1 Résultats démontrés faisant intervenir des résidus quadratiques

Les éléments qui suivent proviennent essentiellement du livre de Marc Guinot aux éditions Aleas "Une époque de transition : Lagrange et Legendre".

1.1 En utilisant le symbole de Legendre

Lorsqu'on utilise ce symbole $\left(\frac{a}{m}\right)$, le dénominateur m est un nombre premier impair et le numérateur a est un entier non divisible par m.

1) Pour qu'un entier a quelconque soit résidu quadratique de p, il faut et il suffit que a soit congru à l'un des entiers

$$1^2, 2^2, \ldots, \left[\frac{1}{2}(p-1)\right]^2$$

En utilisant le symbole de Jacobi, cela s'écrit :

$$\left(\frac{a}{m}\right) = \begin{cases} 1 \textit{ si } a \textit{ est un carré modulo } m \textit{ (i.e. } \exists\, x \leq m,\ a \equiv x^2 \ (mod\ m)); \\ \text{-1 } \textit{si } a \textit{ n'est pas un carré modulo } m \textit{ (i.e. } \forall\, x \leq m,\ a \not\equiv x^2 \ (mod\ m)). \end{cases}$$

2) Le produit de deux résidus quadratiques de p et le produit de deux résidus non quadratiques de p sont toujours des résidus quadratiques de p. Le produit d'un résidu quadratique et d'un résidu non quadratique est un résidu non quadratique.

2') Un entier premier à p résidu quadratique de p l'est aussi de toute puissance de p car $(\mathbb{Z}/p^r\mathbb{Z})^*$ est un groupe cyclique d'ordre $p^{r-1}(p-1)$ sauf si $p = 2$ car $(\mathbb{Z}/2^r\mathbb{Z})^*$ n'est pas cyclique.

2") Si un entier a est premier avec un nombre $m \geq 1$ et si m se décompose en facteurs premiers sous la forme

$$m = p_1^{n_1} \ldots p_r^{n_r}$$

(avec des nombres premiers p_i deux à deux distincts et des exposants $n_i \geq 1$), alors pour que a soit résidu quadratique modulo m, il faut et il suffit qu'il soit résidu quadratique de $p_i^{n_i}$ quel que soit i[1].

3) Dans un système complet de résidus modulo p un nombre premier impair, il y a exactement $\frac{1}{2}(p-1)$ résidus quadratiques de p et $\frac{1}{2}(p-1)$ résidus non-quadratiques.

4) Le nombre -1 est résidu quadratique de tous les nombres premiers p de la forme $4n+1$ et non-résidu quadratique de tous les nombres premiers de la forme $4n+3$.

Corollaire de 4) : Si p est un nombre premier de la forme $4n+1$, les résidus quadratiques (et les non-résidus) se répartissent symétriquement dans l'intervalle $[1, p-1]$; de façon précise, si a est un résidu (resp. un non-résidu) appartenant à l'ensemble $\{1, 2, \ldots, p-1\}$ alors $p-a$ est encore un résidu (resp. un non-résidu) appartenant au même ensemble.

5) Pour tout nombre premier p impair, le caractère quadratique de 2 modulo p est donné par la formule

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

cette formule signifiant que 2 est résidu quadratique des nombres premiers de la forme $8n+1$ et $8n+7$, et non-résidu des nombres premiers de la forme $8n+3$ et $8n+5$.

[1] Je suis hésitante là, j'avais l'impression d'après Gauss qu'on pouvait également obtenir un résidu si on faisait le produit d'un nombre pair de non-résidus.

5') Les résidus quadratiques a de 2 sont les entiers impairs congrus à 1 modulo 2 ; ceux de 4 sont les entiers impairs congrus à 1 modulo 4 et les résidus quadratiques de 2^n (pour $n \geq 3$ fixé) sont congrus à 1 modulo 8.

$$\left(\frac{a}{2}\right) = 1 \iff a \equiv 1 \ (mod\ 2)$$
$$\left(\frac{a}{4}\right) = 1 \iff a \equiv 1 \ (mod\ 4)$$
$$\left(\frac{a}{8}\right) = 1 \iff a \equiv 1 \ (mod\ 8)$$

6) ***Loi de Réciprocité Quadratique*** : Soient p et q deux nombres premiers impairs différents, les symboles de Legendre $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$ sont toujours égaux sauf lorsque p et q sont tous deux des nombres de la forme $4n+3$. Il revient au même de dire que

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

7) Soient a et b des nombres congrus entre eux modulo p. Si a est résidu quadratique de p, il en est de même de b ; si a n'est pas un résidu quadratique de p, b n'en est pas un non plus.

8) quel que soit a un entier donné et quels que soient m, n deux nombres premiers impairs ne divisant pas a,

$$\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right) \ si\ m \equiv n \ (mod\ 4a)$$

9) ***Lemme de Gauss*** : Pour tout entier a non divisible par p un nombre premier impair, on a

$$\left(\frac{a}{p}\right) = (-1)^{\lambda}$$

où λ est le nombre des entiers $a, 2a, \ldots, \frac{1}{2}(p-1)a$ dont le reste minimal modulo p est négatif.

10) ***Critère d'Euler :*** Si a est un entier quelconque non divisible par p un nombre premier impair, alors on a

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \ (mod\ p)$$

1.2 En utilisant le symbole de Jacobi

Lorsqu'on utilise le symbole de Jacobi $\left(\frac{a}{m}\right)$, le dénominateur m est un nombre impair (non forcément premier) et le numérateur a est un entier quelconque.

1)

$$\left(\frac{a}{m}\right) = \begin{cases} 0 \ si\ a\ est\ un\ multiple\ de\ m\ (i.e.\ m|a); \\ 1 \ si\ a\ est\ un\ carré\ modulo\ m\ (i.e.\ \exists\ x \leq m,\ a \equiv x^2\ (mod\ m); \\ \text{-1 } si\ a\ n'est\ pas\ un\ carré\ modulo\ m\ (i.e.\ \forall\ x \leq m,\ a \not\equiv x^2\ (mod\ m). \end{cases}$$

Les résidus ou non-résidus de m ne sont jamais divisibles par m.

2) quels que soient a, b deux entiers non nuls, et m un nombre impair positif premier à a et b (et donc premier à ab),

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$$

et si a est premier à m,

$$\left(\frac{a^2b}{m}\right) = \left(\frac{b}{m}\right)$$

3) quel que soit a non nul, m, n impairs positifs premiers à a,

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

4) quel que soit m un entier impair positif quelconque,

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$$

5) quel que soit m un entier impair positif quelconque,

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

6) ***Loi de Réciprocité Quadratique*** : quels que soient a et b deux nombres impairs positifs premiers entre eux,

$$\left(\frac{b}{a}\right) = \left(\frac{a}{b}\right)(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

7) quel que soit m un entier impair positif premier à a (et donc premier à b)

$$\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right) \; si \; a \equiv b \; (mod \; m)$$

8) quels que soient m et n deux entiers positifs impairs premiers à a tous les deux,

$$\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right) \; si \; m \equiv n \; (mod \; 4a)$$

9) ***Lemme de Gauss*** : pour tout entier non nul a et tout m un nombre impair positif premier à a,

$$\left(\frac{a}{m}\right) = (-1)^{\lambda}$$

avec λ le nombre d'éléments de l'ensemble $a, 2a, 3a, \ldots, \frac{1}{2}(m-1)a$ dont les plus petits résidus positifs sont supérieurs à $\dfrac{m}{2}$.

2 Pourquoi y a-t-il un lien entre les caractères quadratiques à $2m$ de x et $x+m$ lorsque $2m$ est un double d'impair ?

Posons $m = 2n + 1$ un nombre entier impair quelconque.
On a $x \equiv x + m \; (mod \; m)$.
Par (7) de la section 1.2, on en déduit que :

$$\left(\frac{x}{m}\right) = \left(\frac{x+m}{m}\right)$$

et par (3) de la section 1.2,

$$\left(\frac{x}{2m}\right) = \left(\frac{x}{2}\right)\left(\frac{x}{m}\right).$$

Mais comme les résidus de 2 sont les nombres impairs (2 est en facteur dans le module), alors

$$\left(\frac{x}{2m}\right) = \left(\frac{x+m}{2m}\right).$$

En fait, ce qui est peut-être intéressant dans cette propriété, c'est que si on considère la ligne du haut dans les tables, deux nombres symétriques l'un de l'autre autour de la ligne médiane ont pour somme $3m$. Exemple pour rappel de la table modulo $2 \times 45 = 90$ (nota : les résidus quadratiques sont bleus et les non-résidus noirs[2]):

[2]Indiquons entre parenthèses pour chaque résidu quadratique au carré de quel nombre il est congru modulo 90 : 1 (19) 4 (38) 9 (33) 10 (10) 16 (14) 19 (37) 25 (5) 31 (29) 34 (32) 36 (36) 40 (20) 45 (45).

90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	×						×				×						×		×			

67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45
23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
×						×		×						×						×		

31 a même caractère quadratique que $31+45 = 76$ (tous les deux résidus de 90) ou bien 5 a même caractère quadratique que 50 (tous les deux non-résidus de 90).
D'autre part, si l'on ne considère que les nombres de la ligne du haut, 62 et 73 sont symétriques par rapport à la ligne médiane et leur somme est $135 = 3 \times 45$.

3 Reprise de l'idée principale

On cherche

$$p \not\equiv n \ (mod\ p_i),\ \forall\ p_i < \sqrt{n}.$$

Dans la suite, on distingue 3 sortes de nombres premiers impairs inférieurs à $\sqrt{n}$:

- les nombres premiers inférieurs à $\sqrt{n}$ qui ne divisent pas n que l'on note α_i ;
- les diviseurs de n de puissance paire dans la factorisation de n que l'on note β_i ;
- les diviseurs de n de puissance impaire dans la factorisation de n que l'on note γ_i.

On utilise la notation de Gauss : $a\ R\ b$ signifie que $\left(\frac{a}{b}\right) = +1$ tandis que $a\ N\ b$ signifie que $\left(\frac{a}{b}\right) = -1$.

Posons $n = a^2 b$ avec a le plus grand carré divisant n et $b = \gamma_1\gamma_2\ldots\gamma_k$ le produit de tous les facteurs premiers de la factorisation de n de puissance impaire.
On cherche p tel que $\frac{1}{b}.p \not\equiv a^2\ (mod\ p_i)$.

Mais comme $\frac{1}{b}$ a même caractère de résiduosité à p, un nombre premier, que b (cf. article 109 de la section Quatrième des Recherches Arithmétiques de Gauss), cela équivaut à chercher p tel que $bp\ N\ p_i$, quel que soit p_i nombre premier impair inférieur à $\sqrt{n}$.

Puisque $b = \gamma_1\gamma_2\ldots\gamma_k$, on sait déjà que $b\ R\ \gamma_i$ quel que soit γ_i un nombre premier impair inférieur à $\sqrt{n}$.
Mais alors pour que $bp\ N\ \gamma_i$, il faut que $p\ N\ \gamma_i$.

Etudions maintenant la relation qui lie b à chacun des β_i et à chacun des α_i.

- si $b\ R\ \beta_1\beta_2\ldots\beta_j$ et $b\ R\ \alpha_1\alpha_2\ldots\alpha_i$ alors $b\ R\ p_i p_2\ldots p_n$ et on cherche p tel que $p\ N\ p_1 p_2\ldots p_n$. Pour ça, il faut compter combien il y a de nombres premiers de la forme $4n+3$ dans $p_1 p_2\ldots p_n$; s'ils sont en nombre impair et que p est de la forme $4n+3$, p doit être un décomposant ; s'ils sont en nombre pair et que p est non-résidu d'un nombre impair d'entre eux, il est non-résidu du tout, et il doit pouvoir également fournir une décomposition ;
- si $b\ N\ \beta_1\beta_2\ldots\beta_j$ et $b\ N\ \alpha_1\alpha_2\ldots\alpha_i$ alors ...
- si $b\ N\ \beta_1\beta_2\ldots\beta_j$ et $b\ R\ \alpha_1\alpha_2\ldots\alpha_i$ alors ...
- si $b\ R\ \beta_1\beta_2\ldots\beta_j$ et $b\ N\ \alpha_1\alpha_2\ldots\alpha_i$ alors ...