CERTAINS THÉORÈMES DANS LA THÉORIE DES RÉSIDUS QUADRATIQUES.

D. N. LEHMER
Université de Californie

La définition d'un résidu quadratique est habituellement donnée comme suit : *Si l'on peut trouver un entier X qui satisfasse la congruence,*

$$X^2 \equiv D \pmod{m}$$

où D est premier à m, alors D est dit être un résidu quadratique de m. La restriction que D doive être premier à m simplifie de nombreux résultats. Il y a des théories, pourtant, dans lesquelles cette restriction brouille les résultats et dans cet article, nous ne l'imposerons pas. Commençons, tout d'abord, par déterminer le nombre de résidus d'un entier m donné, en utilisant la définition élargie.

On étudie avant tout le cas où le module m est une puissance d'un nombre premier impair p. Aux premières positions vont surgir $\frac{1}{2}\varphi(p^\alpha)$ résidus distincts de l'élévation au carré des nombres k, qui sont inférieurs à p^α, et premiers à p, $p^\alpha - k$ et k fournissant les mêmes résidus. Considérons ensuite les nombres kp, où k est premier à p. Si deux tels nombres quand on les élève au carré donnent le même résidu, on a :

$$k^2p^2 \equiv k_1^2p^2 \pmod{p^\alpha},$$

d'où,

$$k_1^2 \equiv k_1^2 \pmod{p^{\alpha-2}}$$

ou

$$k \equiv \pm k_1 \pmod{p^{\alpha-2}}.$$

Appelons maintenant k les $\varphi(p^{\alpha-2})$ valeurs inférieures à $p^{\alpha-2}$ et premières à p. Les carrés résultant fournissent $\frac{1}{2}\varphi(p^{\alpha-2})$ résidus distincts. De la même façon, les nombres kp^2 où k est premier à p fournissent $\frac{1}{2}\varphi(p^{\alpha-4})$ des résidus distincts qui sont également différents de ceux obtenus à partir de kp obtenus ci-dessus. En procédant de la sorte, on obtient pour le nombre total de résidus distincts :

$$\frac{1}{2}[\varphi(p^\alpha) + \varphi(p^{\alpha-2}) + \varphi(p^{\alpha-4}) + \varphi(p^{\alpha-6}) + \ldots] + 1$$

Traduction Denise Vella-Chemla, juin 2022.
Référence : https://www.jstor.org/stable/2972413.

l'unité étant ajouté pour le résidu zéro.

Pour α pair, la formule résultante est :

$$\frac{p^{\alpha+1}-p}{2(p+1)}+1 \qquad (p \text{ un nombre premier impair}).$$

Pour α impair :

$$\frac{p^{\alpha+1}-1}{2(p+1)}+1.$$

Pour m une puissance de 2, le résultat est un peu différent. Il y a $2^{\alpha-3}$ résidus distincts résultant des carrés des nombres impairs. Cela est dû à la congruence, $(2^{\alpha-2}-k)^2 \equiv (2^{\alpha-2}+k)^2 \pmod{2^\alpha}$. Il y a $2^{\alpha-5}$ résidus provenant des carrés des nombres $2k$ où k est impair. Cela vient de la congruence, $(2^{\alpha-3}-2k)^2 \equiv (2^{\alpha-3}+2k)^2 \pmod{2^\alpha}$. Similairement, il y a $2^{\alpha-7}$ résidus distincts provenant des carrés des nombres 2^2k où k est impair, et en général, il y a $2^{\alpha-(2\kappa+3)}$ résidus provenant des carrés des multiples impairs de 2^κ. Ainsi dans le cas où α est impair, on a la série $2^{\alpha-3}+2^{\alpha-5}+2^{\alpha-7}+\ldots$, qui se termine par 1, le dernier terme résultant des multiples impairs de 2 où $\lambda=(\alpha-3)/2$. Il reste en outre deux résidus ; l'un résultant de 2^λ où $\lambda=(\alpha-1)/2$, et l'autre de 2^λ où $\lambda=(\alpha+1)/2$. On voit que ce dernier est nul, modulus 2, en raison de la congruence,

$$(2^{\alpha+1/2}\cdot k)^2 \equiv 2^{\alpha+1}\cdot k^2 \equiv 0 \pmod{2^\alpha}.$$

Pour α impair donc, la formule est $(2^{\alpha-1}+5)/3$. Pour α pair le résultat est $(2^{-3}+2^{\alpha-5}+2^{\alpha-7}+2)+2$ [1] ; c'est-à-dire que $(2^{\alpha-1}+4)/3$.

Comme illustrations des résultats, le nombre de résidus du nombre $81=3^4$, est $(3^5-3)/2\cdot 4+1$ ou 31. Les résidus sont les nombres : 0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25, 28, 31, 34, 36, 37, 40, 43, 36, 39, 52, 55, 58, 61, 63, 64, 67, 70, 73, 76, 79.

Pour le nombre $27=3^3$ le nombre est $(3^4-1)/2\cdot 4+1$ ou 11. Les résidus sont les nombres : 0, 1, 4, 7, 9, 10, 13, 16, 21, 25.

Pour le nombre $32=2^5$ la formule donne $(2^4+5)/3=7$. Les résidus sont : 0, 1, 4, 9, 16, 17, 25.

Pour le nombre $64=2^6$ on a $(2+4)/3=12$. Les résidus sont : 0, 1, 4, 9, 16, 17, 25, 33, 36, 41, 49, 57.

1. manque un α dans le premier exposant de 2 ?

Pour un module m qui est le produit d'un nombre quelconque de puissances de premiers, le nombre de résidus est obtenu en prenant le produit des nombres de résidus pour les puissances de premiers séparément. Ainsi si $mp_1^{\alpha_1}p_2^{\alpha_2}$, la solution de $X^2 \equiv D \pmod{m}$ est possible si et seulement si les différentes congruences $X^2 \equiv D \pmod{p_1^{\alpha_1}}$ et $X^2 \equiv D \pmod{p_2^{\alpha_2}}$ sont possibles ; et toute solution de la première peut être combinée avec n'importe quelle solution de la seconde pour fournir une solution de la congruence originale. Ainsi si $D \equiv \alpha \pmod{p_1^{\alpha_1}}$ est telle que la congruence $X^2 \equiv D \pmod{p_1^1}$ est résoluble et $D \equiv \beta \pmod{p_2^2}$ telle que la congruence $X^2 \equiv D \pmod{p_2^{\alpha_2}}$ est résoluble, alors comme les modules sont relativement premiers les uns aux autres, une et une seule solution des deux congruences est possible $D \equiv \alpha \pmod{p_1^{\alpha_1}}$ et $D \equiv \beta \pmod{p_2^{\alpha_2}}$ pris simultanément et le D résultat rend $X^2 \equiv D \pmod{p_1^1 p_2^{\alpha_2}}$ résoluble. Ainsi le nombre des résidus du nombre 42 est égal au produit des nombres de résidus de 2, 3 et 7. C'est-à-dire, $2 \cdot 2 \cdot 4$ ou 16. Les résidus sont en fait : 0, 1, 4, 7, 9, 15, 16, 18, 21, 22, 25, 28, 30, 36, 37, 39.

Résidus consécutifs. Certains théorèmes intéressants [2] concernant le nombre de résidus consécutifs pour un nombre premier donné ont été obtenus pour la définition courante du résidu quadratique par M. Aladov [3] et également par M. von Sterneck [4]. Les résultats de M. Aladov - je n'ai pas lu l'article - sont les suivants :

Soient x = le nombre de non-résidus suivis par un non-résidu,
x' = le nombre de non-résidus suivis par un résidu,
y = le nombre de résidus suivis par un non-résidu,
y' = le nombre de résidus suivis par un résidu.

Alors pour p un nombre premier de la forme $4n+1$ on a :

$$x = x' = y = \frac{p-1}{4}\ ; \qquad \text{and} \qquad y' = \frac{p-5}{4}$$

et pour p un nombre premier de la forme $4n+3$ on a :

$$x = x' = y' = \frac{p-3}{4}, \qquad \text{and} \qquad y = \frac{p+1}{4}.$$

M. von Sterneck a étendu ces résultats pour montrer que pour tout nombre premier exceptés 2, 3, 5, 7, 11, and 17, il y a au moins un groupe de quatre résidus consécutifs, ou de quatre non-résidus consécutifs.

2. Ces théorèmes ont été démontrés par Jordan dans son *Traité des Substitutions*, 1870, page 158. Le Professeur Dickson a gentiment attiré mon attention sur la preuve de Jordan, qui est basée sur des principes différents de ceux donnés ici.
3. *Recueil Mathématique*, Société de Moscou, t. XVIII, 1895.
4. *Ibid.*, t. XX, 1898.

Les résultats de M. Aladov ne sont pas difficiles à obtenir en considérant la congruence, $xy \equiv 1 \pmod{p}$. Cette congruence regroupe les $p-1$ nombres, $1, 2, 3, 4, \ldots p-1$, en paires. Pour deux valeurs de x, notamment, ± 1, la valeur de y est égale à x. Pour d'autres valeurs de x la valeur de y est différente. Il y a donc en tout $(p+1)/2$ paires. Appelons x', y', une telle paire. Alors il y a une autre paire $(p-x')(p-y')$, et pour notre but, ces deux paires ne sont pas vraiment distinctes, puisqu'elles fournissent des paires identiques de résidus consécutifs comme suit : si l'on met $a+b \equiv x'$ et $a-b \equiv y'$ on obtient $a^2 - b^2 \equiv 1 \pmod{p}$, ou a et b sont des résidus consécutifs. La paire $(p-x')(p-y')$ donne la même paire de résidus. Le nombre de paires de résidus consécutifs semblerait par conséquent être $(p+1)/4$, et c'est effectivement la bonne formule pour p, un nombre premier de la forme $4n+3$. Pour p un nombre premier de la forme $4n+1$ le nombre de paires sera impair et il y aura une paire dans laquelle $x' = p - y'$, ou bien dans laquelle la paire (x', y') est identique à la paire $(p-y', x')$. Le nombre de paires distinctes de résidus consécutifs pour un tel nombre premier est par conséquent $(p+3)/4$. Dans ces formulæ on a inclus le résidu zéro. Ainsi pour le nombre premier 11, nous avons les paires suivantes de valeurs x, y et les valeurs correspondantes de a et b :

x,	y.	$p-x$,	$p-y$.	Résidus.	
1,	1.	10,	10.	1,	0.
2,	6.	9,	5.	5,	4.
3,	4.	8,	7.	4,	3.

Il y a ainsi trois paires consécutives de résidus pour le nombre premlier 11. Pour le nombre premier 17, on a les paires suivantes :

x,	y.	$p-x$,	$p-y$.	Résidus.	
1,	1.	16,	16.	1,	0.
2,	9.	15,	8.	9,	8.
3,	6.	14,	11.	16,	15.
4,	13.	13,	4.	17,	16.
5,	7.	12,	10.	2,	1.

La formule d'Aladov donnera seulement trois paires parce qu'il n'admet pas le résidu 0. Cela élimine la première et la quatrième paires.

Le reste des résultats de M. Aladov suivent sans trop de difficulté. Ainsi pour un nombre premiler de la forme $4n+1$, si on dénote un résidu par R, et un non-résidu par N, notre formule pour le nombre de séquences RR est $(p+3)/4$. Pour la séquence NN on peut commencer à partir de la congruence $xy \equiv N \pmod{p}$ et par une ligne de raisonnement exactement similaire, on peut dériver la formule $(p-1)/4$ pour le nombre de paires de résidus différant par un non-résidu donné N. Soient R' et R'' deux tels résidus, tels que $R' - R'' \equiv N \pmod{p}$. Multiplions maintenant cette congruence par le non-résidu N' qui est tel que $NN' \equiv 1 \pmod{p}$ et nous obtenons une paire de

non-résidus différant de l'unité. Pour les séquences NR et RN on peut voir qu'elles doivent être égales en nombre, car puisque -1 est résidu de nombres premiers de la forme $4n+1$ la séquence RN implique la séquence $-R, -N$, qui quand on l'écrit $p-N, p-R$ est vue comme étant une séquence NR. Maintenant le nombre total de séquences dans la suite de nombres $0, 1, 2, 3, 4, \ldots, p-1, p$ est égal à p. Parmi ceux-ci, il y a $(p+3)/4$ séquences RR, et $(p-1)/4$, séquences NN. Les $(p-1)/2$ séquences restantes se divisent en séquences NR et séquences RN, et sont donc au nombre de $(p-1)/4$. Avec la notation utilisée pour établir les résultats de M. Aladov, on a, en incluant le résidu zéro,

$$x = x' = y = \frac{p-1}{4}\ ; \qquad \text{et} \qquad y' = \frac{p+3}{4}$$

Le cas où p est de la forme $4n+3$ peut être étudié de la même manière,

$$x' = y' = y = \frac{p+1}{4}, \qquad \text{et} \qquad x = \frac{p-3}{4}.$$

Je ne sais pas si M. Aladov a étendu ces résultats pour les appliquer aux modules composés ou pas. Nous allons faire cela, et d'abord, prenons le cas où le module est une puissance d'un nombre premier impair p. On montrera comment on peut dériver, à partir d'une paire de résidus consécutifs pour le module p^α, p paires de résidus consécutifs pour le module $p^{\alpha+1}$, à moins que l'une des paires de résidus consécutifs pour p^α ne soit congrue à zéro mod p^α.

Soit $x_1^2 - y_1^2 \equiv 1 \pmod{p^\alpha}$ une paire de résidus consécutifs. Alors $(x_1 + kp^\alpha)^2 - (y_1 + lp^\alpha)^2 \equiv 1 \pmod{p^\alpha}$ fournira la même paire pour toutes les valeurs de k et 1. Multiplions et posons $x_1^2 - y_1^2 - 1 = mp^\alpha$, alors

$$mp^\alpha + 2(kx_1 - ly_1)p^\alpha + (k^2 - l^2)p^{2\alpha} \equiv 0 \pmod{p^\alpha}.$$

Le dernier terme sur la gauche est congru à zéro mod $p^{\alpha+1}$ si α est plus grand que l'unité. Les autres termes seront aussi divisibles par $p^{\alpha+1}$ si

$$m + 2(kx_1 - ly_1) \equiv 0 \pmod{p}.$$

Dans cette congruence m, x_1, et y_1 sont connus et k et l sont inconnus. On peut montrer qu'une congruence de la forme $ax + by + c \equiv 0 \pmod{p}$ a exactement p racines, à moins que a et b ne soient divisibles par p, et que c ne le soit pas. Nous différons la preuve de ce théorème et notons que si $y_1 \equiv 0 \pmod{p^\alpha}$ alors la congruence $m + 2kx_1 \equiv 0 \pmod{p}$ fournit seulement une paire effective, car quelle que soit la valeur de 1, l'expression $(y_1 + lp^\alpha)^2$ sera divisible par $p^{\alpha+1}$ pour α plus grand que un. Donc une paire de résidus consécutifs pour le module p^α fournit en général p résidus consécutifs pour le module $p^{\alpha+1}$ excepté la paire consécutive $(1, 0)$ qui amène la paire unique $(1, 0)$. Aussi, si p est de la forme $4n+1$ alors une paire $(0, -1)$ peut

être obtenue qui amène également la paire unique $(0, -1)$ pour le module $p^{\alpha+1}$. Le théorème est ainsi démontré.

Le théorème concernant le nombre de solutions de la congruence $ax + by + c \equiv 0 \pmod{p}$ est un cas particulier du théorème plus général :

La congruence $ax + by + c \equiv 0 \pmod{m}$ a $m\delta$ solutions, ou aucune selon que δ, le plus grand diviseur commun de a, b et m, divise ou ne divise pas c.

La congruence n'a clairement pas de solutions quand δ ne divise pas c. Prenons d'abord le cas où δ est l'unité, et appelons δ' le plus grand commun diviseur de a et m. Alors selon la théorie bien connu des congruences, $ax + b \equiv 0 \pmod{m}$, on voit qu'il y aura δ' valeurs de x pour toute valeur de y satisfaisant la congruence $by + c \equiv 0 \pmod{\delta'}$. Maintenant, b est premier à δ' et donc cette dernière congruence a une et une seule racine β, disons. Les m/δ' nombres inférieurs ou égaux à m et congruents à $\beta \pmod{\delta'}$ serviront de valeurs de y, chacune fournissant les valeurs correspondantes de δ' correspondant aux valeurs de x. D'autres valeurs de y ne donneront aucune valeur du tout de x. Le nombre total de solutions dans ce cas $m/\delta' \cdot \delta'$, ou m. Si maintenant δ n'est pas l'unité, on peut diviser les deux côtés de la congruence par δ et obtenir la congruence $(a/\delta)x + (b/\delta)y + (c/\delta) \equiv 0 \pmod{(m/\delta)}$, qui a par la discussion ci-dessus m/δ solutions. Soit (α, β) l'une de ces solutions. Alors à la place de α on peut prendre n'importe lequel des nombres δ congruents à $\alpha \bmod(m/\delta)$ qui sont inférieurs ou égaux à m. De même pour β. Le nombre total de solutions est donc $(m/\delta) \cdot \delta \cdot \delta$, ou $m\delta$, ce qui prouve le théorème. Une ligne de raisonnement similaire montrera que le nombre de solutions de la congruence $ax + by + cz + d \equiv 0 \pmod{m}$, est $m^2\delta$, ou zéro, selon que δ, le plus grand diviseur commun de a, b, c, et m ne divise pas d. En général aussi, par une induction simple, on peut établir que le nombres de solutions de la congruence $a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + \ldots + a_nx_n + a_{n+1} \equiv 0 \pmod{m}$ is $m^{n-1}\delta$, ou zéro, selon que δ, le plus grand diviseur de $a_1, a_2, a_3, \ldots a_n$ et m divise ou ne divise pas a_{n+1}. Ces théorèmes sont, bien sûr, des cas particuliers du problème général des congruences linéaires simultanées discutées par H. J. S. Smith (*Works*, Vol. II, p. 367).

On peut maintenant écrire les formulæ pour le nombre de résidus consécutifs pour un module qui est la puissance de n'importe quel nombre premier impair p. On a vu que le nombre de résidus consécutifs pour un nombre premier de la forme $4n + 1$ est $(p + 3)/4$, et en éliminant les deux séquences $(0, 1)$ et $(-1, 0)$ il reste $\{(p + 3)/4\} - 2$ séquences ordinaires. Pour le module p^2, on doit multiplier cela par p et les deux séquences finales $(0, 1)$ et $(-1, 0)$ sont ajoutées, ce qui donne pour le module p^2 le nombre total de résidus consécutifs comme étant $\{(p - 5)/4\}p^{\alpha-1} + 2$. En général, pour la puissance p^α le nombre de résidus consécutifs sera $\{(p - 5)/4\}p^{\alpha-1} + 2$. La formule est fausse pour le nombre premier 5, puisque dans le cas de cet nombre pre-

mier $(p+3)/4$ est égal à 2, et rejeter les deux résidus consécutifs finaux donnera zéro. La formule donnerait toujours comme nombre 2. Ceci est correct pour α égale à 1, ou 2, mais pour α plus grand que 2 la formule correcte est $4 \cdot 5^{\alpha-3} + 2$.

L'argument est facile à établir également pour p de la forme $4n-1$ et la formule est $\{(p-3)/4\}p^{\alpha-1} + 1$, pour le nombre de résidus consécutifs pour le module p^α. Le nombre premier 3 est une exception. Pour α égal à 1 ou 2 le nombre est 1. Pour α plus grand que 2 le nombre est $3^{\alpha-3} + 1$.

Pour un module qui est une puissance de 2 la formule se réduit au plus grand entier dans $(2^{\alpha-5}+5)/3$, pour 2^α, où α est plus grand que 4. Pour α inférieur à 4 le nombre de séquences vaut 1.

Pour un module composé général, il est maintenant possible de calculer le nombre de résidus consécutifs. En fait, le nombre de tels résidus pour le produit de deux nombres premier l'un à l'autre est égal au produit des nombres pour chacun de ces facteurs. Supposons que les deux facteurs soient p et q, et que nous ayons trouvé pour chacun une paire de résidus consécutifs, de telle façon que

$$P_1 - P_2 \equiv 1 \pmod{p}$$

et

$$Q_1 - Q_2 \equiv 1 \pmod{q}$$

et que ceux-ci proviennent des carrés,

$$x_1^2 - y_1^2 \equiv 1 \pmod{p}$$

et

$$x_2^2 - y_2^2 \equiv 1 \pmod{q};$$

déterminons maintenant k et l pour satisfaire les congruences :

$$x_1 + kp \equiv x_2 \pmod{q}, y_1 + lp \equiv y_2 \pmod{q};$$

p étant premier à q celles-ci auront une et uniquement une solution chacune. Ainsi le nombre de résidus consécutifs pour le module pq est au moins aussi grand que le produit du nombre deux ceux existant pour le module p par le nombre de ceux existant pour le module q. Mais puisque un résidu de pq doit nécessairement être un résidu de p et de q séparément, toute paire de résidus consécutifs pour pq sera également une paire de résidus consécutifs pour p et pour q.

Comme illustration de la méthode pour trouver les résidus consécutifs pour un module composé, prenons le module $253 = 11.23$. Pour le module 11 on a les résidus consécutifs 3, 4 provenant de 5^2 et 2^2. Pour le module 23, on a les résidus 1, 2 provenant de 1^2 et 5^2. Les congruences $2 + 11k \equiv 5 \pmod{23}$ et $5 + 11l \equiv 1 \pmod{23}$ donnent $k \equiv 17$, et $l \equiv 8 \pmod{23}$. Alors $2+187$, ou 189, et $5+88$ ou 93 doivent fournir une paire de résidus consécutifs pour 253. On trouve que $189^2 \equiv 48$ et $93^2 \equiv 47$. Puisque de plus, il y a 3 résidus consécutifs pour le module 11, et 6 pour le module 23 il y en aura 18 pour le module 253.

En conclusion, on doit dire un mot à propos de la détermination de la possibilité de la congruence $x^2 \equiv D \pmod{m}$ où D n'est pas contraint à être premier à m. En premier lieu, il est nécessaire de ne considérer que le cas où le module est une puissance d'un nombre premier. Car on peut trouver x tel que $x^2 - D$ est divisible par pq, où p et q sont premiers l'un à l'autre, alors $x^2 - D$ sera divisible par p et q, et inversement. Considérons alors le module p^α ; et soit $D = Ap^\lambda$ où A est premier à p.

Si λ est plus grand que α la congruence aura la racine $x \equiv 0$.

I. Supposons que λ est inférieur à α, et supposons d'abord que A est un résidu de p et écrivons $A \equiv y^2 \pmod{p^\alpha}$. Alors si λ est pair, la congruence est possible et a la racine $x \equiv \pm y p^{\lambda/2}$

II. Si A est un résidu de p et λ est impair, la congruence n'a pas de racine. Car en écrivant $x^2 \equiv Ap^\lambda + Mp^\alpha$ alors x contient p^λ comme un facteur. Il doit donc contenir un autre facteur p. Mais le côté droit ne peut pas contenir de tel facteur.

III. Si A est un non-résidu de p et λ est pair, la congruence est impossible. Pour diviser par p^λ nous aurions la congruence impossible

$$x'^2 \equiv A \pmod{p^{\alpha-2}}.$$

IV. Si A est un non-résidu, et λ est impair alors Ap^λ est un non-résidu. La preuve est comme dans le cas II. En général, alors Ap^λ est un résidu de p^α quand λ est supérieur ou égal à α et quand λ est inférieur à α et pair, et A est un résidu de p.