Transcription des Recherches arithmétiques de Gauss, sections 121, 122 et 123 (Denise Vella-Chemla, 24.12.2017)

121. L'induction fait voir que +5 n'est résidu d'aucun nombre impair de la forme $5n+2$, ou $5n+3$, c'est-à-dire d'aucun nombre impair qui soit non-résidu de 5 lui-même. Or nous allons démontrer que cette règle ne souffre d'aucune exception. Soit, s'il est possible, t le plus petit nombre à en excepter, 5 sera résidu de t et t non-résidu de 5. Soit $a^2 = 5 + tu$ de sorte que a soit pair et $< t$; u sera impair et $< t$, et +5 sera résidu de u. Si a n'est pas divisible par 5, u ne le sera pas non plus ; mais il est évident que tu est résidu de 5 ; donc comme t est non-résidu de 5, u le sera aussi, c'est à dire qu'il y a un nombre impair $< t$ qui est non-résidu de 5 et dont 5 est résidu ; mais si a est divisible par 5, soit $a = 5b$ et $u = 5v$, il en résultera $tv \equiv -1 \equiv 4$ $(mod\ 5)$, c'est-à-dire que tv sera résidu de 5. La marche de la démonstration est pour le reste la même que dans le cas précédent.

122. Donc +5 et −5 sont non-résidus de tous les nombres premiers qui sont à la fois non-résidus de 5 et de la forme $4n+1$, c'est-à-dire de tous les nombres premiers de la forme $20n+13$ ou $20n+17$; mais 5 sera non-résidu, et -5 résidu de tous les nombres premiers de la forme $20n+3$ ou $20n+7$.

Or on démontrera absolument de la même manière que −5 est non-résidu de tous les nombres premiers de la forme $20n+11$, $20n+13$, $20n+17$, $20n+19$, et l'on voit facilement qu'il suit de là que +5 est résidu de tous les nombres premiers de la forme $20n+11$, ou $20n+19$; enfin non-résidu de tous ceux de la forme $20n+13$, ou $20n+17$; et comme tout nombre premier, excepté 2, et 5, dont ±5 est résidu, est contenu dans l'une des formes : $20n+1, +3, +7, +9, +11, +13, +17, +19$, il est clair que l'on peut juger de tous, excepté de ceux qui sont de la forme $20n+1$, ou $20n+9$.

123. Par induction, on trouve facilement que +5 et −5 sont résidus de tous les nombres premiers de la forme $20n+1$ et $20n+9$; et si cette proposition est généralement vraie, on aura cette loi élégante que +5 *est résidu de tous les nombres premiers qui sont résidus de 5 lui-même,* (car ces nombres sont contenus dans les formes $5n+1$ ou $5n+4$, ou ce qui revient au même dans les formes $20n+1, +9, +11, +19$, parmi lesquelles la troisième et la quatrième ont déjà été traitées), *et non-résidu de tous les nombres premiers impairs, qui sont résidus de 5,* comme nous l'avons déjà démontré plus haut. Or il est clair que ce théorème suffit pour juger si +5 et partant −5, qui n'est autre que $+5 \times -1$, sont résidus ou non-résidus d'un nombre donné quelconque. On peut observer aussi l'analogie de ce théorème avec celui du n°120 sur le résidu -3.

Mais la vérification de cette induction n'est pas facile. Quand le nombre proposé est de la forme $20n+1$ ou plus généralement de la forme $5n+1$, on peut employer une méthode semblable à celle des n^{os}114, 119. Soit en effet a un nombre quelconque appartenant à l'exposant 5, suivant le module $5n+1$, nombre qu'on a appris à trouver dans la section précédente, on aura $a^5 \equiv 1$, ou $(a-1)(a^4+a^3+a^2+a+1) \equiv 0$ $(mod\ 5n+1)$. Mais comme on ne peut avoir $a \equiv 1$, il s'ensuit qu'on aura $a^4+a^3+a^2+a+1 \equiv 0$; donc $4(a^4+a^3+a^2+a+1) = (2a^2+a+2)^2 - 5a^2 \equiv 0$; c'est-à-dire, que $5a^2$ est résidu de $5n+1$; et partant 5 lui-même, puisque a^2 est un résidu non-divisible par $5n+1$; car à cause de $a^5 \equiv 1$, a n'est pas divisible par $5n+1$.

Comme le cas où il est question d'un nombre premier de la forme $5n+4$ demande des artifices particuliers de calculs, et comme nous traiterons par la suite, d'une manière générale, les propositions au moyen desquelles on peut résoudre ce problème, nous nous contenterons d'en parler ici en passant.

1°. Si p est un nombre premier, et b un nombre aussi donné non-résidu de p, la valeur de l'expression $\dfrac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}} = A$, dont le développement ne contiendra pas d'irrationnelles, sera toujours divisible par p, quelque valeur que l'on attribue à x. En effet il est clair, par l'inspection des coefficients qui naissent de ce développement, que tous les termes, depuis le second jusqu'à l'avant-dernier inclusivement, sont divisibles par p, et que partant $A \equiv 2(p+1)\left(x^p + xb\dfrac{p-1}{2}\right)$ $(mod\ p)$; mais parce que b est non-résidu de p, on aura $b\dfrac{p-1}{2} \equiv -1$ $(mod\ p)$, (n°106) ; or on a toujours $x^p \equiv x$ (section précédente), d'où s'ensuit $A \equiv 0$.

2°. Dans la congruence $A \equiv 0$, l'indéterminée x aura p dimensions, et tous les nombres $0, 1, 2, 3 \ldots p-1$, seront racines de cette congruence. Soit e un diviseur de $p+1$, l'expression $\dfrac{(x+\sqrt{b})^e - (x-\sqrt{b})^e}{\sqrt{b}}$, que nous représenterons par B, sera rationnelle, x y aura $e-1$ dimensions, et il est constant par les premiers éléments d'analyse, que A est divisible par B. Or, je dis qu'il y a $e-1$ valeurs, qui rendent B divisible par

p. En effet, soit $A = BC$, x aura dans C, $p - e + 1$ dimensions, et partant la congruence $C \equiv 0 \ (mod\ p)$, ne pourra avoir plus de $p - e + 1$ racines, d'où il suit que les $e - 1$ autres nombres pris dans la série $0, 1, 2, \ldots p - 1$, seront racines de la congruence $B \equiv 0$.

3°. Supposons maintenant p de la forme $5n+4$, $e = 5$, b un non-résidu de p, et le nombre a déterminé de manière à rendre $\dfrac{(a+\sqrt{b})^5 - (a-\sqrt{b})^5}{\sqrt{b}}$ divisible par p. Cette expression devient $= 10a^4 + 20a^2b + 2b^2 = 2\{(b+5a^2)^2 - 20a^4\}$; donc $(b+5a^2) - 20a^4 \equiv 0 \ (mod\ p)$; c'est-à-dire que $20a^4$ est résidu de p ; mais comme $4a^4$ est un résidu non-divisible par p,(car on voit facilement que a ne peut être divisible par p), 5 sera lui-même résidu de p.

Il est clair par là que le théorème énoncé au commencement de cet article est généralement vrai.

Observons encore que les démonstrations des deux cas sont dûes à *Lagrange. (Mémoires de l'Académie de Berlin, 1775,* p.352).