A ; mais on voit aisément qu'on n'a à considérer que les valeurs de A qui ne sont divisibles par aucun carré ; car si $A = a^2A'$, tous les diviseurs de $x^2 - A$ premiers avec A, seront diviseurs de $x^2 - A'$, et de même pour les non-diviseurs. Or nous distinguerons trois cas : 1°. quand A est de la forme $4n+1$ ou $-(4n-1)$; 2°. quand A est de la forme $4n-1$ ou $-(4n+1)$; 3°. quand A est pair ou de la forme $\pm(4n+2)$.

[14] communément appelé actuellement la *"loi de réciprocité quadratique"*.
[15] Gauss utilise la lettre R pour signifier *"est résidu quadratique de"* et la lettre N pour signifier *"est non-résidu quadratique de"*.

page 111, article 148 : *Premier cas.* Quand A est de la forme $4n+1$ ou $-(4n-1)$. On résoudra A en facteurs premiers a, b, c, d, *etc.*, en affectant du signe + ceux de la forme $4n+1$, et du signe − ceux de la forme $4n-1$ qui seront en nombre pair ou impair, suivant que A sera de la forme $4n+1$ ou $-(4n-1)$ (n^o 132). On distribuera en deux classes les nombres plus petits que A et premiers avec lui ; en mettant dans la première ceux qui ne sont non-résidus d'aucun diviseur de A, ou qui sont non-résidus d'un nombre pair de ces diviseurs, et dans la seconde ceux qui sont non-résidus d'un nombre impair des mêmes diviseurs. Désignons les premiers par r, r', r'', *etc.* et les seconds par n, n', n'', *etc.* ; alors $Ak+r$, $Ak+r'$, *etc.* sont les formes des diviseurs de x^2-A, et $Ak+n$, $Ak+n'$, *etc.* celles des non-diviseurs. C'est-à-dire que tout nombre premier, excepté 2, sera diviseur ou non-diviseur de x^2-A, suivant qu'il sera contenu dans l'une des premières ou l'une des dernières formes.
En effet, si p est un nombre premier résidu ou non-résidu d'un des facteurs de A, ce facteur sera résidu ou non-résidu de p (théor. fond.) ; donc si parmi les facteurs de A, il y en a m dont p soit non-résidu, il y en aura autant qui seront non-résidus de p, et partant, lorsque p sera contenu dans l'une des premières formes, m sera pair et ARp, et lorsque p sera contenu dans une des dernières, p sera impair et ANp.
Exemple. Soit $A=+105=(-3)\times(+5)\times(-7)$[16] ;
les nombres r, r', r'', *etc.* sont :
1, 4, 16, 46, 64, 79, qui ne sont non-résidus d'aucun facteur. ;
2, 8, 23, 32, 53, 92, qui sont non-résidus de 3 et 5 ;
26, 41, 59, 89, 101, 104, ... 3 et 7 ;
23, 52, 73, 82, 97, 103, ... 5 et 7 ;
les nombres n, n', n'', *etc.* sont :
11, 29, 44, 71, 74, 86, non-résidus de 3 ;
22, 37, 43, 58, 67, 88, ... de 5 ;
19, 31, 34, 61, 76, 94, ... de 7 ;
17, 38, 47, 62, 68, 83, ... de 3, 5 et 7 ;
On déduit facilement de la théorie des combinaisons et des $n^{os}(32,96)$ que la multitude des nombres r, r', *etc.* sera

$$t\Big(1+\frac{l(l-1)}{1.2}+\frac{l(l-1)(l-2)(l-3)}{1.2.3.4}+etc.\Big)$$

et celle des nombres n, n', *etc.*

$$t\Big(l+\frac{l(l-1)(l-2)}{1.2.3}+\frac{l(l-1)(l-2)(l-3)(l-4)}{1.2.3.4.5}+etc.\Big)$$

l désignant le nombre des facteurs a, b, c, d, *etc.*, t étant
$=2^{-l}(a-1)(b-1)(c-1)etc.$, et chaque série devant être continuée jusqu'à ce qu'elle s'arrête d'elle-même. (En effet il y a t nombres résidus de a, b, c, d, *etc.*, $t.\frac{l.(l-1)}{1.2}$ non-résidus de deux de ces facteurs, etc. Mais pour abréger, nous sommes forcés de ne pas donner plus de développement à la démonstration). Or chacune des séries a pour somme $l.2^{l-1}$; car la première provient de
$1+\frac{l-1}{1}+\frac{(l-1)(l-2)}{1.2}+\frac{(l-1)(l-2)(l-3)}{1.2.3}+etc.$ en prenant le premier terme, puis la somme du second et du troisième, puis la somme du quatrième et du cinquième, etc. : la seconde provient aussi de la même série, en joignant le premier terme au second, le troisième au quatrième, etc. Il y a donc autant de formes de diviseurs de x^2-A, que de formes de non-diviseurs ; et ils sont en nombre $2^{l-1}.t$ de chaque espèce, ou $\frac{1}{2}(a-1)(b-1)(c-1)(d-1)etc.$

page 113, article 149 : Nous pouvons traiter ensemble le second et le troisième cas. En effet on pourra toujours poser $A=(-1)Q$, ou $=(+2)Q$, ou $=(-2)Q$, Q étant un nombre de la forme $4n+1$ ou $-(4n-1)$. Soit généralement $A=\alpha Q$, de sorte que α soit ou -1 ou ± 2. Alors A sera résidu de tout nombre dont α et Q seront tous deux résidus, ou tous deux non-résidus : au contraire il sera non-résidu de tout nombre dont l'un d'eux seulement sera non-résidu. De là on déduit sans peine les formes des diviseurs et des non-diviseurs de x^2-A. Si $\alpha=-1$; nous partagerons tous les nombres plus petits que $4A$ et premiers avec lui, en deux classes. La première renfermera ceux qui sont dans quelque forme des diviseurs de x^2-Q, et en même temps de la forme $4n+1$, et aussi ceux qui sont dans quelque forme des non-diviseurs de x^2-Q et en même temps de la forme $4n-1$: la seconde renfermera tous les autres. Soient r, r', r'', *etc.* les premiers et n, n', n'', *etc.* les derniers ; A sera résidu de tous les nombres premiers contenus dans une

[16] Cela peut surprendre d'utiliser ainsi des nombres négatifs dans la factorisation mais Gauss explique qu'il affecte systématiquement les nombres premiers de la forme $4n+3$ du signe − et ceux de la forme $4n+1$ du signe + à cause de leur comportement démontré par le théorème fondamental.

des formes $4Ak+r$, $4Ak+r'$, $4Ak+r''$, *etc.*, et non-résidu de tous les nombres premiers contenus dans une des formes $4Ak+n$, $4Ak+n'$, $4Ak+n''$, *etc.* Si $\alpha = \pm 2$, nous distribuerons tous les nombres plus petits que $8Q$ et premiers avec lui en deux classes : la première renfermera tous ceux qui sont contenus dans quelque forme des diviseurs de $x^2 - Q$, et qui sont de la forme $8n+1$ ou $8n+7$, pour le signe supérieur, et de la forme $8n+1$ ou $8n+3$ pour le signe inférieur ; cette classe comprendra aussi tous ceux qui sont contenus dans quelque forme de non-diviseurs de $x^2 - Q$ et qui sont, pour le signe supérieur, de la forme $8n+3$, $8n+5$, et pour le signe inférieur, de la forme $8n+5$, $8n+7$, et la seconde tous les autres. Alors désignant les nombres de la première classe par r, r', r'', *etc.*, ceux de la seconde par n, n', n'', *etc.*, $\pm 2Q$ sera résidu de tous les nombres premiers contenus dans les formes $8Qk+r$, $8Qk+r'$, $8Qk+r''$, *etc.* et non-résidu de tous ceux contenus dans les formes $8Qk+n$, $8Qk+n'$, $8Qk+n''$, *etc.* Au reste, on peut démontrer facilement qu'il y a autant de formes de diviseurs qu'il y en a de non-diviseurs.
Exemple. On trouve ainsi que 10 est résidu de tous les nombres premiers contenus dans les formes $40K+1$, $+3$, $+9$, $+13$, $+27$, $+31$, $+37$, $+39$, et non-résidu de tous les nombres premiers contenus dans les formes $40K+7$, $+11$, $+17$, $+19$, $+21$, $+23$, $+29$, $+33$.

page 114, article 150 : Ces formes ont plusieurs propriétés assez remarquables ; nous n'en citerons cependant qu'une seule. Si B est un nombre composé premier avec A, tel qu'un nombre $2m$ de ses facteurs premiers soient compris dans quelque forme de non-diviseurs de $x^2 - A$, B sera contenu dans quelque forme de diviseurs de $x^2 - A$; mais si le nombre de facteurs premiers de B contenus dans quelque forme de non-diviseurs de $x^2 - A$ est impair, B sera aussi contenu dans quelque forme de non-diviseurs. Nous omettons la démonstration, qui n'a rien de difficile[17]. Il suit de là que non-seulement tout nombre premier ; mais aussi tout nombre composé impair et premier avec A est non-diviseur dès qu'il est contenu dans une des formes de non-diviseur ; car nécessairement quelque facteur premier de ce nombre sera non-diviseur.

page 116, article 152 : Jusqu'à présent nous n'avons traité que la congruence simple $x^2 \equiv A (mod\ m)$, et nous avons appris à reconnaître les cas où elle est résoluble. Par le n^o 105, la recherche des racines elles-mêmes est ramenée au cas où m est un nombre premier, ou une puissance d'un nombre premier ; et par le n^o 101, ce dernier cas est ramené à celui où m est un nombre premier. Quant à celui-ci, en comparant ce que nous avons dit (n^{os} 61 et suiv.) avec ce que nous enseignerons sect. V et VIII, on aura presque tout ce qui peut se faire par les méthodes générales. Mais dans les cas où elles sont applicables, elles sont infiniment plus longues que les méthodes indirectes que nous exposerons dans la section VI, et partant elles sont moins remarquables par leur utilité dans la pratique que par leur beauté.

Annexe 3 : Deux extraits de la lettre de Carl Frédéric Gauss à Sophie Germain du 30 avril 1807 (extrait des Oeuvres philosophiques de Sophie Germain, 1879, p. 274-282)

Voici une autre proposition relative aux residus quarrés, dont la demonstration est moins cachée : je ne l'ajoute pas, pour ne pas vous derober le plaisir de la developper vous-même, si vous la trouverez digne d'occuper quelques moments de votre loisir.
Soit p un nombre premier. Soient les $p-1$ nombres inférieurs à p partagés en deux classes :
A.....$1, 2, 3, 4....\frac{1}{2}(p-1)$
B.....$\frac{1}{2}(p+1), \frac{1}{2}(p+3), \frac{1}{2}(p+5), ...p-1$ Soit a un nombre quelconque non divisible par p. Multipliés tous les nombres A par a; prenés-en les moindres residus selon le module p, soient, entre ces residus, α appartenants à A, et β appartenants à B, de sorte que $\alpha + \beta = \frac{1}{2}(p-1)$. Je dis que a è residu quarré de p lorsque β è pair, non residu lorsque β è impair.

Le second extrait est davantage *"connu"*

Le goût pour les sciences abstraites en général et surtoût pour les mysteres des nombres est fort rare : on ne s'en étonne pas ; les charmes enchanteurs de cette sublime science ne se decelent dans toute leur

[17] On suppose donc que Gauss l'a faite, dans une quelconque marge...

beauté qu'à ceux qui ont le courage de l'approfondir. Mais lorsqu'une personne de ce sexe, qui, par nos moeurs et par nos préjugés, doit rencontrer infiniment plus d'obstacles et de difficultés, que les hommes, à se familiariser avec ces recherches epineuses, sait neansmoins franchir ces entraves et penétrer ce qu'elles ont de plus caché, il faut sans doute, qu'elle ait le plus noble courage, des talens tout à fait extraordinaires, le génie supérieur. En effet, rien ne pourroit me prouver d'une manière plus flatteuse et moins équivoque, que les attraits de cette science, qui ont embelli ma vie de tant de jouissances, ne sont pas chimériques, que la predilection, dont vous l'avez honorée.

Annexe 1 : Articles 75 à 78 des Recherches arithmétiques de Carl-Friedrich Gauss

75. Avant d'abandonner ce sujet, nous présenterons quelques propositions qui ne nous paraissent pas indignes d'attention, à cause de leur simplicité.
Le produit de tous les termes de la période d'un nombre quelconque est $\equiv 1$ *quand leur nombre ou l'exposant auquel appartient le nombre dont il s'agit est impair, et* $\equiv -1$ *quand il est pair.*
Par exemple, pour le module 13, la période de 5 est composée des termes $1, 5, 12, 8$ dont le produit $480 \equiv -1$ (*mod* 13), suivant le même module, la période de 3 est composée des termes $1, 3, 9$, dont le produit $27 \equiv 1$ (*mod* 13).
Soit t l'exposant auquel le nombre appartient ; on peut toujours trouver (n°71) une base pour laquelle l'indice du nombre soit $\frac{p-1}{t}$. Or l'indice du produit de tous les termes sera

$$(1 + 2 + 3 + etc. + t - 1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2};$$

donc il sera $\equiv 0$ (*mod* $p-1$), quand t est impair et $\equiv \frac{p-1}{2}$ quand t est pair. Dans le premier cas, le produit est $\equiv 1$ (*mod* p) ; dans le second, $\equiv -1$ (*mod* p).

76. Si le produit du théorème précédent est une racine primitive, sa période comprendra tous les nombres $1, 2, 3, 4, \ldots p-1$, dont le produit sera par conséquent toujours $\equiv -1$; car $p-1$ est toujours pair, excepté dans le cas où $p = 2$, et alors on a indifféremment $+1$ ou -1. Ce théorème élégant qu'on énonce ordinairement de cette manière : *Le produit de tous les nombres plus petits qu'un nombre premier étant augmenté de l'unité, est divisible par ce nombre premier,* a été publié par *Waring* qui l'attribue à *Wilson* (*Meditationes Algeb. Ed. 3, p. 380*) ; mais aucun des deux n'a pu le démontrer, et *Waring* avoue que la démonstration lui en semble d'autant plus difficile qu'il n'y a point de *notation* par laquelle on puisse exprimer un nombre premier ; pour nous, nous pensons que la démonstration de cette sorte de vérités doit être puisé dans les principes plutôt que dans la notation. *Lagrange* en a depuis donné une démonstration (*Nouv. Mém. de l'Ac. de Berlin, 1771)*, dans laquelle il s'appuie sur la considération des coefficients que l'on trouve en développant le produit

$$(x+1)(x+2)(x+3)\ldots(x+p-1) :$$

et il fait voir qu'en supposant ce produit

$$= x^{p-1} + Ax^{p-2} + Bx^{p-3} + etc. + Mx + N,$$

les coefficients A, B, etc. M sont divisibles par p ; or

$$N = 1.2.3\ldots p-1$$

Maintenant si $x = 1$, le produit est divisible par p, mais alors il sera $\equiv 1 + N$ (*mod* p) donc $1 + N$ est divisible par p.
Enfin Euler *(Opusc. analyt. T.1, p.329)* en a donné une démonstration qui rentre dans celle que nous venons d'exposer ; ainsi puisque de tels hommes n'ont

pas cru ce sujet indigne de leurs méditations, nous espérons qu'on ne nous désapprouvera pas d'offrir encore ici une autre manière de démontrer ce théorème.

77. Nous dirons que deux nombres sont *associés*, comme l'a fait *Euler*, lorsque leur produit sera congru à l'unité. Cela posé, par la section précédente, tout nombre positif moindre que p, aura toujours un nombre associé moindre que p et il n'en aura qu'un ; or il est facile de prouver que parmi les nombres $1, 2, 3, -1$, il n'y a que 1 et $p-1$ qui soient eux-mêmes leurs associés, car ceux qui jouiront de cette propriété seront donnés par la congruence $x^2 \equiv 1$ qui ne peut avoir que 2 racines 1 et $p-1$. Supprimant donc ces deux nombres, les autres $2, 3, 4 \ldots p-2$, seront associés deux à deux, donc leur produit sera $\equiv 1$; enfin multipliant par $p-1$, le produit de tous $1.2.3.4 \ldots p-1 \equiv p-1 \equiv -1$.
Par exemple, pour $p = 13$, les nombres $2, 3, 4, 5, \ldots 11$ s'associent de la manière suivante : 2 avec 7, 3 avec 9, 4 avec 10, 5 avec 8, 6 avec 11 ; donc $2.3.4 \ldots 11 \equiv 1$, et partant..... $1.2.3 \ldots 12 \equiv 12 \equiv -1$.

78. Le théorème de *Wilson* peut être rendu plus général en l'énonçant comme il suit : *Le produit de tous les nombres premiers avec un nombre donné A et moindres que ce nombre, est congru suivant A, à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A = 4$; et positivement dans tous les autres cas. Le théorème de Wilson est contenu dans le premier cas. *Exemple.* Pour $A = 15$, le produit des nombres $1, 2, 4, 7, 8, 11, 13, 14$ est $\equiv 1$ (*mod* 15). Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de 2 racines, ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le n°75, si l'on y joint ce que nous dirons tout à l'heure des modules composés.

Annexe 2 : Article 41 des Recherches arithmétiques de Carl-Friedrich Gauss

Dans l'article 41 des Recherches arithmétiques de Gauss, on retrouve la notion de permutations et on pense aux travaux de Galois à venir.

41. *Si p est un nombre premier, et qu'on ait p choses parmi lesquelles il peut s'en trouver un certain nombre d'égales entre elles, pourvu que toutes ne le soient pas : le nombre des permutations de ces choses sera divisible par p.*

Par exemple, cinq choses A, A, A, B, B peuvent se disposer de dix manières différentes.

La démonstration de ce théorème se déduit facilement de la théorie connue des permutations. En effet, supposons que parmi ces p choses, il y en ait a égales à A, b égales à B, c égales à C etc., de sorte qu'on ait $a + b + c + etc = p$, les nombres a, b, c,etc. pouvant aussi désigner l'unité. Le nombre de permutations sera $= \dfrac{1.2.3 \ldots p}{1.2 \ldots a.1.2 \ldots b.1.2 \ldots c.etc.}$; or le numérateur est évidemment divisible

par le dénominateur, puisque le nombre des permutations est entier ; mais il est divisible par p, tandis que le dénominateur, qui est composé de facteurs plus petits que p, n'est pas divisible par p (n°15) ; donc le nombre des permutations sera divisible par p.

Nous espérons cependant que la démonstration suivante ne déplaira pas à quelques lecteurs.

Lorsque dans deux permutations l'ordre des choses ne différera qu'en ce que celle qui tient la première place dans l'une, en occupe une différente dans l'autre, mais que du reste toutes les autres choses, à partir de celle-là, suivent le même ordre dans chacune des permutations, de manière que la dernière de l'une se trouve placée immédiatement avant la première, dans l'autre ; nous les appellerons permutations semblables[3]. Ainsi $ABCDE$ et $DEABC$, $ABAAB$ et $ABABA$ seront semblables.

Or comme chaque permutation est composée de p choses, il est clair qu'on pourra en trouver $p-1$ semblables à une quelconque d'entre elles, si l'on met successivement à la seconde, à la troisième place, etc., la chose qui occupait la première ; donc si aucunes de ces permutations semblables ne sont identiques, il est évident que le nombre total des permutations sera égal à p fois le nombre des permutations dissemblables, et conséquemment sera divisible par p. Supposons que deux permutations semblables $PQ\dots TV\dots, V\dots YZPQ\dots T$ puissent être identiques, et que P qui occupe la première place dans la première, occupe la $n+1^{ième}$ dans la seconde : on aura dans la dernière série le $n+1^{ième}$ terme égal au 1^{er}, le $n+2^{ième}$ égal au $2^{ième}$, etc., d'où résulte que le $2n+1^{ième}$ est encore égal au premier et par conséquent le $3n+1^{ième}$, et généralement le $kn+m^{ième}$ égal au $m^{ième}$ (où quand $kn=m>p$, il faut imaginer qu'on reprenne toujours par le commencement, la série $V\dots T$, à moins qu'on ne retranche de $kn+m$, le multiple de p, qui en approche le plus en moins). Cela posé, si on détermine k de manière que $kn\equiv 1\ (mod\ p)$, ce qui peut toujours se faire, puisque p est premier, il suivra de là que généralement le $m^{ième}$ terme serait égal au $m+1^{ième}$, c'est à dire qu'un terme quelconque serait égal au suivant, ou que tous les termes seraient égaux entre eux, ce qui est contre l'hypothèse.

[3]Si l'on écrivait en cercle les permutations semblables, de manière que la dernière chose touchât la première, il n'y aurait aucune différence entre elles, parce qu'aucune place ne peut s'appeler la première ni la dernière.