Voici encore une autre démonstration de la propriété du nombre 2 d'être résidu ou non résidu des nombres premiers suivant leurs formes par rapport à 8. mais celle-ci ne peut servir pour distinguer les nombres $8k+5$ des nombres ~~dans lesquels~~ $4k+1$ dans lesquels k est divisibles par une puissance paire de 2.

On peut au moins démontrer que pour les nombres $4k+3$ 2 est non résidu lorsque k est pair et ~~non~~ résidu lorsque k est impair en effet k étant $=2k'$

$p=4k+3=8k'+2+1 \quad -1\equiv 2(4k'+1)$

-1 est non résidu ; $4k'+1$ a un nombre pair de facteurs de la forme $4k-1$ parconséquent comme tous les facteurs premiers de $4k'+1$ ~~son~~ de la forme $4k+1$ sont résidus et que ceux de la forme $4k-1$ pris avec le signe $-$ sont également résidus le produit $4k'+1$ est résidu ~~po~~ d'où il résulte 2 non résidu. Au contraire lorsque $k=2k'+1$ $p=8k+7=2(4k'+3)+1$, $-1\equiv 2(4k'+3)$
$4k'+3$ a un nombre impair de facteurs de la forme $4k-1$ parconséquent c'est $-(4k'+3)$ au lieu de $4k'+3$ qui est résidu et 2 est alors résidu car $1\equiv -2(4k'+3)$

On peut encore démontrer que 2 est résidu pour les nombres $4n+1$ dans lesquels n est divisible par une puissance impaire de 2

En effet soit N pairement pair et $2n=N$ $4n+1=2N+1=p$, -1 est résidu (mod. p) aussi bien que tous les facteurs premiers de N et parconséquent leur produit et N lui-même puisqu'il est supposé ne contenir qu'une puissance paire de 2 donc à cause de $-1\equiv 2N$ 2 est aussi résidu. mais on voit que cette méthode n'apprend rien pour le cas $p=2^{2m}n+1$ —

Observations sur les nombres premiers de la forme $4n+1$ considérés comme résidus d'autres nombres premiers de même forme

Si on a un nombre premier $P=4N+1$ tel que P soit résidu de $p=4n+1$ $-P$ sera également résidu $(\bmod p)$, on aura donc

$x^2 \equiv -P \pmod p$ ou $x^2+P=Mp$.

Comme il est démontré d'ailleurs que tout nombre premier de la forme $4n+1$ est la somme de deux quarrés, on a sans aucune nouvelles suppositions, et en observant que quelque soit M il peut toujours être considéré comme la somme de quatre quarrés: et mettant A^2+B^2 au lieu de P, a^2+b^2 au lieu de p et $p^2+q^2+r^2+s^2$ au lieu de M;
$$x^2+A^2+B^2=(a^2+b^2)(p^2+q^2+r^2+s^2)$$
$$=(ap\pm bq)^2+(pb\mp qa)^2+(ar\pm bs)^2+(as\mp br)^2$$

On peut supposer $ap=bq$, $pb+qa=A$ $ar+bs=B$ $as-br=x$
des deux premières équations il résulte; d'abord de la première, à cause de a et b premiers entr'eux, $p=bm$, $q=am$, et de la seconde $A=m(b^2+a^2)$
On auroit encore pû supposer $A=ap+bq$, $pb=qa$ d'où il résulteroit $p=am'$ $q=bm'$ $A=m'(b^2+a^2)$, c'est a dire que A se réduiroit toujours au produit du nombre premier p par un nombre quelconque. Comme il est indifferent de prendre r et s au lieu de p et q puisque les quantités que ces lettres representent ne sont assujetties a aucune condition particulière, on voit que les suppositions que l'on vient d'examiner sont les seules par lesquelles on puisse égaler terme a terme les deux membres de l'équation que l'on considère; car, si on faisoit $A=pb\pm qa$ et $B=ap\mp qb$, il en resulteroit $A^2+B^2=(a^2+b^2)(p^2+q^2)$, c'est a dire, que, A^2+B^2 ne pourroit être un nombre premier

N^{ota} Je ne vois pas d'ailleurs que l'on puisse affirmer que le produit de deux nombres qui seroient, l'un et l'autre décomposables en 4 quarrés que d'une seule façon, ne le soit que de 2

c'est a dire par les racines que [illegible]

Théorème

n étant un nombre impair plus grand que l'unité, il est impossible de satisfaire en nombres entiers à l'équation $2z^{2n} = y^{2n} + x^{2n}$.

Démonstration

Nous supposerons comme à l'ordinaire, z, y et x premiers entr'eux et nous observerons que tout diviseur de z^{2n} est nécessairement la somme de deux quarrés.

Cela posé, soit, s'il se peut, $2z^{2n} = y^{2n} + x^{2n}$ et parconséquent $z^n = P^2 + Q^2$, $x^n = P^2 - Q^2 - 2PQ$, $y^n = P^2 - Q^2 + 2PQ$. En prenant $z = z'z''$, $x^{n-1} - x^{n-2}y + \&c = H$, $x^{n-1} + x^{n-2}y + \&c = F$ $z''^n = x^{2n-2} - x^{2n-4}y^2 + \&c$ et $2z'^{2n} = x^2 + y^2$ on aura : $z'^n = p^2 + q^2$, $x = p^2 - q^2 - 2pq$, $y = p^2 - q^2 + 2pq$ d'où on tire

$$\left.\begin{aligned} P^2 + Q^2 &= z''^n (p^2 + q^2) \\ P^2 - Q^2 &= H(p^2 - q^2) \\ 2PQ &= 2Fpq \end{aligned}\right\} \cdots\cdots (1)$$

Il faut encore faire $z''^n = U^2 + V^2$; la première des équations (1) donne alors $P^2 + Q^2 = (Uq \pm Vp)^2 + (Up \mp Vq)^2$, $P = Uq \pm Vp$ et $Q = Up \mp Vq$. En substituant ces valeurs de P et de Q dans les deux dernières des équations (1) elles deviennent

$$\left.\begin{aligned} \{U(p+q) \pm V(p-q)\}\{U(q-p) \pm V(p+q)\} &= H(p^2 - q^2) \\ 2\{(U^2 - V^2)pq \pm (p^2 - q^2)VU\} &= 2Fpq \end{aligned}\right\} \cdots (2)$$

On voit par la première que VU doit être divisible par $p^2 - q^2$; la seconde montre que le même produit VU doit aussi être divisible par pq.

Soit $z''^{n-1} = V'^2 + U'^2$, $z'' = v^2 + u^2$ et parconséquent

$z''^n = U^2 + V^2 = (U'u \pm V'v)^2 + (U'v \mp V'u)^2$, $U = U'u \pm V'v$, $V = U'v \mp V'u$, $VU = (U'^2 - V'^2)vu \pm (v^2 - u^2)V'U'$.

Les valeurs de VU données par l'un et l'autre signes devront également satisfaire ; ainsi, leur somme $2(U'^2 - V'^2)vu$, et leur différence, $2(v^2 - u^2)U'V'$, seront l'une et l'autre divisibles par $pq(p^2 - q^2)$.

En supposant, comme on le doit V' et U' premiers entr'eux, $U'^2 - V'^2$ et $V'U'$ seront également premiers entr'eux, parconséquent $V'U'$ ne peut avoir d'autre diviseur commun avec $2(U'^2 - V'^2)vu$ que le produit vu.

Par la même raison $U'^2 - V'^2$ ne peut avoir d'autre diviseur commun avec $2(v^2-u^2)UV$ que le nombre v^2-u^2; il faut donc que $2(v^2-u^2)vu$ soit divisible par $(p^2-q^2)pq$.

On ne peut satisfaire a cette condition qu'a l'aide de l'une ou l'autre des suppositions : $2(v^2-u^2)vu > pq(p^2-q^2)$, $2(v^2-u^2)vu = 0$.

Examinons d'abord la première.

En mettant pour p et q leurs valeurs, $2(v^2-u^2)uv > pq(p^2-q^2)$ donne $32(v^2-u^2)vu > 2(y^2-x^2)$. A cause de $2(y-x) = 8pq$ et $y+x = 2(p^2-q^2)$, $2(y^2-x^2)$ est $> (x+y)^2$. La même supposition donne donc aussi $32(v^2-u^2)vu > (x+y)^2$.

Il résulte de l'équation $2z^{2n} = x^{2n} + y^{2n}$ que $z^{2n} = z'^{2n}(v^2+u^2)^{2n}$ est plus petit que y^{2n}. $z'^2(v^2+u^2)^2 < y^2$ et a plus forte raison $2z'^2(v^2+u^2)vu < y^2$. Il faut encore observer que z' étant impair et la somme de deux quarrés on a $z' > 4$; parconséquent $32(v^2+u^2)vu < 2z'^2(v^2+u^2)vu$ et $32(v^2+u^2)vu < y^2$. On ne peut donc supposer dans aucun cas $32(v^2-u^2)vu > (y+x)^2$.

Voyons aprésent quels sont ceux dans lesquels on peut satisfaire a l'équation $2(v^2-u^2)vu = 0$.

Si on prend $v^2-u^2 = 0$, les nombres x et y ne pourront être premiers entr'eux; c'est cequ'il est aisé de voir a l'aide des équations (2) car les quantités F et H ayant alors un commun diviseur, il faudra que x et y ayent pareillement aussi un diviseur commun.

Si on veut que l'un des facteurs v ou u, v, par exemple, soit nul, on verra de même que x et y ne pourront être premiers entr'eux que dans le seul cas ou l'on auroit en même tems $u = 1$. Soit donc $u = 1$, $v = 0$. on trouvera $U = 1$, $V = 0$, $P = p$, $Q = q$, $x^n = x$, $y^n = y$ et enfin $n = 1$. Ce cas est donc le seul dans lequel il soit possible de satisfaire a l'équation $2z^{2n} = y^{2n} + x^{2n}$.

—

La même démonstration s'appliqueroit également a l'impossibilité de l'équation $2z^{2n} = y^{2(n-2d)} + x^{2(n-2d)}$; il faudroit seulement mettre $n-2d$ aulieu de $\underline{n}$ dans les valeurs de P Q et z''^{2n} ce qui ne changeroit rien a la forme des équations (1) et (2).

On seroit mené, comme dans le cas du théorème precedent, a l'une ou l'autre des suppositions $2(v^2-u^2)vu > pq(p^2-q^2)$ ou $2(v^2-u^2)vu = 0$. L'impossibilité de la première resulteroit, à plus forte raison de la condition $z'^{2n}(v^2+u^2)^{2n} < y^{2n-4d}$. La seconde donneroit toujours $u=1$, $v=0$, $\mathrm{V}=0$, $\mathrm{U}=1$, $\mathrm{P}=p$, $\mathrm{Q}=q$, et parconséquent $x^{n-2d}=x$, $y^{n-2d}=y$ $n-2d=1$.

En mettant $\underline{n}$ aulieu de $n-2d$ et réciproquement $n+2d$ aulieu de $\underline{n}$ on pourra donc établir le théorème suivant:

Si $\underline{n}$ est un nombre impair plus grand que l'unité, quelque soit d'ailleurs le nombre $\underline{d}$, il est impossible de satisfaire en nombres entiers a l'équation $2z^{2(n+2d)} = x^{2n} + y^{2n}$

Théorème

Pour toute valeur de n plus grande que l'unité il est impossible de satisfaire en nombres entiers a l'équation $\mathrm{Z}^{2n} = \mathrm{X}^{2n} + \mathrm{Y}^{2n}$.

Démonstration

Si l'équation $\mathrm{Z}^{2n} = \mathrm{X}^{2n} + \mathrm{Y}^{2n}$ étoit possible l'un des nombres X et Y seroit pair on auroit donc en prenant $\mathrm{X} = 2xx'$

$$x = \cdots (x)$$
$$= \cdots (x')'$$
$$= \cdots (x'')''$$

$$\mathrm{Z}^n \pm \mathrm{Y}^n = 2x'^{2n}$$

$$\mathrm{Z}^n \mp \mathrm{Y}^n = 2^{2n-1} x^{2n} \qquad \mathrm{Z} \mp \mathrm{Y} = 2^{2n-1}(x)^{2n}$$

$$\mathrm{Z}^n = x'^{2n} + 2^{2n-2} x^{2n} \qquad \mathrm{Z} - x'^2 = 2^{2n-2}(x)'^{2n}$$

$$\pm \mathrm{Y}^n = x'^{2n} - 2^{2n-2} x^{2n} \qquad x'^2 \mp \mathrm{Y} = 2^{2n-2}(x)''^{2n}$$

et parconséquent $2^{n-1}(x)^{2n} = 2^{2n-2}\{(x)'^{2n} + (x)''^{2n}\}$, $2(x)^{2n} = (x)'^{2n} + (x)''^{2n}$ équation dont l'impossibilité vient d'être demontrée pour toute valeur de $\underline{n}$ plus grande que l'unité.

est non residu d'un nombre premier de la même forme $24k+13$

que, l'auteur ne dit rien des nombres de la forme $24k+13$.

J'observe que l'on peut demontrer que les nombres $12n+7$ (lesquels font partie de ceux $24k+13$) sont non residus pour quelques nombres premiers moindres que les nombres dont il s'agit.

En effet si on prend pour a le nombre pair immédiatement plus grand que $\sqrt{\frac{p}{3}}$, en faisant $p=12n+7$ $3aa-p$ sera $<$ que p et de la forme $12k+5$.

or en examinant tous les produit des nombres non divisibles par 12 on voit qu'un nombre $12k+5$ a pour facteur un nombre de la forme $12k+1$ et un de celle $12k+5$. ou est le produit de $12k+11$ par $12k+7$. dans le premier cas soit $12k+5=q$ on aura $3aa\equiv p$ (mod. q) mais pour les nombres $12k+5$ $+3$ et -3 sont non residus et parconsequent p est non residu (mod. q)

dans le second soit $q=12k+7$ on a a ceux de -3 residu, mais $+3$ non residu (mod. q) p non residu même modul.

On peut demontrer la même chose pour les nombres $12k+5$.

A l'égard des nombres $120k+1$ il n'y a qu'à prendre un nombre $10n+2 > \sqrt{\frac{5}{2}\cdot 120k+1}$

$2(10n+2)^2 - 5(120k+1)$ sera un nombre de la forme $40k+11$ mais pour les nombres $8n+3$ (Pt. 11) 2 est non résidu et pour les nombres $20k+11$ 5 est résidu (Pt. 9) donc si $40k+11$ est le produit des deux facteurs $40k+1$, $40k+11$ et que l'on fasse $4k+11=q$

$2(10n+2)^2 \equiv 5(120k+1) \pmod q$ à cause de 2 non résidu le premier membre est non résidu et par conséquent à cause de 5 résidu $120k+1$ non résidu (mod. q)

1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39

$29\cdot 39 \equiv 11$ $q = 40k+29$ 2 non résidu 5 résidu

$9\cdot 19 \equiv 11$ $q = 40k+19$ 2 non résidu 5 résidu

$21\cdot 31 \equiv 11$ $q = 40k+21$ 2 non résidu 5 résidu

$33\cdot 27 \equiv 11$ $q \equiv 40k+27$ 2 non résidu 5 résidu

$07\cdot 13 \equiv 11$ $q \equiv 40k+13$ 2 non résidu 5 résidu

$37\cdot 23 \equiv 11$ $q \equiv 40k+37$

$3\cdot 17 \equiv 11$

en effet soit a le nombre pair immédiatement plus petit que $\sqrt{\frac{p}{3}}$ dans lequel $p = 12n+5$ $p - 3aa$ sera plus petit que p ce nombre sera de la forme $12k+5$ et on conclura comme ci-dessus qu'il doit être le produit de $12k+5$ par $12k+1$ ou celui de $12k+11$ par $12k+7$. d'où il résulte que dans le premier cas p est non résidu (mod $12k+5$) et dans le second non résidu (mod $12k+7$)

En examinant la manière dont Gauss démontre (N° 145) que tout nombre premier $p=4n+1$ pris négativement est non résidu d'un nombre premier moindre que p on voit que la même démonstration serait applicable au cas où p ne serait pas premier de sorte que l'on peut affirmer que tout nombre de la forme $4n+1$ pris négativement est non résidu de quelque nombre premier moindre que lui et de la forme $4n+3$. On voit dans la feuille ci-jointe que tout nombre de la forme $4k+3$ pris négativement est non résidu d'un nombre ~~de la~~ premier de la même forme et moindre que lui il résulte des ces remarques que : Tout nombre impair $2N+1$ pris avec le signe $-$ est non résidu d'un nombre premier de la forme $4k+3$ et $<$ que $2N+1$

Je me propose de démontrer qu'un nombre quelconque de la forme $4k+3$, pris, tant avec le signe $+$, qu'avec le signe $-$, est non résidu de quelque nombre premier moindre que lui.

D'abord soit $p=4k+3$ et soit proposé de prouver que $-p$ est non résidu d'un nombre $<$ que lui. Prenons $2a$ pour le nombre pair immédiatement $<\sqrt{p}$ $p-4aa$ sera positif et de la forme $4k+3$ et de plus ce nombre est évidemment $<$ que p. il est clair que $p-4aa$ est premier ou divisible par un nombre premier de la forme $4k+3$. soit q ce nombre on aura $p \equiv 4aa \pmod{q}$ c'est à dire p résidu (mod. q) et par conséquent $-p$ non résidu.

Pour les nombres premiers $4k+3$ positivement pris nous distinguerons deux cas premièrement si p est de la forme $8k+3$. ~~soit a un nombre quelconque~~
soit $2a$ le nombre pair immédiatement $<$ que $\sqrt{\frac{p}{2}}$ $p-8aa$ sera de la forme $8k+3$ et moindre que p. ce nombre sera ou premier ou le produit des facteurs $8k+1$ $8k+3$ ~~et~~ $8k+7$ $8k+5$ ~~et~~ ce sont de 2 non résidu (mod. $8k+3$) et (mod. $8k+5$) nommons q le facteur de l'une de ces formes qui divise $p-8aa$ on aura $p \equiv 2(2a)^2 \pmod{q}$ d'où il résulte p non résidu même modul.

Secondement si p est de la forme $8k+7$. soit a un nombre impair $<$ que $\sqrt{\frac{p}{2}}$ $p-2aa$ sera de la forme $8k+5$ or tout nombre $8k+5$ s'il n'est premier a pour facteur $8k+1$ et $8k+5$, ou $8k+7$ et $8k+3$ nommons donc q le facteur de l'une des formes $8k+5$ et $8k+3$ qui divise $p-2aa$ et nous conclurons comme ci-dessus $p \equiv 2aa \pmod{q}$ p non résidu (mod q).

La condition que $2a$ soit immédiatement plus petit de $\sqrt{p}$, dans le premier cas démontré, et ~~de~~ $\sqrt{\frac{p}{2}}$ dans le second, est évidemment superflue; il suffit de prendre $2a <$ que $\sqrt{p}$ et $2a < \sqrt{\frac{p}{2}}$.

[illegible] $4k+3$ Le but de l'auteur étant de passer au théorème fondamental il s'est borné à démontrer que les nombres $4k+3$ tant positifs que négatifs sont non résidus. Il faut examiner si on ne pourrait pas faire usage [illegible] pour prouver

Je me propose de démontrer qu'un nombre quelconque de la forme $4n+3$, pris tant avec le signe $+$ qu'avec le signe $-$, est non résidu de quelque nombre premier moindre que lui.

D'abord soit $p=4n+3$ et soit proposé de démontrer que p est non résidu d'un nombre $<$ que lui. [illegible]

[illegible]

Si on se bornoit à vouloir démontrer que tout nombre de la forme $3k-1$ ~~est~~ non résidu d'un nombre premier, sans exiger que ce nombre soit $<$ que $3k-1$; on y parviendroit en considérant un nombre de la forme $p+3aa$ dans lequel $p=3k-1$; car, $p+3aa$ est de la forme $3k-1$ et par conséquent il est, ou premier, ou divisible par un nombre de la même forme ; soit q ce nombre, on a $p\equiv -3aa$ (mod. q) mais -3 est non résidu pour tout nombre de la forme $3k-1$ donc p est aussi non résidu (mod. q)
si p est pair a doit être supposé impair, et pair si p est impair afin que $p+3aa$ soit un nombre impair. car si ce nombre étoit pair il seroit possible que 2 fut le seul nombre $3k-1$ qui le divise et on sait que ~~tout nombre est divisible~~ tout nombre impair $\equiv 1$ (mod. 2) ~~-3 est résidu mod. 2~~
On voit que dans la suite des différentes valeurs que l'on peut donner à a il doit se trouver des valeurs de $p+3aa$ divisibles par des valeurs de $q > p$. mais je ne sais pas le démontrer

p. 125 L'auteur se borne à démontrer le cas des nombres premiers de la forme $4n+1$ parcequ'il n'emploie que celui-là dans sa démonstration de son théorème ~~fondamental~~ (V. n° 139. & 146) si on vouloit démontrer la proposition générale :

Tout nombre, excepté les quarrés positivement pris, est non résidu de quelque nombre premier.

Nous observerons qu'en supposant la chose accordée pour les nombres $4n+1$ il ne reste à examiner que ceux $4n+2$, $4n+3$ parceque les nombres $4n$ étant multiples d'un quarré seront non résidus si n l'est.

Pour les nombres $4n+2$

soit $4n+2+(2k+1)^2$ ce nombre est de la forme $4h+3$ et par conséquent divisible par un nombre premier de la même forme soit q ce nombre on aura $4n+2\equiv -(2k+1)^2$ et à cause de -1 non résidu (mod. $4h+3$) $4n+2$ sera également non résidu (mod. $4h+3=q$). Je n'ai pas vu comment démontrer $-(4n+2)$ non résidu il est clair que parmi les nombres de la forme $3k-1$ il s'en trouvent qui sont en même tems de celle $8n+5$; tels sont ceux de la forme $24n+17$.

Pour les nombres $4n+3$ positivement pris

soit $4n+3+4k^2$ un nombre tjrs de la forme $4k+3$ et par conséquent divisible par un nombre premier, q de la même forme et a cause de -1 non résidu mod q ; il résulte de $4n+3 \equiv -4k^2$ (mod q) ... $4n+3$ non résidu (mod q)

.....

Pour les nombres $4n+3$ négativement pris

soit $4n+3 \equiv 4k^2$, $4n+3-4k^2$ sera toujours de la forme $4k+3$ donc divisible par un nombre premier q de la même forme ; il est clair que $4n+3$ est ici résidu (mod q). Donc a cause de -1 non résidu $-(4n+3)$ non résidu (mod. q)

de la comparaison des deux cas que nous venons de traiter il résulte cette proposition remarquable : tout nombre de la forme $4k+3$ pris tant avec le signe + qu'avec le signe −

Il s'agit de prouver qu'un nombre premier quelconque de la forme $8n+1$, pris avec le signe $+$, est toujours non résidu d'un autre nombre premier plus petit que lui.

Les nombres premiers $8n+1$, appartiennent à l'une ou l'autre des formes $24k+1$, $24k+17$.

Nous examinerons d'abord les nombre $24k+17$. et nous observerons qu'ils sont compris dans cette forme $12k+5$. Nous supposerons donc qu'il s'agisse de prouver qu'un nombre premier $p=12k+5$ est non résidu d'un nombre premier moindre que lui. pour cela, en designant par $\underline{a}$ un nombre quelconque (pair) et $<\sqrt{\frac{p}{3}}$, le nombre $p-3aa$ sera positif $<$ que p et de la forme $12k+5$. Or tout nombre premier appartient a l'une des quatre formes suivantes $12k+1$, $12k+5$, $12k+7$, $12k+11$: et parmi les six produits differens des quarrés il n'y a que $12k+1$ par $12k+5$ et $12k+7$ par $12k+11$ qui soient de la forme $12k+5$. posons donc, a cause de 3 non-résidu mod. $12k+5$ et $12k+7$, (S. P. 116) $q=12k+5$ ou $=12k+7$ et nous aurons $p\equiv 3aa \pmod q$ c'est a dire p non résidu mod q: et q sera evidemment $<p$ puisqu'il est facteur d'une quantité moindre que ce nombre. ce qu'il fallait demontrer.

A l'égard des nombres $24k+1$ nous observerons qu'ils sont la somme de deux quarrés. puisque cette propriété appartient généralement a tous les nombres premiers de la forme $4n+1$. Or, en considérant les formes de x et y, dans x^2+y^2 par rapport au nombre 5, on voit que, si on fait $x=5n\pm1$ ou $=5n\pm2$ il faut, pour que x^2+y^2 soit un nombre premier, que y^2 soit ou de la même forme que x^2, ou un multiple de 5: en effet: si on faisoit $x=5n\pm1$ et $y=5n\pm2$ on auroit

$$x^2+y^2=25n\pm2\cdot5n+1$$
$$+25n\pm2\cdot5\cdot2n+4\equiv0 \pmod 5$$

361

Si ς est non résidu des nombres premiers compris sous la forme E ς sera aussi non résidu d'un des facteur des nombres de la même forme E qui ne sont pas premiers c'est à dire que le produit d'un nombre quelconque de nombres premiers pour lesquels ς est résidu ne pourra jamais être de la forme E qui renferme les nombres premiers pour lesquels ς est non résidu.

-3 est non résidu des nombres premiers compris sous la forme $3n-1$ -3 sera aussi non résidu d'un des facteurs des nombres de la même forme qui ne sont pas premiers c'est à dire que le produit d'un nombre quelconque de nombres premiers de la forme $3n+1$ pour lesquels -3 est résidu ne pourra jamais être de la forme $3n-1$

360

Supposons que tous les nombres premiers, jusqu'à P, pour lesquels a est résidu, soient de la forme $ma+b^2$ et en prenant e pair et non divisible par a faisons $e^2=a+fP$ f ~~est~~ impair on a $e^2\equiv a \pmod f$ c'est à dire a résidu mod. f par conséquent mod. tout facteur de f, mais comme $f<P$ tous ces facteurs seront à plus forte raison $<P$ par conséquent de la forme $ma+b^2$ $(b<a)$
et le produit de tant de nombre de la forme $ma+b^2$ que l'on voudra sera de cette même forme laquelle appartient aussi au quarré e^2 donc aussi à P

si $ma+b^2=p$ et que $p<a$
m est negatif

Supposons que tous les nombres premiers, jusqu'à P, pour lesquels a est résidu, soient de la forme $ma+b^2$ et un premier c pair et non divisible par a. Soit $c^2 = a + fP$ f impair $< a$. $c^2 = a$ (mod f) c'est à dire a résidu mod f par conséquent résidu tout facteur de f, mais comme $f < P$ tous ces facteurs seront a plus forte raison $< P$ par conséquent de la forme $ma+b^2$ $(b < a)$

et le produit de tout de nombres de la forme $ma+b^2$ qu'on considère sera de cette même forme laquelle appartient aussi au quarré c^2 donc aussi à P

Si $ma+b^2 = p$ et que $p < a$ m est négatif

p. 116.

Pour tout nombre premier de la forme $4k+3$ si n est non-résidu $-n$ sera résidu en effet prenant la racine primitive r et supposant $r^{2f+1} = n$ si on voulait que $r^{2g+1} = -n$ on aurait

$$r^{2g+1} + r^{2f+1} = 0$$

$$r^{2(g-f)} + 1 = 0$$ c'est à dire -1 résidu.

L'induction a mis l'auteur à établir pour les nombres $12n+11$ 3 résidu et -3 non résidu je ne vois pas qu'on puisse rien conclure pour ces nombres de la formule $4(a^3-1) = (2n+1)f+3$ mais à l'égard des nombres compris sous la forme $4k+1$ à cause de $+1$ et $-n$ résidu ou non résidu si on voulait que 3 fût résidu

$$r^{nk} = f$$
$$r^{mk} = -f$$
$$r^{nk} + r^{mk} = 0$$
$$r^{(n-m)k} + 1 = 0$$

$$A = ma + b^2$$
$$a = d^2 - nA$$
$$A = md^2 - mnA + b^2$$
$$(1+mn)A = md^2 + b^2$$
$$a = d^2 - n(ma + b^2)$$
$$(1+mn)a = d^2 - nb^2$$

étant le nombre de lettres
la déterminante de l'o…
de l'ordre n+1 la déte…
l'ordre n dans laquelle…
les coefficients de la…
supérieure ceux de l…
de l'ordre n² no…

Pour tout nombre premier $12n+5$ dans lesquels $3n+1$ est premier 3 est racine primitive

En effet pour les nombres $12n+5$ 3 est non-résidu par conséquent si 3 n'est pas racine primitive on aura $r^{3n+1} \equiv 3$ puisque 4 et $3n+1$ sont les seuls facteurs de $p-1$ ainsi à cause de $r^{4(3n+1)} \equiv 1$, $3^4 \equiv 1$, $3^2+1 \equiv 0$ mais $3^2+1 = 10$ est < que $12n+5$ donc &c.

tels sont
$4 \cdot 7+1=29$
$4 \cdot 13+1=53$
$4 \cdot 19+1=77$
$4 \cdot 23+1=93$:

~~Soit en général $3n+1 = p^n$~~ [illegible]

$3(r^{(v-1)p} - (3n+1)$ [illegible]

$3r^{(v-1)p}$

Nombres premiers de la forme $2^{2^i}+1$

T. Si aRa' $a'Ra$

Soit $a'>a$ pour que la condition $a'Ra$ soit satisfaite il faut que $a'=ma+d^2$ d étant $<a$.

Il résulte de là que, pour tout nombre premier $2^{2^i}+1$ les nombres premiers plus petits et de même forme sont non résidus et par conséquent racines primitives

En effet soit $2^{2^{i+\delta}}+1$ un nombre premier ; pour prouver qu'il ne peut être résidu (mod. $2^{2^i}+1$) on mettra $2^{2^{i+\delta}}+1$ sous une autre forme, et on trouvera

$$2^{2^{i+\delta}}+1=(2^{2^i\cdot m}-1)\,2^{2^{i+\delta}-2^i\cdot m}+2^{2^{i+\delta}-2^i\cdot m}+1$$

$$=2^{2^{i+\delta}-2^i\cdot m}\cdot(2^{2^i}+1)\{2^{m(2^i-1)}-2^{m(2^i-2)}+\cdots-1\}+2^{2^{i+\delta}-2^i m}+1$$

on prendra m de manière que $2^{2^{i+\delta}-2^i m}+1$ soit $<(2^{2^i}+1)^2$ et il faudra pour satisfaire à la condition $a'=ma+d^2$ que $2^{2^{i+\delta}-2^i m}+1$ soit un quarré c'est ce qui ne peut avoir lieu puisque le seul cas où 2^x+1 soit quarré est celui où $x=3$.

cela est faux parce qu'il suffit que $2^{2^{i+\delta}-2^i\cdot m}+1=a^2$

De même à cause de T. si bRa aRb

a étant $>b$ on a $a=mb+d^2$ $d<b$

Soit a $2^{2^i}+1$ et $b=2^n-1$ on aura

$$2^{2^i}+1=2^{2^i-xn}(2^{xn}-1)+2^{2^i-nx}+1.$$

$$=2^{2^i-xn}(2^n-1)\{2^{n(x-1)}+2^{n(x-2)}+\cdots+1\}+2^{2^i-nx}+1$$

on prendra x de manière que $2^{2^i-nx}+1$ soit $<(2^n-1)^2$

il faut pour satisfaire que $2^i-nx=3$ par conséquent n ne peut être $n=2$ $n=3$ c'est à dire que $2^2-1=3$ et $2^3-1=7$ sont non résidus (mod $2^{2^i}+1$) c'est ce que j'avois déja trouvé d'une autre manière