A propos de l'indicatrice d'Euler

J. Dautrevaux
C.S.U. Mulhouse

Notation : On écrit $d|n$ pour exprimer que l'entier *d divise* l'entier n.

On sait que, si n est un entier naturel quelconque, on désigne par $\varphi(n)$ le nombre des entiers $p \leq n$, et premiers avec n.

Il est clair que $\varphi(1) = 1$ et que, pour tout entier *premier* p, $\varphi(p) = p-1$ pour $p \geq 2$. De même, si p est un entier premier ≥ 2 et α un exposant entier ($\alpha \geq 1$), on a : $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$; en effet, les seuls entiers plus petits que p^α, qui ne soient pas premiers avec p^α sont les multiples de p, entiers de la forme Np où $1 \leq N \leq p^{\alpha-1}$, qui sont précisément au nombre de $p^{\alpha-1}$.

L'indicatrice d'Euler jouit de propriétés fort curieuses, en relation d'une part avec la décomposition d'un entier en facteurs premiers, d'autre part avec la théorie des groupes.

1. Nombre de diviseurs d'un entier naturel.

Soit n un entier naturel, décomposé en un produit de facteurs premiers sous la forme :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

où les p_i sont des nombres premiers ≥ 2 et les α_i des exposants ≥ 1.

Tout diviseur d de n est décomposable en un produit de facteurs premiers sous la forme suivante :

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$$

où les p_i sont les mêmes que ci-dessus et les β_i des exposants tels que, pour chaque indice $i (1 \leq i \leq k)$ on ait : $0 \leq \beta_i \leq \alpha_i$.

Le nombre des diviseurs de n (y compris les diviseurs triviaux 1 et n) est donc égal à : $\delta(n) = (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1)$ si $n \geq 2$, et, bien évidemment, $\delta(1) = 1$.

De cette expression on peut aussi facilement déduire la *somme* de tous les diviseurs de n sous la forme :

$$\sum_{d|n} d = (1+p_1+p_1^2+\ldots+p_1^{\alpha_1})(1+p_2+p_2^2+\ldots+p_2^{\alpha_2})\ldots(1+p_k+p_k^2+\ldots+p_k^{\alpha_k})$$

soit :

$$\sum_{d|n} d = \frac{(p_1^{\alpha_1+1}-1)(p_2^{\alpha_2+1}-1)\ldots(p_k^{\alpha_k+1}-1)}{(p_1-1)(p_2-1)\ldots(p_k-1)}$$

2. Propriétés de l'indicatrice d'Euler.

Lemme : Soient p et q deux entiers premiers entre eux. Alors :

$$\varphi(pq) = \varphi(p).\varphi(q)$$

$\varphi(pq)$ est le nombre d'entiers $x < pq$, premiers avec pq.

Soit x un entier de cette sorte :

a) On divise x par p par exemple : on obtient un quotient z et un reste y, certainement $y \neq 0$, sinon p diviserait x et x ne serait pas premier avec pq. On a donc : $0 < y < p$ et $0 \leq z < q$ (puisque $x < pq$).

y est nécessairement premier avec p, sinon un diviseur commun à y et p diviserait x et dès lors x ne serait pas premier avec p, donc avec pq, ce qui est contraire à l'hypothèse.

On a donc $\varphi(p)$ possibilités pour le choix de y.

b) Choisissons y premier avec p ($0 < y < p$), ce qui détermine un x premier avec p par : $x = pz + y$ avec $0 \leq z < q$; z est, pour le moment, encore arbitraire. Il faut que x soit premier avec pq et pour cela nous devrons choisir z.

On divise x par q, ce qui donne un quotient t et un reste r et, pour la même raison que précédemment, on a : $r \neq 0$ et r premier avec q et, par conséquent, on aura $\varphi(q)$ choix possibles pour r (car $0 < r < q$).

Par conséquent, si x est un entier $x < pq$, premier avec pq, les restes y et r des divisions de x par p et q respectivement sont des entiers vérifiant : $0 < y < p$, y premier avec p et $0 < r < q$, r premier avec q.

Réciproquement, si on se donne arbitrairement deux entiers y et r vérifiant ces conditions, ils déterminent un entier x unique tel que $x < pq$ et x premier avec pq; en effet, supposons par exemple que $r \geq y$ (dans le cas contraire on intervertirait les rôles de p et q), et considérons tous les entiers de la forme pz, pour tous les entiers z vérifiant $0 \leq z < q$. Les divisions de l'un quelconque de ces q entiers par q fournit un reste ρ_z tel que $0 \leq \rho_z < q$, et ce reste peut prendre q valeurs possibles. Or, si $z \neq z'$, on a nécessairement $\rho_z \neq \rho_{z'}$; si, en effet, il existait un couple d'entiers (z, z') avec $z > z'$ tel que $\rho_z = \rho_{z'}$, alors q diviserait $pz - pz' = p(z - z')$; q étant premier avec p devrait diviser $z - z'$, ce qui est impossible car z et z' sont tous deux inférieurs à q, donc *a fortiori* leur différence. Par suite, les q restes sont exactement les q entiers 0, 1, 2, ..., $q-1$ pris chacun une fois et dans un ordre quelconque. Il y en a donc un et un seul qui ait la valeur $r - y$, et par suite il existe un quotient t tel que : $pz = qt + r - y$, soit : $pz + y = qt + r$, et la valeur commune à ces deux sommes est précisément l'entier x cherché : $x = pz + y = qt + r$. Comme $0 < y < p$ et $0 \leq z < q$ on a bien $x < pq$, et x est premier séparément avec p et avec q (puisque y est premier avec p et r l'est avec q), donc avec leur produit pq.

Il existe donc autant d'entiers x qu'il existe de couples (y, r) d'entiers tels que :

$0 < y < p$, y premier avec p, soit $\varphi(p)$ choix possibles,

$0 < r < q$, z premier avec q, soit $\varphi(q)$ choix possibles,

et par suite on a bien :

$$\boxed{\varphi(pq) = \varphi(p).\varphi(q)}$$

Plus généralement, si $q_1, q_2, \ldots, q_k$ sont k entiers premiers entre eux deux à deux, alors on aura :

$$\varphi(q_1 q_2 \ldots q_k) = \varphi(q_1)\varphi(q_2)\ldots\varphi(q_k)$$

Théorème 1. — Pour un entier n décomposé en un produit de facteurs premiers sous la forme :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t} \qquad \begin{cases} p_i \text{ premier}, & p_i \geq 2 \\ \alpha_i \text{ entier}, & \alpha_i \geq 1 \end{cases}$$

alors :

$$\boxed{\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right)}$$

En effet, les entiers $p_i^{\alpha_i}$, au nombre de k, sont premiers entre eux deux à deux (on suppose évidemment $k \geq 2$), et par suite :

$$\varphi(n) = \varphi(p_1^{\alpha_1}).\varphi(p_2^{\alpha_2})\dots\varphi(p_k^{\alpha_k})$$

soit, les p_i étant premiers :

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1})\dots(p_k^{\alpha_k} - p_k^{\alpha_k-1})$$

et le résultat annoncé s'en déduit immédiatement. On remarquera que $\varphi(n)$ est effectivement un entier, car $p_1, p_2, \dots, p_k$ divisent tous n.

Le résultat subsiste aussi lorsque $k = 1$, car alors : $n = p^\alpha$, et on sait que : $\varphi(n) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right)$.

Ce résultat est d'une grande importance dans la théorie analytique des nombres entiers.

3. Relation avec les diviseurs de n.

Soit d un diviseur de n. Il peut s'écrire :

$$d = p_1^{\beta_1} p_2^{\beta_2}\dots p_k^{\beta_k} \qquad \text{où} \qquad 0 \leq \beta_i \leq \alpha_i$$

Pour avoir $\varphi(d)$, on utilisera le résultat précédent, mais en prenant soin de se limiter aux seuls facteurs premiers d'exposant $\beta_i \neq 0$; il vaut mieux procéder autrement si on veut se relier à n.

Théorème 2. — Pour tout entier n, on a :

$$\boxed{\sum_{d \mid n} \varphi(d) = n}$$

En effet, on a reconnu qu'un diviseur quelconque de n (y compris les deux diviseurs triviaux 1 et n) n'était autre qu'un terme du développement du produit :

$$(1+p_1+\dots+p_1^{\alpha_1})(1+p_2+\dots+p_2^{\alpha_2})\dots(1+p_k+\dots+p_k^{\alpha_k})$$

et que réciproquement chacun des termes de ce produit fournit un diviseur de n : on obtient de cette façon la totalité des diviseurs de n et la valeur de ce produit est la somme de tous ces diviseurs.

Si $d = p_1^{\beta_1} p_2^{\beta_2}\dots p_k^{\beta_k}$ (où $0 \leq \beta_i \leq \alpha_i$) est l'un de ces diviseurs, alors :

$$\varphi(d) = \varphi(p_1^{\beta_1}).\varphi(p_2^{\beta_2})\dots\varphi(p_k^{\beta_k})$$

et ce produit est l'un des termes du développement du produit :

$$(1+\varphi(p_1)+\varphi(p_1^2)+\dots+\varphi(p_1^{\alpha_1}))(1+\varphi(p_2)+\dots+\varphi(p_2^{\alpha_2}))\dots(1+\varphi(p_k)+\dots+\varphi(p_k^{\alpha_k}))$$

et la valeur de ce produit est évidemment : $\sum_{d \mid n} \varphi(d)$.

Or, p_i étant un entier premier, on a :

$$1+\varphi(p_i)+\varphi(p_i^2)+\ldots+\varphi(p_i^{\alpha_i}) = 1+(p_i-1)+(p_i^2-p_i)+\ldots+(p_i^{\alpha_i}-p_i^{\alpha_i-1}) = p_i^{\alpha_i}$$

de sorte que :

$$\sum_{d|n} \varphi(d) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = n$$

ce qui établit la propriété annoncée.

Cette propriété est liée à la théorie des groupes et elle permet d'établir commodément certaines propriétés fines de certains groupes.

Exemple. — On désigne par Z_p l'ensemble des classes résiduelles des entiers modulo p, p étant un entier premier. On peut le munir d'une addition définie par : $\bar{x}+\bar{y} = (\overline{x+y})$, où $\bar{x}$ est l'image dans Z_p d'un élément $x \in Z (\bar{x} = \{x+kp,\ \forall k \in Z\})$, définition bien cohérente puisque si $\xi \in \bar{x}$ et $\eta \in \bar{y}$ on a : $\xi = x+kp$ et $\eta = y+k'p$ d'où $\xi+\eta$ (c'est un élément de $\bar{x}+\bar{y}$) s'écrit : $x+y+(k+k')p$, et c'est un élément de $(\overline{x+y})$ (la réciproque s'étudie aisément); et on sait que cette addition donne à Z_p une structure de *groupe abélien* qui est d'ailleurs un groupe cyclique engendré par $\bar{1}$, image de $1 \in Z$.

On peut munir également Z_p d'une multiplication définie par : $\bar{x}\bar{y} = (\overline{xy})$, et cette définition est également elle-même bien cohérente, car $\xi\eta$ (élément de $\bar{x}\bar{y}$) s'écrit : $xy+(ky+k'x+kk')p$, et est donc un élément de $(\overline{xy})$, la réciproque s'étudiant aisément.

p étant premier, tout élément non nul de Z_p admet un inverse dans Z_p : en effet, soit $\bar{x} \in Z_p (\bar{x} \neq \bar{0})$. L'ensemble des éléments de la forme $\bar{x}\bar{y}$, $\forall \bar{y} \in Z_p$ est composé de p éléments de Z_p qui sont tous distincts. Démontrons ce point : si deux produits étaient égaux $\bar{x}\bar{y} = \bar{x}\bar{y}'$, on aurait $\bar{x}\bar{y}-\bar{x}\bar{y}' = \bar{0}$. Soient $\xi \in \bar{x}$, $\eta \in \bar{y}$ et $\eta' \in \bar{y}'$ ce sont des entiers de la forme : $\xi = x+\lambda p$, $\eta = y+kp$, $\eta' = y'+k'p$ et on peut choisir les entiers λ, k, k' pour que $0 \leq \xi < p$, $0 \leq \eta < p$ et $0 \leq \eta' < p$. On a : $\xi\eta \in \bar{x}\bar{y}$, $\xi\eta' \in \bar{x}\bar{y}'$, donc $\xi\eta-\xi\eta' \in \bar{0}$ et par suite p divise $\xi(\eta-\eta')$; ceci est parfaitement impossible si $\eta \neq \eta'$, car p étant premier doit diviser au moins l'un des entiers ξ ou $|\eta-\eta'|$: or, chacun de ces deux entiers est strictement plus petit que p. Nécessairement, on a donc $\eta = \eta'$, d'où : $\bar{y} = \bar{y}'$, et les produits sont tous distincts. Comme ils ont p valeurs possibles et que le nombre des éléments de Z_p est justement égal à p, ces produits sont donc tous les éléments de Z_p rangés dans un ordre différent, et l'un de ces produits est nécessairement égal à $\bar{1}$. Comme d'autre part on vérifie facilement que $\bar{x}\bar{1} = \bar{1}\bar{x} = \bar{x}$, $\forall \bar{x} \in Z_p$, on voit que l'ensemble des éléments non nuls de Z_p, muni de la multiplication, constitue un *groupe abélien*.

Ce groupe, noté Z_p^*, est un groupe ayant $p-1$ éléments.

Théorème 1. — p étant un entier premier, on a : $\bar{x}^{p-1} = \bar{1}$, $\forall \bar{x} \in Z_p^*$ (théorème de FERMAT).

En effet, soit $\bar{x} \in Z_p^*$ un élément donné. Les $p-1$ éléments $\bar{x}\bar{y}$, $\forall \bar{y} \in Z_p^*$ sont les $p-1$ éléments de Z_p^* pris dans un ordre différent; puisque la multiplication dans Z_p^* est commutative, leur produit est égal au produit des $p-1$ éléments de Z_p^*.

Si $\bar{u} = \prod_{\bar{y} \in Z_p^*} \bar{y}$ est ce produit, on aura : $\bar{x}^{(p-1)}\,\bar{u} = \bar{u}$, soit : $\bar{x}^{(p-1)}\,\bar{u}-\bar{u} = \bar{0}$.

Soit $\xi \in \bar{x}$, choisi de telle sorte que : $0 \leq \xi < p$.

Pour chaque élément $\bar{y} \in Z_p^*$ on choisit $y \in \bar{y}$ tel que : $0 \leq y < p$; les y ainsi choisis dans tous les éléments de Z_p^* seront donc les $p-1$ entiers compris entre 1 et $p-1$

($\bar{0}$ est à exclure car $\bar{y} \neq \bar{0}$), et leur produit $(p-1)!$ est un élément de $\bar{u}$; on a donc : $\xi^{p-1}(p-1)!-(p-1)!\in\bar{0}$, ce qui montre que p divise $(\xi^{p-1}-1)(p-1)!$; ne pouvant diviser $(p-1)!$, produit dont chaque facteur est inférieur à l'entier premier p, il divise $\xi^{p-1}-1$. Il en résulte $\xi^{p-1}-1\in\bar{0}$, donc : $\xi^{p-1}\in\bar{1}$ et enfin $\bar{x}^{p-1} = \bar{1}$.

Théorème 2. — p étant un entier premier, le groupe multiplicatif Z_p^* est cyclique.

En effet, soit $\bar{x}\in Z_p^*$ un élément quelconque de Z_p^* : Z_p^* étant un groupe, les puissances successives de $\bar{x}$ seront des éléments de ce groupe. La suite $\{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^k, \ldots\}$ est composée d'éléments de Z_p^*; comme Z_p^* n'a que $p-1$ éléments, les éléments de cette suite ne sont pas tous distincts. Supposons que $\bar{x}^i$ soit le premier terme de la suite (ordonnée dans le sens des i croissants) rencontré égal à un terme $\bar{x}^j$ déjà écrit ($j<i$). Nécessairement, on a : $j = 0$ et ce terme est $\bar{x}^i = \bar{1}$; en effet, si on avait $j \neq 0$, on aurait : $\bar{x}^i = \bar{x}^j = \bar{x}^j(\bar{x}^{i-j})$, de sorte que :

$$\bar{x}^j\bar{x}^{i-j}-\bar{x}^j = \bar{0}$$

Choisissons un élément $x\in\bar{x}$ tel que $0<x<p$: alors $x^jx^{i-j}-x^j\in\bar{0}$ et donc p divise $x^j(x^{i-j}-1)$; ne pouvant diviser x^j (puisque $x<p$ ne peut avoir aucun facteur premier égal à p), il divise $x^{i-j}-1$, donc : $x^{i-j}-1\in\bar{0}$, d'où : $x^{i-j}\in\bar{1}$ et $\bar{x}^{i-j} = \bar{1}$, et ceci est en contradiction avec l'hypothèse que x^i était le premier terme rencontré égal à un terme de la suite déjà écrit, car $\bar{x}^{i-j}$ est placé dans la suite avant $\bar{x}^i$, puisque $i-j<i$.

Par suite :

a) Pour chaque élément $\bar{x}\in Z_p^*$, il existe un entier t strictement positif, tel que : $\bar{x}^t = \bar{1}$ et que : $\forall i$ et j avec $0\leq i<j<t$, alors $\bar{x}^i \neq \bar{x}^j$.

t s'appelle l'*ordre* de l'élément $\bar{x}$ dans Z_p^*.

Pour tout entier $i>0$, on effectue la division euclidienne de i par t : $i = qt+j$ avec $0<j<t$; alors : $\bar{x}^i = \bar{x}^j \neq 1$ si $j \neq 0$. Il en résulte que : $\bar{x}^i = \bar{1}$ si, et seulement si i est un multiple de t.

Comme d'après le théorème de Fermat, on a : $\bar{x}^{p-1} = \bar{1}$, $\forall\bar{x}\in Z_p^*$, alors :

b) L'ordre de chaque élément $\bar{x}\in Z_p^*$ est un diviseur de $p-1$.

Soit $\bar{x}\in Z_p^*$ un élément d'ordre t : alors l'ordre de $\bar{x}^\alpha$ (où α est un entier strictement positif) est égal à $\frac{\alpha}{\text{P.G.C.D. de } \alpha \text{ et } t}$ (on peut toujours supposer $0<\alpha<t$); en effet, si t' est l'ordre de $\bar{x}^\alpha$, on a : $\bar{x}^{\alpha t'} = 1$ et $\alpha t'$ doit être un multiple de t, le plus petit entier t' jouissant de cette propriété est précisément celui qui est indiqué. Pour avoir $t' = t$, il faut et il suffit que α soit premier avec t et, pour un élément $\bar{x}\in Z_p^*$, le nombre des éléments $\bar{x}^\alpha$ qui ont le même ordre t est égal au nombre $\varphi(t)$ des entiers $\alpha>0$ plus petits que t et premiers avec t ; $\varphi(t)$ est l'indicatrice d'Euler de l'entier t et on sait que t divise $p-1$. Ces $\varphi(t)$ éléments figurent parmi les éléments $\{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{t-1}\}$, qui, tous, vérifient l'équation $X^d = \bar{1}$, et il n'y en a pas d'autres car le polynôme $X^d-\bar{1}$ se factorise en $(X-\bar{1})(X-\bar{x})(X-\bar{x}^2)\ldots(X-\bar{x}^{t-1}) = \bar{0}$, de sorte que s'il existait un autre élément $\bar{y}$ vérifiant la même équation $X^d-\bar{1} = \bar{0}$ et ne figurant pas dans la liste précédente, on aurait :

$$(\bar{y}-\bar{1})(\bar{y}-\bar{x})(\bar{y}-\bar{x}^2)\ldots(\bar{y}-\bar{x}^{t-1}) = \bar{0}$$

Choisissant $x\in\bar{x}$ avec $0<x<p$ et $y\in\bar{y}$ avec $0<y<p$ (p ne divise ni x ni y puisque $\bar{x} \neq \bar{0}$ et $\bar{y} \neq \bar{0}$), on aurait :

$$(y-1)(y-x)(y-x^2)\ldots(y-x^{t-1})\in\bar{0}$$

donc : p divise $(y-1)(y-x)(y-x^2)\ldots(y-x^{t-1})$. Or, ceci est impossible puisqu'on a supposé $\bar{y}-\bar{1} \neq \bar{0}$, $\bar{y}-\bar{x} \neq \bar{0}$, $\bar{y}-\bar{x}^2 \neq \bar{0}$, ..., $\bar{y}-\bar{x}^{t-1} \neq 0$, p premier ne divisant aucun des facteurs du produit ne saurait diviser ce produit.

Par conséquent :

c) S'il existe un élément $\bar{x}$ d'ordre t, il existe exactement $\varphi(t)$ éléments d'ordre t dans Z_p^*.

Il est maintenant facile de terminer le raisonnement.

Pour chaque diviseur d de $p-1$, appelons $\psi(d)$ le nombre des éléments de Z^* qui ont pour ordre d. D'après ce qui précède, on a :

$$\begin{cases} \text{ou bien} : \psi(d) = 0, \\ \text{ou bien} : \psi(d) = \varphi(d). \end{cases}$$

D'autre part, chaque élément de Z_p^* (il y en a $(p-1)$) a évidemment un ordre, et cet ordre est un diviseur d de $(p-1)$. Par suite :

$$\sum_{d/p-1} \psi(d) = p-1$$

Comme par ailleurs on sait que : $\sum_{d/p-1} \varphi(d) = p-1$, on voit qu'il est impossible qu'un $\psi(d)$ soit égal à 0, car du fait que $\psi(d)$ est égal à 0 ou à $\varphi(d)$, on a nécessairement $\sum_{d/p-1} \psi(d) \leq \sum_{d/p-1} \varphi(d)$, et ce qui précède montre qu'on a nécessairement l'égalité.

Par suite :

d) Pour chaque diviseur d de $p-1$ on a : $\psi(d) = \varphi(d)$.

Ceci est vrai en particulier pour $d = p-1$ et on est assuré qu'il existe dans Z_p^* un élément $\bar{g}$ d'ordre $p-1$ (car $\varphi(p-1) \geq 1$).

On obtient alors tous les éléments de Z_p^* par :

$$Z_p^* = \{1, \bar{g}, \bar{g}^2, \bar{g}^3, \ldots, \bar{g}^{p-2}\} \qquad \text{avec} \qquad \bar{g}^{p-1} = 1$$

Ceci montre que le groupe Z_p^* est effectivement cyclique.

Remarque. — Le théorème n'est plus vrai si p n'est pas premier, même alors Z_p^* se réduit aux seuls éléments inversibles de Z_p, c'est-à-dire à ceux qui sont images d'entiers premiers avec p.

Ainsi, Z_{10}^* est un groupe cyclique de 4 éléments, mais Z_{12}^* est aussi un groupe de 4 éléments, mais non cyclique : l'ordre de chacun de ses éléments est 2. Ce groupe, ou groupe de Klein, peut par exemple être représenté par le groupe des symétries (dans le plan) par rapport à deux droites perpendiculaires Ox et Oy et par rapport à O.

Exemple. — Z_7^* est un groupe cyclique d'ordre 6 engendré par $\bar{3}$ (on voit facilement que $\bar{2}$ est d'ordre 3 seulement). (Cf. Cours A.P.M. 1, p. 111, rectifié Cours A.P.M. 2, p. 199.)

Ce théorème n'est qu'un cas particulier d'un théorème plus général, mais il était intéressant d'en donner une démonstration élémentaire dans ce cas particulièrement important.

A titre documentaire, on donne ci-dessous les natures des groupes multiplicatifs Z_p^* pour les 25 premiers entiers (premiers ou non); le nombre N_p des éléments composant le groupe Z_p^* n'est autre que $\varphi(p)$.

$p =$	2	3	4	5	6	7	8	9	10	11	12	13
$N_p =$	1	2	2	4	2	6	4	6	4	10	4	12
Z_p^*	C	C	C	C	C	C	V	C	C	C	V	C

$p =$	14	15	16	17	18	19	20	21	22	23	24	25
$N_p =$	6	8	8	16	6	18	8	12	10	22	8	20
Z_p^*	C	K	K	C	C	C	K	H	C	C	E	C

Notations. — C est le groupe cyclique.
V est le groupe de Klein (« Viergruppe » à 4 éléments).
K est le groupe abélien de type (2, 1) à 8 éléments.
E est le groupe élémentaire de 8 éléments (type (1, 1, 1)).
H est le groupe à 12 éléments de la forme 6×2.

Jacques DAUTREVAUX,