NOUVELLES ANNALES DE MATHÉMATIQUES

C. MOREAU

Sur quelques théorèmes d'arithmétique

Nouvelles annales de mathématiques 3^e série, tome 17 (1898), p. 293-307

<http://www.numdam.org/item?id=NAM_1898_3_17__293_0>

[I2c]

SUR QUELQUES THÉORÈMES D'ARITHMÉTIQUE;

PAR M. C. MOREAU,
Colonel d'Artillerie en retraite.

THÉORÈME I. — *Les restes de la division par p de p termes successifs d'une progression arithmétique de raison* N, *p et* N *étant premiers entre eux, sont dans un certain ordre, en n'admettant pas de reste nul, les p premiers nombres*

$$1,\quad 2,\quad 3,\quad \ldots,\quad (p-1),\quad p. \tag{1}$$

En effet, soit

$$\left\{\begin{array}{l} a,\quad a+\mathrm{N},\quad \ldots,\quad a+\mathrm{KN},\quad \ldots, \\ a+\mathrm{K'N},\quad \ldots,\quad a+(p-1)\mathrm{N} \end{array}\right. \tag{2}$$

la progression arithmétique considérée; les restes de la division de ses termes par p sont, en n'admettant pas de reste nul, au plus égaux à p; de plus, ils sont tous différents; car si, par exemple, $a+\mathrm{KN}$ et $a+\mathrm{K'N}$ donnaient le même reste, il en résulterait que p diviserait la différence $(\mathrm{K'}-\mathrm{K})\mathrm{N}$, ce qui est impossible, puisqu'il est premier avec N et forcément plus grand que $\mathrm{K'}-\mathrm{K}$; ces restes sont donc, dans un certain ordre, les termes de la suite (1).

COROLLAIRE. — Il y a dans la suite (2) autant de nombres premiers avec p que dans la suite (1) et il s'y trouve un terme, et un seul, divisible par p.

Définition.— On appelle *indicateur* d'un nombre N, et l'on désigne par la notation $\varphi(\mathrm{N})$ le nombre qui

exprime combien la suite

$$1,\quad 2,\quad 3,\quad \ldots,\quad (N-1),\quad N$$

contient de termes premiers avec N.

D'après cette définition, on a

$$\varphi(1)=1,\qquad \varphi(2)=1,\qquad \varphi(N)=N-1$$

lorsque N est un nombre premier.

THÉORÈME II. — *Si l'on multiplie un nombre quelconque* N *par un nombre premier* p, *on a*

$$\varphi(pN)=p\,\varphi(N)\qquad \text{ou}\qquad (p-1)\,\varphi(N),$$

suivant que p *divise ou ne divise pas* N.

Pour le démontrer formons le Tableau des pN premiers nombres en les écrivant par rangées successives de N nombres

$1,$	$2,$	$3,$	$\ldots$	$a,$	$\ldots,$	$N-1,$	N
$1+N,$	$2+N,$	$3+N,$	$\ldots$	$a+N,$	$\ldots,$	$2N-1,$	$2N$
$\ldots\ldots$	$\ldots\ldots,$	$\ldots\ldots,$	$\ldots,$	$\ldots\ldots,$	$\ldots$	$\ldots\ldots,$	$\ldots$
$1+kN,$	$2+kN,$	$3+kN,$	$\ldots,$	$a+kN,$	$\ldots,$	$(k-1)N-1,$	$(k-1)N$
$\ldots\ldots,$	$\ldots\ldots,$	$\ldots\ldots,$	$\ldots,$	$\ldots\ldots,$	$\ldots$	$\ldots\ldots,$	$\ldots\ldots$
$1+(p-1)N,$	$2+(p-1)N,$	$3+(p-1)N,$	$\ldots,$	$a+(p-1)N,$	$\ldots,$	$pN-1,$	pN

et cherchons combien il y en a qui sont premiers avec le produit pN.

Prenons le terme quelconque $a+KN$. Pour que ce terme soit premier avec pN, il faut qu'il le soit avec N et cela ne peut arriver que si a lui-même est premier avec N; les nombres cherchés ne peuvent donc se rencontrer que dans les $\varphi(N)$ colonnes commençant par ceux des nombres de la première rangée qui sont premiers avec N. Voyons maintenant combien chacune de ces colonnes en contient, par exemple celle commençant par a.

Premier cas : *Le nombre premier p divise* N. — Les p termes de la colonne considérée étant premiers avec N le sont aussi avec le produit pN qui ne contient pas de facteurs premiers étrangers à N. Ainsi, dans ce cas, on a

$$\varphi(p\mathrm{N}) = p\varphi(\mathrm{N}).$$

Deuxième cas : *Le nombre premier p ne divise pas* N. — Les p termes de la colonne considérée forment une progression arithmétique de raison N; or, d'après le corollaire du théorème I, p étant premier avec N, il y a dans cette progression autant de termes premiers avec p que dans la suite des p premiers nombres, c'est-à-dire $p-1$, et ces $p-1$ nombres étant à la fois premiers avec N et avec p le sont avec le produit pN. Ainsi, dans ce cas, on a

$$\varphi(p\mathrm{N}) = (p-1)\varphi(\mathrm{N}).$$

Corollaire I. — Il résulte de ce qui précède que, si $p, q, r, \ldots$ sont les facteurs premiers entrant dans la composition de N, on a

$$(3) \qquad \varphi(\mathrm{N}) = \frac{\mathrm{N}}{pqr\ldots}(p-1)(q-1)(r-1)\ldots,$$

ce que l'on écrit aussi

$$(4) \qquad \varphi(\mathrm{N}) = \mathrm{N}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\ldots.$$

Corollaire II. — M et N étant deux nombres quelconques premiers entre eux, on a

$$\varphi(\mathrm{MN}) = \varphi(\mathrm{M})\varphi(\mathrm{N}).$$

Si, au contraire, M ne contient pas de facteurs premiers étrangers à N, on a

$$\varphi(\mathrm{MN}) = \mathrm{M}\varphi(\mathrm{N}).$$

Remarque. — $\varphi(N)$ est toujours un nombre pair, excepté pour $N = 1$ ou 2.

THÉORÈME III. — *Si l'on multiplie les* $\varphi(N)$ *nombres qui ne surpassent pas* N *et sont premiers avec lui, par l'un quelconque d'entre eux, on obtient une suite de termes dont les restes de la division par* N *sont dans un certain ordre les* $\varphi(N)$ *nombres desquels on est parti.*

Soient, en effet,

$$1,\ a,\ b,\ c,\ \ldots,\ N-1, \tag{5}$$

les $\varphi(N)$ nombres qui ne surpassent pas N et sont premiers avec lui; en les multipliant, par exemple, par a, nous aurons une suite de termes

$$a,\ a^2,\ ab,\ ac,\ \ldots,\ a(N-1) \tag{6}$$

qui seront tous premiers avec N : donc les restes de la division par ce nombre seront également premiers avec lui et feront, en conséquence, partie de la suite (5); de plus, ces restes sont tous différents, car si deux termes quelconques ab et ac donnaient le même reste, il en résulterait que N diviserait leur différence $(c-b)a$, ce qui est impossible, puisqu'il est premier avec a et forcément plus grand que $c-b$; ce sont donc, dans un certain ordre, les nombres mêmes de la suite (5).

COROLLAIRE. — Ce théorème montre que, si l'on désigne par A un nombre quelconque de la suite (5), il existe dans la suite (6) un terme, et un seul, qui, divisé par N, donne A pour reste. On peut donc dire qu'a chaque nombre a de la suite (5) en correspond un autre b tel que $ab - A$ soit divisible par N, à moins

que a ne se corresponde à lui-même et que N ne divise $a^2 - A$.

Ainsi, les nombres de la suite (5) sont de deux espèces par rapport à A :

1° Ceux a, b, c, d, ... qui sont tels que les différences $ab - A$, $cd - A$, ... soient divisibles par N ; ils sont dits *associés deux à deux par rapport à* A *pour le module* N ;

2° Ceux α, β, ... qui sont tels que les différences $\alpha^2 - A$, $\beta^2 - A$, ... soient divisibles par N ; ils sont dits *égaux à leurs associés par rapport à* A *pour le module* N et nous en désignerons le nombre par la notation $\mu_A(N)$.

Remarque. — Il est à remarquer que les nombres de cette dernière catégorie sont deux à deux complémentaires à N, car il est évident que, si $\alpha^2 - A$ est divisible par N, il en est de même de $(N - \alpha)^2 - A$.

Il y a lieu d'examiner en particulier le cas de $A = 1$ et de déterminer combien il y a alors de nombres égaux a leurs associés par rapport à 1, ou simplement égaux à leurs associés, pour le module N.

Théorème IV. — *Le nombre* $\mu_1(N)$ *des nombres égaux à leurs associés pour le module* N *peut être représenté par une puissance de* 2 *dont l'exposant est égal au nombre des facteurs premiers impairs entrant dans la composition de* N *augmenté de* 0, *de* 1 *ou de* 2, *suivant que le facteur* 2 *y entre lui-même au plus une fois, deux fois ou plus de deux fois.*

La démonstration de ce théorème repose sur les considérations qui vont être exposées.

Premier cas : *Lorsque* N *est une puissance de* 2, *on a*

$$\mu_1(N) = 1, 2 \text{ ou } 4,$$

suivant que l'exposant de cette puissance est 1, 2 *ou est supérieur à* 2.

Les deux premiers résultats sont évidents. Quant au troisième, pour que $\alpha^2 - 1 = (\alpha - 1)(\alpha + 1)$ soit divisible par N, il faut que l'un des deux nombres $\alpha - 1$ ou $\alpha + 1$ soit divisible par $\frac{N}{2}$, car, N étant une puissance de 2, ces nombres sont des nombres pairs consécutifs dont l'un ne contient, par conséquent, qu'une fois le facteur 2; or il n'y a que quatre valeurs de α pour lesquelles cette condition soit remplie, savoir : 1, $\frac{N}{2} - 1$, $\frac{N}{2} + 1$, $N - 1$, ce qui démontre le troisième résultat.

Deuxième cas : *Lorsque* N *est un nombre premier impair, on a*

$$\mu_1(N) = 2.$$

En effet, le nombre premier N doit diviser $\alpha - 1$ ou $\alpha + 1$ et cela ne peut arriver, α étant inférieur à N, que pour $\alpha = 1$ et $\alpha = N - 1$.

Troisième cas : *Si l'on multiplie un nombre quelconque* N *par un nombre premier impair* p, *on a*

$$\mu_1(pN) = \mu_1(N) \quad \text{ou} \quad 2\mu_1(N),$$

suivant que p *divise ou ne divise pas* N.

Écrivons de la même manière que précédemment le Tableau des pN premiers nombres et cherchons com-

bien il y en a dont le carré, diminué d'une unité, soit divisible par pN.

1,	2,	3,	...,	α,	...,	$N-1$,	N
$1+N$,	$2+N$,	$3+N$,	...,	$\alpha+N$,	...,	$2N-1$,	$2N$
.....,	.....,	.....,	...,	.....	.....	.....,	...
$1+KN$,	$2+KN$,	$3+KN$,	...,	$\alpha+KN$,	...,	$(K+1)N-1$,	$(K+1)N$
.....,	.....	.....	.....	.....,	.....	.....,	.....
$1+(p-1)N$,	$2+(p-1)N$,	$3+(p-1)N$,	...,	$\alpha+(p-1)N$,	...,	$pN-1$,	pN

Prenons le terme quelconque $\alpha+KN$, son carré, diminué de 1, est $\alpha^2-1+2\alpha KN+K^2N^2$, et il est clair que cette quantité n'est divisible par N que si α^2-1 lui-même l'est; on ne peut donc rencontrer les nombres cherchés que dans les colonnes commençant par les $\mu_1(N)$ nombres jouissant de la même propriété par rapport à N. Voyons maintenant combien chacune de ces colonnes en contient, par exemple celle commençant par α.

Le nombre premier impair p divise N. — Pour que $\alpha^2-1+2\alpha KN+K^2N^2$ soit divisible par pN, il faut et il suffit que $\frac{\alpha^2-1}{N}+2\alpha K+K^2N$ ou, puisque p est facteur de N, que $\frac{\alpha^2-1}{N}+2\alpha K$ soit divisible par p; faisons la même opération sur tous les nombres de cette colonne, nous obtiendrons p termes successifs d'une progression arithmétique de raison 2α; or p est premier avec 2α puisqu'il est impair et que, divisant N, il ne peut diviser α qui est premier avec N: donc (théorème I, corollaire) cette progression contient un terme et un seul divisible par p. Ainsi, dans chaque colonne commençant par un nombre tel que α, il y a un nombre et un seul dont le carré, diminué de 1, est divisible par pN, d'où il suit $\mu_1(pN)=\mu_1(N)$.

Le nombre premier impair p ne divise pas N. — Pour que $(\alpha + KN)^2 - 1$ soit divisible par pN, comme il est déjà divisible par N et que p est premier avec N, il faut et il suffit qu'il soit divisible par p; mais, au point de vue de la divisibilité par p, il revient au même, au lieu de considérer les nombres eux-mêmes tels que $\alpha + KN$, de considérer les restes de leur division par p. Or ces nombres forment une progression arithmétique de raison N et, d'après le théorème I, les restes de leur division par p sont, dans un certain ordre, les p premiers nombres; il y en a donc parmi eux deux (2e cas) qui sont tels que leur carré, diminué de 1, soit divisible par p et, par conséquent, par pN. Il suit de là $\mu_1(pN) = 2\mu_1(N)$.

Conclusion. — L'exactitude du théorème énoncé résulte de la combinaison des divers cas examinés.

Corollaire I. — Les nombres pour lesquels μ_1 est égal à 2 sont p^k, $2p^k$ *et* 4, p étant un nombre premier impair et k un nombre quelconque. Pour tous les autres nombres μ_1 est divisible au moins par 4.

Corollaire II. — Si M et N sont deux nombres premiers entre eux, on a $\mu_1(MN) = \mu_1(M)\,\mu_1(N)$.

Au contraire, si M est un nombre impair qui ne contient pas de facteurs premiers étrangers à N, on a $\mu_1(MN) = \mu_1(N)$.

Définition. — On dit que deux nombres A et B sont congrus pour le module N, lorsque leur différence A — B est divisible par N. Cette propriété des nombres A et B s'écrit sous la forme

$$A \equiv B \pmod{N},$$

qui s'énonce A *congru à* B *module* N et qui prend le nom de *congruence.*

D'après cette définition, il est évident que l'on peut appliquer aux congruences de même module les opérations suivantes de l'Algèbre : addition, soustraction, multiplication, élévation aux puissances.

THÉORÈME V. — *Le produit* P *des* $\varphi(N)$ *nombres qui ne surpassent pas* N *et sont premiers avec lui est congru pour le module* N *à la puissance d'exposant* $\frac{1}{2}\varphi(N)$ *d'un quelconque* A *de ces* $\varphi(N)$ *nombres, cette puissance étant prise positivement ou négativement suivant que* $\mu_A(N)$ *est divisible par* 4 *ou seulement par* 2.

Le produit P *et le nombre* A *satisfont donc à la congruence*

$$P \equiv (-1)^{\frac{1}{2}\mu_A(N)} A^{\frac{1}{2}\varphi(N)} \pmod{N}.$$

Pour effectuer le produit P, prenons les nombres dont il se compose en réunissant d'abord deux à deux les nombres associés par rapport à A pour le module N, puis en groupant avec leurs complémentaires à N les nombres égaux à leurs associés, nous aurons ainsi la suite de congruences de même module

$$\left.\begin{array}{l} \left.\begin{array}{l} ab \equiv A \pmod{N} \\ cd \equiv A \pmod{N} \\ \cdots\cdots\cdots\cdots \end{array}\right\} \frac{1}{2}\varphi(N) \text{ congruences} \\ \left.\begin{array}{l} \alpha(N-\alpha) \equiv -A \pmod{N} \\ \beta(N-\beta) \equiv -A \pmod{N} \\ \cdots\cdots\cdots\cdots\cdots \end{array}\right\} \frac{1}{2}\mu_A(N) \text{ congruences} \end{array}\right.$$

et, en les multipliant membre à membre, nous aurons, comme cela a été annoncé,

$$(7) \qquad P \equiv (-1)^{\frac{1}{2}\mu_A(N)} A^{\frac{1}{2}\varphi(N)} \pmod{N}.$$

Corollaire I. — En faisant $A = 1$ dans la formule (7), il vient

$$P \equiv (-1)^{\frac{1}{2}\mu_1(N)} \pmod{N}, \tag{8}$$

ce qui montre que N *divise toujours* $P + 1$ *ou* $P - 1$ (théorème de Wilson généralisé).

Pour que ce soit $P + 1$ qui soit divisible par N, il faut, puisque μ_1 est une puissance de 2 (théorème IV), que l'on ait $\mu_1 = 2$ et, en se reportant au corollaire I du même théorème, on voit que les nombres qui remplissent cette condition sont *une puissance quelconque d'un nombre premier impair, le double d'une telle puissance et le nombre* 4. Dans tous les autres cas, c'est $P - 1$ qui est divisible par N. Le nombre 2 fait exception et appartient aux deux catégories.

En particulier, si N est un nombre premier, P est égal à $(N - 1)!$ et N *divise* $(N - 1)! + 1$ (théorème de Wilson).

Corollaire II. — Par comparaison, on déduit des formules (7) et (8)

$$(-1)^{\frac{1}{2}\mu_A(N)} A^{\frac{1}{2}\varphi(N)} \equiv (-1)^{\frac{1}{2}\mu_1(N)} \pmod{N}$$

ou, en élevant au carré,

$$A^{\varphi(N)} \equiv 1 \pmod{N}, \tag{9}$$

ce qui peut s'énoncer ainsi : *Si* N *est premier avec* A, *il divise* $A^{\varphi(N)} - 1$ (théorème de Fermat, généralisé par Euler).

En particulier, *si* N *est un nombre premier qui ne divise pas* A, *il divise* $A^{N-1} - 1$ ou, si l'on veut, *tout nombre premier* N *divise* $A^N - A$, *quel que soit* A (théorème de Fermat).

Remarque. — Conformément au théorème d'Euler,

l'indicateur est tel que $A^{\varphi(N)} - 1$ est divisible par N si A et N sont premiers entre eux; mais il existe généralement, pour chaque valeur de N, des nombres plus petits que $\varphi(N)$ et qui jouissent de la même propriété.

D'après le corollaire I du théorème II, l'indicateur est égal au produit des nombres

$$\frac{N}{pqr\ldots}, (p-1), (q-1), (r-1), \ldots.$$

Or il suffit, pour que $A^m - 1$ soit divisible par N, que m soit un multiple commun de ces nombres, par exemple leur plus petit commun multiple; car alors, en mettant en évidence les puissances

$$p^h, q^h, r^l, \ldots$$

des nombres premiers qui composent N, m est divisible par les quantités

$$p^{h-1}(p-1), q^{h-1}(q-1), r^{l-1}(r-1), \ldots$$

qui en sont respectivement les indicateurs et, par suite, $A^m - 1$ est divisible par chacune de ces puissances et, par conséquent, par leur produit, qui est N.

On peut même ajouter que si N, sans être égal à 4, est divisible par 4, il suffit de prendre le plus petit commun multiple des nombres

$$\frac{N}{2pqr\ldots}, (p-1), (q-1), (r-1), \ldots$$

parce que, dans ce cas, A est impair, m toujours pair et qu'une puissance paire d'un nombre impair, diminuée de 1, contient le facteur 2 deux fois de plus au moins qu'il n'est contenu dans l'exposant de cette puissance.

En résumé, le plus petit commun multiple des

nombres

$$\frac{N}{2pqr\ldots}, (p-1), (q-1), (r-1), \ldots$$

(N divisible par 4 sans être égal à 4),

ou

$$\frac{N}{pqr\ldots}, (p-1), (q-1), (r-1), \ldots$$

(N non divisible par 4 ou égal à 4),

peut remplacer l'indicateur $\varphi(N)$ dans l'application du théorème d'Euler. On donne à ce nombre le nom d'*indicateur réduit*, et on le désigne par la notation $\psi(N)$.

Il y a une certaine catégorie de nombres pour lesquels $\psi(N)$ est égal à $\varphi(N)$: ce sont ceux qui n'ont qu'un couple de nombres égaux à leurs associés pour le module N et qui ont déjà été cités aux corollaires I des théorèmes IV et V, c'est-à-dire p^k, $2p^k$ et 4, p étant un nombre premier impair et k un nombre quelconque; il est en effet évident que le plus petit multiple commun des nombres p^{k-1} et $p-1$ ne peut être que leur produit.

Autre remarque. — Ces mêmes nombres possèdent encore une autre propriété importante, qui consiste en ce que ce sont les seuls pour lesquels il existe des *racines primitives*.

Si l'on prend les restes de la division par N ou les *résidus* des puissances successives d'un nombre a plus petit que N et premier avec lui, on obtient une suite de nombres premiers avec N; cette suite est périodique et l'amplitude de la période est au plus égale à $\psi(N)$, car, puisque $a^{\psi(N)}$ donne 1 pour résidu, il est clair que les deux puissances d'exposants k et $\psi(N)+k$ fourniront le même résidu. Cela posé, on dit que le nombre a est *racine primitive relativement au module* N lorsque les résidus de ses $\varphi(N)$ premières puissances sont tous dif-

férents et reproduisent, dans un certain ordre, le dernier étant 1 conformément au théorème d'Euler, les $\varphi(N)$ nombres inférieurs à N et premiers avec N; or, d'après ce qu'on vient de voir, cela est impossible si $\psi(N)$ est plus petit que $\varphi(N)$ et, par conséquent, *il n'y a que les nombres pour lesquels l'indicateur et l'indicateur réduit sont égaux qui puissent avoir des racines primitives.*

Tableau faisant connaître, au moins jusqu'à 1000, *les nombres correspondant aux diverses valeurs de l'indicateur réduit de* 1 *à* 100.

$\psi(N)$.	N.
1.	1.2.
2.	3.4.6.8.12.24.
4.	5.10.15.16.20.30.40.48.60.80.120.240.
6.	7.9.14.18.21.28.36.42.56.63.72.84.126.168.252. 504.
8.	32.96.160.480.
10.	11.22.33.44.66.88.132.264.
12.	13.26.35.39.45.52.65.70.78.90.91.104.105.112. 117.130.140.144.156.180.182.195.208.210.234. 260.273.280.312.315.336.360.364.390.420.455. 468.520.546.560.585.624.630.720.728.780.819. 840.910.936.....65520.
16.	17.34.51.64.68.85.102.136.170.192.204.255.272. 320.340.408.510.544 680.816.960.1020.1088. 1360.1632.2040.2720.3264.4080.5440.8160.16320.
18.	19.27.38.54.57.76.108.114.133.152.171.189.216. 228.266.342.378.399.456.513.532.684.756.798. 1026.1064.1197.1368.1512.1596.2052.2394.3192. 3591.4104.4788.7182.9576.14364.28728.
20.	25.50.55.75.100.110.150.165.176.200.220.275. 300.330.400.440.528.550.600.660.825.880.1100. 1200.1320.1650.2200.2640.3300.4400.6600.13200.
22.	23.46.69.92.138.184.276.552.
24.	224.288.416.672.1120.1248.1440.2016.2080.2912. .....131040.

$\psi(N)$.	N.
28.	29.58.87.116.145.174.232.290.348.435.464.580. 696.870.1160.1392.1740.2320.3480.6960.
30.	31.62.77.93.99.124.154.186.198.217.231.248.279. 308.341.372.396.434.462.558.616.651.682.693. 744.792.868.924.....171864.
32.	128.384.640.1920.2176.6528.10880.32640.
36.	37.74.95.111.135.148.185.190.222.247.259.270. 285.296.304.333.351.370.380.432.444.481.494. 518.540 555.570.592.665.666.702.703.740.741. 760.777.855.888.912.945.962.988.999..... 138181680.
40.	41.82.123.164.205.246.328.352.410.451.492.615. 656.800.820.902.984.....1082400
42.	43.49.86.98.129.147.172.196.258.294.301.344.387. 392.441.516.588.602.774.882.903.....151704.
44.	115.230.345.368.460.690.920.1104.1380.1840.2760. 5520.
46.	47.94.141.188.282.376.564.1128.
48.	119.153.221.238.306.357.442.448.476.576.595.612. 663.714.765.832.884.952.....455360.
52.	53.106.159.212.265.318.424.530.636.795.848.1060. 1272.1590.2120.2544.3180.4240.6360.12720.
54.	81.162.324.567.648.1134 1539.2268.3078.4536. 6156.10773.12312.21546.43092.86184.
56.	928.2784.4640.13920.
58.	59.118.177.236.354.472.708.1416.
60.	61.122.143.155.175.183.225.244.286.305.310.325. 350.366.385.403.427.429.450.465.488.495.496. 525.549.572.610.620.650.671.700.715.732.770. 775.793.806.854.858.900.915.930.975.976.990. .....681440760o.
64.	256.768.1280.3840.4352.13056.21760.65280.
66.	67.134.161.201.207.268.322.402.414.469.483.536. 603.644.804.828.938.966.....776664.
70.	71.142.213.284.426.568.781.852.1562.1704.2343. 3124.4686.6248.9372.18744.
72.	73.146.219.292.365.438.511.584.608.657.730.864. 876.949.1022.1095.1168.1184.1314.1387.1460. 1533.1752.1824.1898.1971.....2017452280.

$\psi(N)$.	N.
78.	79.158.237.316.474.553.632.711.948.1106.1422. 1659.1896.2212.2844.3318.4424.4977.5688.6636. 9954.13272.19908.39816.
80.	187.374.425.561.697.704.748.850.935.1122.1275. 1394.1496.1600.1700.1870.....36801600.
82.	83.166.249.332.498.664.996.1992.
84.	203.215.245.261.377.406.430.490.522.559.609.637. 645.688.735.754.784.812.860.980.1015.1044. 1118.1131.1218.1247.1274.1290.1305.1491.1470. 1505.1508.1624.1677.1720.1827.1885.1911.1935. 1960.....571924080.
88.	89.178.267.356.445.534.712.736.890.1068.1335. 1424.1780.....982560.
90.	209.297.418.589.594.627.836.837.1178.1188.1254. 1463.1672.1674.1767.1881.....9796248.
92.	235.470.705.752.940.1410.1880.2256.2820.3760. 5640.11280.
96.	97.194.291.388.485.582.679.776.873.896.970.1152. 1164.1261.1358.1455.1552.1649.1664.1746 1940. .....864339840.
100.	101.125.202.250.303.375.404.500.505.606.750.808. 1000.1010.1111.1212.1375.1500 1515.1616.2000. .....6666000.