Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 3 (1931)

Artikel: Sur les sytèmes cycliques de triples de Steiner différents pour N premier (ou puissance de nombre premier) de la forme 6n + 1(suite).
Autor: Bays, S.
DOI: https://doi.org/10.5169/seals-4681

Sur les systèmes cycliques de triples de Steiner différents pour N premier (ou puissance de nombre premier) de la forme $6n+1$ (suite)

Par S. BAYS, Fribourg

Chapitre IV

Les systèmes de caractéristiques différents

34. Pour obtenir tous les systèmes cycliques de triples de Steiner pour un N donné, il faut obtenir (§ 16) tous les systèmes de n caractéristiques, dans lesquels les n caractéristiques sont sans élément commun ou, ce qui revient au même, contiennent les $3n$ éléments 1, 2, ..., $3n$; nous disons plus court (§ 31) tous *les systèmes de caractéristiques.*

Chaque système de caractéristiques est changé en lui-même par la substitution-identité $\tau^{3n} = |\underline{x},\ \underline{\alpha^{3n}x}| = |\underline{x},\ \underline{x}|$.

Si la *première* puissance de τ qui change le système de caractéristiques Σ en lui-même est $\tau^d = |\underline{x},\ \underline{\alpha^d x}|$, les puissances précédentes de τ: $\tau^0, \tau^1, \tau^2, \ldots, \tau^{d-1}$ le changent en d systèmes $\Sigma = \Sigma_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_{d-1}$ qui diffèrent l'un de l'autre (au sens ordinaire du mot) au moins par une caractéristique. En effet si deux de ces systèmes, Σ_i et Σ_k, $i < k$, étaient identiques, la puissance de τ: $\tau^i.\tau^{d-k} = \tau^{d+i-k}$, inférieure à d, changerait Σ en lui-même, ce qui n'est pas. Les puissances suivantes de τ: $\tau^d, \tau^{d+1}, \ldots$, reproduisent indéfiniment la même série $\Sigma_0, \Sigma_1, \ldots, \Sigma_{d-1}$ dans le même ordre.

Il résulte de là que d est diviseur de $3n$ et que chacun des systèmes $\Sigma_0, \Sigma_1, \ldots, \Sigma_{d-1}$ est invariant par les puissances de τ: $\tau^0, \tau^d, \tau^{2d}, \ldots, \tau^{\left(\frac{3n}{d}-1\right)d}$, et par aucune autre. Nous dirons dans ce cas que Σ (ou Σ_i, $i = 0, 1, \ldots, d-1$) *appartient au diviseur d de* $3n$.

Nous appellerons deux systèmes de caractéristiques, *équivalents* ou *différents*, selon qu'ils se déduisent ou non l'un de l'autre par une puis-

sance de la substitution τ. Nous verrons au chapitre suivant que les systèmes de caractéristiques *différents* sont les seuls qu'il nous importe de connaître. *Si Σ appartient à d, il y a donc d systèmes de caractéristiques équivalents à Σ (Σ compris); chacun possède dans le groupe $\{\tau\}$ le diviseur d'ordre maximum $\{|\underline{x}, \underline{\alpha^d x}|\}$, d'ordre $\frac{3n}{d}$.* L'un quelconque de ces d systèmes nous suffira pour la suite.

Nous ferons encore les deux remarques:

1° Si le système de caractéristiques Σ possède le diviseur $\{|\underline{x}, \underline{\alpha^d x}|\}$[41] et contient la caractéristique quelconque C, il contient la série complète des caractéristiques qui se déduisent de C par les puissances de la substitution $|\underline{x}, \underline{\alpha^d x}|$.

2° Si le système de caractéristiques Σ appartient à d ou à un diviseur de d, Σ possède le diviseur $\{|\underline{x}, \underline{\alpha^d x}|\}$, et inversement. Les deux expressions: appartenir à d ou à un diviseur de d et posséder le diviseur $\{|\underline{x}, \underline{\alpha^d x}|\}$ sont donc équivalentes. Nous entendrons toujours, dans la première, par *diviseur* de d, un diviseur $< d$.

35. Le système des caractéristiques principales appartient au diviseur $d = 1$ de $3n$ (§ 31). Il est le *seul* système qui appartient à ce diviseur $d = 1$. En effet une caractéristique qui n'est pas principale est changée en $3n$ caractéristiques différentes par les puissances successives de τ; donc si Σ appartenant au diviseur $d = 1$, contenait une caractéristique qui n'est pas principale, il en contiendrait $3n$, ce qui est impossible.

Nous désignerons désormais par le seul mot *caractéristique*, une caractéristique qui n'est pas principale et nous la noterons sans autre par $\underline{\alpha^a}\ \underline{\alpha^b}\ \underline{\alpha^c}$, en sous-entendant que a, b, c sont trois entiers positifs, d'ailleurs quelconques, mais pour lesquels on n'a pas $a \equiv b \equiv c \bmod n$.

Aucun système de caractéristiques n'appartient au diviseur $d = 2$ de $3n$, dans le cas où n est *pair*. En effet Σ, appartenant au diviseur 2, contiendrait une caractéristique $\underline{\alpha^a}\ \underline{\alpha^b}\ \underline{\alpha^c}$. Par suite il contiendrait les $\frac{3n}{2}$ caractéristiques suivantes:

---

41) Nous entendons par là que le diviseur d'ordre le plus élevé du groupe $\{\tau\}$ qui change Σ en lui-même est $\{|\underline{x}, \underline{\alpha^d x}|\}$ ou un diviseur plus étendu du groupe $\{\tau\}$ contenant ce dernier (voir la note 33 où le mot *posséder* a été fixé dans le même sens).

$\underline{\alpha^a\ \alpha^b\ \alpha^c}$, $\underline{\alpha^{a+2}\ \alpha^{b+2}\ \alpha^{c+2}}$, $\underline{\alpha^{a+4}\ \alpha^{b+4}\ \alpha^{c+4}}$, ..., $\underline{\alpha^{a+3n-2}\ \alpha^{b+3n-2}\ \alpha^{c+3n-2}}$;

ce qui est impossible, puisque $n < \frac{3n}{2}$.

36. Soit Σ appartenant au diviseur $d \geqq 3$ de $3n$, ou à un diviseur $d' \geqq 3$ de d. Il contient une caractéristique $\underline{\alpha^a\ \alpha^b\ \alpha^c}$. Il possède le diviseur $\{|\underline{x},\ \underline{\alpha^d x}|\}$. Il contient donc les $\frac{3n}{d}$ caractéristiques suivantes de la même colonne cyclique de caractéristiques:

$$\begin{array}{lll} \underline{\alpha^a} & \underline{\alpha^b} & \underline{\alpha^c}\ , \\ \underline{\alpha^{a+d}} & \underline{\alpha^{b+d}} & \underline{\alpha^{c+d}}\ , \\ \underline{\alpha^{a+2d}} & \underline{\alpha^{b+2d}} & \underline{\alpha^{c+2d}}\ , \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ \underline{\alpha^{a+3n-d}} & \underline{\alpha^{b+3n-d}} & \underline{\alpha^{c+3n-d}}\ . \end{array} \tag{31}$$

Nous appellerons cet ensemble de $\frac{3n}{d}$ caractéristiques un *rectangle* de caractéristiques. Il est invariant comme Σ par les substitutions du diviseur $\{|\underline{x},\ \underline{\alpha^d x}|\}$. Si Σ, possédant le diviseur $\{|\underline{x},\ \underline{\alpha^d x}|\}$, contient l'une quelconque des caractéristiques du rectangle, il contient le rectangle entier.

Nous avons introduit au § 31 pour représenter les caractéristiques principales qui sont les cycles de la substitution:

$$|\underline{x},\ \underline{\alpha^n x}| = (\underline{\alpha^0\ \alpha^n\ \alpha^{2n}})\ (\underline{\alpha^1\ \alpha^{n+1}\ \alpha^{2n+1}})\ \ldots\ (\underline{\alpha^{n-1}\ \alpha^{2n-1}\ \alpha^{3n-1}})$$

les nouveaux éléments $\mathbf{0, 1, \ldots, n-1}$, (mod n).

Plus généralement nous représenterons les cycles de la substitution:

$$\begin{gathered} |\underline{x},\ \underline{\alpha^d x}| = (\underline{\alpha^0\ \alpha^d\ \alpha^{2d}\ \ldots\ \alpha^{3n-d}})\ (\underline{\alpha^1\ \alpha^{d+1}\ \alpha^{2d+1}\ \ldots\ \alpha^{3n-d+1}})\ \ldots \\ \ldots\ (\underline{\alpha^{d-1}\ \alpha^{2d-1}\ \ldots\ \alpha^{3n-1}}) \end{gathered} \tag{32}$$

par les nouveaux éléments $\mathbf{0, 1, \ldots, d-1}$, (mod d).

Nous ajoutons (mod n) et (mod d); nous spécifierons ainsi dans la suite, lorsque ce sera nécessaire, par rapport à quel module ces nouveaux éléments sont pris.

L'ensemble des éléments $\underline{\alpha^a}$, $\underline{\alpha^{a+d}}$, $\underline{\alpha^{a+2d}}$, ..., $\underline{\alpha^{a+3n-d}}$, disposés verticalement dans le rectangle (31), est évidemment l'un des cycles de la substitution (32), le cycle $(\underline{\alpha^{a'}}\ \underline{\alpha^{a'+d}}\ \underline{\alpha^{a'+2d}}\ \ldots\ \underline{\alpha^{a'+3n-d}})$, si a' est le plus petit reste positif ou nul de l'entier a (mod d). Il suffit pour le voir, de remarquer que les d premières puissances de la substitution $|\underline{x}, \underline{\alpha x}|$ changent le premier cycle de la substitution (32) successivement en tous les autres et que les puissances suivantes, égale ou supérieures à d, reproduisent indéfiniment ces mêmes cycles dans le même ordre.

En conséquence, nous représenterons les $\frac{3n}{d}$ éléments $\underline{\alpha^a}$, $\underline{\alpha^{a+d}}$, ..., $\underline{\alpha^{a+3n-d}}$ par $\boldsymbol{a}$, $\boldsymbol{a}$ *étant le plus petit reste positif ou nul de l'entier* a (mod d), et le rectangle des $\frac{3n}{d}$ caractéristiques (31) par le triple $\boldsymbol{a, b, c}$ (mod d).

Pour que le rectangle (31) contienne $\frac{9n}{d}$ éléments différents, autrement dit pour que les $\frac{3n}{d}$ caractéristiques du rectangle puissent faire partie d'un système de caractéristiques, *il faut* et *il suffit* que les 3 éléments $\boldsymbol{a, b, c}$ soient différents. C'est là en effet la condition nécessaire et suffisante pour que les trois rangées verticales des éléments (31) soient trois cycles différents de la substitution (32).

37. La colonne cyclique de caractéristiques, déterminée par la caractéristique $\underline{\alpha^a}\ \underline{\alpha^b}\ \underline{\alpha^c}$, se décompose en d rectangles de la forme (31), contenant $\frac{3n}{d}$ caractéristiques chacun. Nous les écrirons horizontalement, en deux rangées, faute de place:

$$
\begin{array}{llll}
\underline{\alpha^a} & \underline{\alpha^b} & \underline{\alpha^c}, & \underline{\alpha^{a+1}} \quad \underline{\alpha^{b+1}} \quad \underline{\alpha^{c+1}}, \\
\underline{\alpha^{a+d}} & \underline{\alpha^{b+d}} & \underline{\alpha^{c+d}}, & \underline{\alpha^{a+d+1}} \quad \underline{\alpha^{b+d+1}} \quad \underline{\alpha^{c+d+1}}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
\underline{\alpha^{a+3n-d}} & \underline{\alpha^{b+3n-d}} & \underline{\alpha^{c+3n-d}}, & \underline{\alpha^{a+3n-d+1}} \quad \underline{\alpha^{b+3n-d+1}} \quad \underline{\alpha^{c+3n-d+1}}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & & \underline{\alpha^{a+d-1}} \quad \underline{\alpha^{b+d-1}} \quad \underline{\alpha^{c+d-1}}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & & \underline{\alpha^{a+2d-1}} \quad \underline{\alpha^{b+2d-1}} \quad \underline{\alpha^{c+2d-1}}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & & \underline{\alpha^{a+3n-1}} \quad \underline{\alpha^{b+3n-1}} \quad \underline{\alpha^{c+3n-1}}.
\end{array}
\qquad (33)
$$

Ces rectangles sont des systèmes imprimitifs vis-à-vis des substitutions du groupe $\{|\underline{x}, \underline{\alpha x}|\}$. Ils se représentent par les triples suivants (mod d) des éléments $0, 1, \ldots, d-1$, que nous écrirons de nouveau en colonne cyclique verticale :

$$\begin{array}{lll} a, & b, & c, \\ a+1, & b+1, & c+1, \\ a+2, & b+2, & c+2, \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ a+d-1, & b+d-1, & c+d-1. \end{array} \qquad (34)$$

Le groupe des permutations des rectangles (33) entre eux par les substitutions du groupe $\{|\underline{x}, \underline{\alpha x}|\}$, ou celui des permutations des triples (34) entre eux par les mêmes substitutions, est isomorphe au groupe cyclique $\{(0\,1\,2 \ldots \overline{d-1})\}$. Le groupe $\{|\underline{x}, \underline{\alpha x}|\}$ est $\frac{3n}{d}$ fois isomorphe à ces trois derniers groupes.

Pour simplifier, nous appellerons la colonne cyclique (34) des éléments $0, 1, \ldots, d-1$, la colonne *réduite* (mod d) de la colonne cyclique de caractéristiques (33), les triples de cette colonne (34) les triples *réduits* (mod d) et les éléments $0, 1, \ldots, d-1$, les éléments *réduits* (mod d).

Formons le tableau des colonnes réduites (mod d) des $n-1$ colonnes cycliques de $3n$ caractéristiques (§ 33). D'après ce qui a été dit, il suffit pour cela de prendre dans chacune de ces $n-1$ colonnes, les trois exposants d'une caractéristique quelconque, les réduire à leurs plus petits restes positifs ou nuls (mod d) et écrire la colonne cyclique (mod d) des éléments $0, 1, 2, \ldots, d-1$, qui en découle. Soit ce tableau :

(35)

$$\begin{array}{llllllll} a, & b, & c, & a', & b', & c', & \ldots\ldots\ldots, \\ a+1, & b+1, & c+1, & a'+1, & b'+1, & c'+1, & \ldots\ldots\ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots, & & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & & \ldots\ldots\ldots, \\ a+d-1, & b+d-1, & c+d-1, & a'+d-1, & b'+d-1, & c'+d-1, & \ldots\ldots\ldots. \end{array}$$

Si dans l'une de ces colonnes, le triple de tête ou l'un quelconque des triples de la colonne a ses trois éléments différents, tous les triples de la colonne ont leurs trois éléments différents. Si le triple de tête ou l'un des triples de la colonne a deux de ses éléments ou ses trois éléments égaux, il en est ainsi de tous les triples de la colonne.

D'après le dernier alinéa du § 36, *seules les colonnes réduites (35) qui ont leurs triples formés de trois éléments différents pourront servir à*

former des systèmes de caractéristiques appartenant à d ou à un diviseur de d. Toute combinaison de m triples pris dans ces colonnes, formés d'éléments tous différents, représentera un ensemble de $m \cdot \frac{3n}{d}$ caractéristiques sans élément commun et invariant par les substitutions du diviseur $\{\underline{x}, \underline{\alpha^d x}\}$.

38. Les diviseurs immédiats de $3n$ sont 3 et n.

Le cas du diviseur 3 ne présente aucune difficulté.

Le rectangle (31) contient dans ce cas $\frac{3n}{3} = n$ caractéristiques; il est donc à lui seul un système de caractéristiques. Chaque colonne cyclique de $3n$ caractéristiques dont la colonne réduite (mod 3) a le triple de tête **0 1 2** se décompose donc en trois systèmes de n caractéristiques équivalents, invariants par les substitutions du groupe $\{\underline{x}, \underline{\alpha^3 x}\}$.

Le nombre des systèmes de caractéristiques *différents* appartenant à $d = 3$ est donc au plus $n - 1$; aucune caractéristique principale ne peut entrer dans l'un de ces systèmes.

39. Avant de passer au cas du diviseur n, nous ferons encore les considérations suivantes.

Si Σ possède le diviseur $\{\underline{x}, \underline{\alpha^d x}\}$ et contient la caractéristique principale $\underline{\alpha^a}\ \underline{\alpha^{a+n}}\ \underline{\alpha^{a+2n}}$, il contient la série des caractéristiques principales suivantes:

$$\underline{\alpha^a}\ \underline{\alpha^{a+n}}\ \underline{\alpha^{a+2n}},\ \underline{\alpha^{a+d}}\ \underline{\alpha^{a+d+n}}\ \underline{\alpha^{a+d+2n}},\ \underline{\alpha^{a+2d}}\ \underline{\alpha^{a+2d+n}}\ \underline{\alpha^{a+2d+2n}},\ \ldots\ldots\ldots \quad (36)$$

1° *Si d est premier à n,* étant diviseur de $3n$, il ne peut être que 1 ou 3 (dans le cas où n n'est pas multiple de 3). Ces deux cas ont déjà été traités.

2° *Si d est diviseur de n,* la série (36) est formée des $\frac{n}{d}$ caractéristiques principales différentes[42]):

---

[42]) La caractéristique principale, $\underline{\alpha^a}\ \underline{\alpha^{a+n}}\ \underline{\alpha^{a+2n}}$, $a = 0, 1, 2, \ldots$, est la caractéristique principale $\underline{\alpha^{a'}}\ \underline{\alpha^{a'+n}}\ \underline{\alpha^{a'+2n}}$, où a' est le plus petit reste positif ou nul de l'entier a (mod n), représentée par l'élément $\boldsymbol{a}$ (§ 31). Les caractéristiques principales (37) sont différentes car $a + kd$ et $a + ld$, k et l étant deux des entiers $0, 1, 2, \ldots, \frac{n}{d} - 1$, $k > l$, sont incongrus entre eux (mod n), sinon on aurait $(k - l)\, d \equiv 0$ (mod n) ou $k - l \equiv 0 \left(\mathrm{mod}\ \frac{n}{d}\right)$, ce qui n'a lieu que pour $k = l$.

$$\underline{\alpha^a\ \alpha^{a+n}\ \alpha^{a+2n}},\ \underline{\alpha^{a+d}\ \alpha^{a+d+n}\ \alpha^{a+d+2n}},\ \ldots\ \ldots\ \ldots,\ \underline{\alpha^{a+n-d}\ \alpha^{a+2n-d}\ \alpha^{a+3n-d}} \quad (37)$$

Cet ensemble est invariant par les substitutions du diviseur $\{|\underline{x},\ \underline{\alpha^d x}|\}$. Si Σ possède ce diviseur et contient l'une quelconque des caractéristiques (37), il contient l'ensemble complet. Cet ensemble se représente par les $\frac{n}{d}$ éléments réduits (mod n), représentant ces caractéristiques principales (37): $\boldsymbol{a,\ a+d,\ \ldots,\ a+n-d}$.

3° *Si n est diviseur de d,* on a, d étant diviseur de $3n$, $d=3n$ ou $d=n$. Dans les deux cas la série (36) ne contient que la caractéristique principale $\underline{\alpha^a\ \alpha^{a+n}\ \alpha^{a+2n}}$.

4° *Si d et n ont un p. g. c. d. $\delta>1$, $<d$ et n;* autrement dit si $d=d'\delta$, $n=n'\delta$, $\delta>1$, d' et $n'>1$ premiers entre eux, on a, $d=d'\delta$ étant diviseur de $3n=3n'\delta$, $d'=3$ et $d=3\delta$. Dans ce cas la série (36) contient les $\frac{n}{\delta}=n'$ caractéristiques principales différentes:

$$\underline{\alpha^a\ \alpha^{a+n}\ \alpha^{a+2n}},\ \underline{\alpha^{a+d}\ \alpha^{a+d+n}\ \alpha^{a+d+2n}},$$
$$\ldots\ldots\ldots,\ \underline{\alpha^{a+(n'-1)d}\ \alpha^{a+(n'-1)d+n}\ \alpha^{a+(n'-1)d+2n}}. \quad (38)$$

En effet le premier des exposants $a,\ a+d,\ a+2d,\ \ldots$, qui est $\equiv a$ (mod n) est déterminé par la première solution de $xd=x.3\delta\equiv 0$ (mod $n'\delta$) ou $3x\equiv 0$ (mod n'), qui est $x=n'$, puisque $3=d'$ est premier à n'.

De nouveau cet ensemble (38) est invariant par les substitutions du diviseur $\{|\underline{x},\ \underline{\alpha^d x}|\}$. Si Σ, possédant ce diviseur, contient l'une quelconque des caractéristiques (38), il contient l'ensemble complet. L'ensemble se représente par les éléments réduits (mod n) $\boldsymbol{a,\ a+d,\ \ldots\ldots,\ a+(n'-1)d}$.

40. Nous prendrons maintenant le cas du diviseur n.

Dans ce cas le rectangle (31) devient le *carré* des trois caractéristiques:

$$\begin{array}{ccc} \underline{\alpha^a} & \underline{\alpha^b} & \underline{\alpha^c} \\ \underline{\alpha^{a+n}} & \underline{\alpha^{b+n}} & \underline{\alpha^{c+n}} \\ \underline{\alpha^{a+2n}} & \underline{\alpha^{b+2n}} & \underline{\alpha^{c+2n}} \end{array} \quad (39)$$

contenant les éléments des trois caractéristiques principales $\underline{\alpha^a}\ \underline{\alpha^{a+n}}\ \underline{\alpha^{a+2n}}$, $\underline{\alpha^b}\ \underline{\alpha^{b+n}}\ \underline{\alpha^{b+2n}}$, $\underline{\alpha^c}\ \underline{\alpha^{c+n}}\ \underline{\alpha^{c+2n}}$, représentées par les éléments réduits (mod n) $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$.

Pour ce cas je suis fixé sur les colonnes réduites qui ont leurs triples formés de trois éléments différents et qui peuvent donc *seules* servir à former des systèmes de caractéristiques, appartenant à n ou à un diviseur de n (§ 37). J'ai démontré dans *T.*, pages 14 à 17, que pour $N > 7$, il y a *une seule colonne* réduite (mod n) qui n'a pas dans ses triples trois éléments différents, celle de la colonne de caractéristiques dont la caractéristique de tête est $\underline{\alpha^0}\ \underline{\alpha^n}\ \underline{\alpha^n} + 1$ ou $\underline{\alpha^0}\ \underline{\alpha^{2n}}\ \underline{\alpha^{2n}} - 1$. Cette colonne réduite a évidemment deux fois l'élément **0** dans son triple de tête; le troisième élément est d'ailleurs différent. J'y ai démontré ensuite, pages 17 à 28, que pour $N > 19$, il y a une paire, fixée aussi et unique, de colonnes de caractéristiques qui ont *la même colonne* réduite (mod n). Ce dernier fait, bien qu'il m'ait coûté beaucoup plus de peine pour l'établir que le précédent, a en réalité peu d'importance pour obtenir les systèmes de caractéristiques appartenant à n ou à un diviseur de n. Il en résulte seulement que dans la constitution de ces systèmes de caractéristiques, aux triples de l'une de ces deux colonnes, on pourra indifféremment substituer les triples correspondants de l'autre [43]).

Le tableau (35) des colonnes réduites (mod $d = n$), qui peuvent servir à former des systèmes de caractéristiques possédant le diviseur $\{|\underline{x}, \underline{\alpha^n x}|\}$, ne contient donc que $n - 2$ colonnes; nous y ajoutons les éléments réduits (mod n) eux-mêmes $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n-1}$, représentant, comme les éléments de ces colonnes, les caractéristiques principales:

$$\begin{array}{llllll}
\boldsymbol{a}, & \boldsymbol{b}, & \boldsymbol{c}, & \boldsymbol{a'}, & \boldsymbol{b'}, & \boldsymbol{c'}, \quad \ldots\ldots\ldots, \\
\boldsymbol{a+1}, & \boldsymbol{b+1}, & \boldsymbol{c+1}, & \boldsymbol{a'+1}, & \boldsymbol{b'+1}, & \boldsymbol{c'+1}, \quad \ldots\ldots\ldots, \\
\ldots\ldots\ldots\ldots\ldots\ldots, & & & \ldots\ldots\ldots\ldots\ldots\ldots, & & \ldots\ldots\ldots, \\
\boldsymbol{a+n-1}, & \boldsymbol{b+n-1}, & \boldsymbol{c+n-1}, & \boldsymbol{a'+n-1}, & \boldsymbol{b'+n-1}, & \boldsymbol{c'+n-1}, \quad \ldots\ldots\ldots
\end{array} \tag{40}$$

[43]) Avant la généralisation au diviseur d quelconque de $3n$ de la ***réduction*** introduite dans *J.* et *T.* relativement au diviseur n, je ne m'étais pas rendu compte de la portée, ou plutôt de la situation exacte, dans l'ensemble du problème, des résultats que j'établissais pour ces colonnes de caractéristiques appelées dans *T.* les colonnes II, III et IV (*T.*, § 4). Ces colonnes présentent des cas particuliers relativement aux ***carrés*** de caractéristiques et aux caractéristiques principales, cycles de la substitution $|\underline{x}, \underline{\alpha^n x}|$, qui en sont les rangées verticales. Mais, pour d diviseur ***quelconque*** de $3n$, les colonnes cycliques de caractéristiques se décomposent en ***rectangles***, dont les rangées verticales sont les cycles de la substitution $|\underline{x}, \underline{\alpha^d x}|$, et dès lors, toute la réduction faite par rapport à n pouvant se faire aussi bien par rapport à d, les particularités et les résultats trouvés sur les colonnes considérées relativement à n, prenaient leur sens et leur situation exacts dans l'ensemble de la question.

En se référant à la dernière phrase du § 37 et à ce qui est dit au § 39 pour le cas $d = n$ (2° et 3°), *obtenir tous les systèmes de caractéristiques possédant le diviseur* $\{|\underline{x}, \underline{\alpha^n x}|\}$, *équivaut maintenant à trouver tous les ensembles de m triples (40) et de l éléments (41) pour lesquels* $3m + l = n$ *et qui ne contiennent pas deux fois le même élément.* Nous obtiendrons ainsi tous les systèmes de caractéristiques appartenant à n ou à un diviseur de n. Le cas $m = 0$, $l = n$ nous donnera même le système des caractéristiques principales appartenant à $d = 1$.

41. Nous appellerons *système réduit* (mod d) chaque ensemble d'éléments réduits (mod d) représentant un système de caractéristiques.

Deux systèmes réduits (mod n) du résultat précédent seront dits *équivalents* ou *différents* selon qu'ils se déduisent ou non l'un de l'autre par les substitutions du groupe cyclique $\{(0\ 1\ 2\ \ldots\ \overline{n-1})\} = \{|x, 1+x|\}$ (mod n). Le groupe $\{|\underline{x}, \underline{\alpha x}|\}$ est triplement isomorphe à ce dernier groupe (§ 31 ou 37). Si la première puissance de τ qui change le système de caractéristiques Σ en lui-même, est $|\underline{x}, \underline{\alpha^n x}|$, respectivement $|\underline{x}, \underline{\alpha^{n'} x}|$ où n' est diviseur de n, la première puissance de $|x, 1+x|$ (mod n) qui change le système réduit correspondant $\underline{\Sigma}$ en lui-même, est $|x, n+x| = |x, x|$ (mod n), respectivement $|\dot{x}, n'+x|$ (mod n), et inversement. Nous dirons dans ce cas que le système réduit $\underline{\Sigma}$ *appartient* à n, respectivement à n' diviseur de n. Il est évident aussi que les systèmes de caractéristiques seront équivalents ou différents, selon que les systèmes réduits correspondants seront équivalents ou différents.

Obtenir tous les systèmes de caractéristiques **différents** *appartenant à n, resp. à n' diviseur de n, revient maintenant à trouver dans le tableau (40)-(41) tous les systèmes réduits* **différents** *appartenant à n, resp. à n' diviseur de n.*

J'ai cherché à obtenir, sinon le nombre exact, du moins une approximation simple de ce nombre des systèmes réduits différents appartenant à n ou à n' diviseur de n, possibles dans ce tableau (40)-(41). Je n'ai pu jusqu'ici y parvenir. Dans *T.*, p. 33 à 40, j'ai donné des expressions qui deviennent rapidement compliquées et qui sont des bornes inférieure et supérieure du nombre de ces systèmes réduits différents, formés d'abord avec des triples pris dans *une seule* colonne réduite, ensuite

formés avec des triples pris dans *deux* colonnes réduites. Avec des triples pris dans *trois* colonnes réduites, les deux expressions prendraient déjà à peu près la place d'une page entière; leur complication leur enlève presque tout intérêt. Pour le cas d'une *seule* colonne réduite, ces deux bornes, inférieure et supérieure, sont:

$$(n-2)\left\{1+\frac{n-7}{2}+\frac{(n-7)\,(n-14)}{2\cdot 3}+\frac{(n-7)(n-14)(n-21)}{2\cdot 3\cdot 4}+\ldots\ldots\right\},$$

$$(n-2)\left\{1+\frac{n-1}{2}+\frac{(n-1)\,(n-2)}{2\cdot 3}+\frac{(n-1)\,(n-2)(n-3)}{2\cdot 3\cdot 4}+\ldots\ldots\right\}.$$

Dans ces expressions, par chaque quotient j'entends directement le plus grand entier inférieur ou égal à ce quotient et les quotients sont à écrire, tant que les facteurs aux numérateurs restent *positifs*.

A. Ici, nous ferons d'abord les remarques suivantes:

1° Le système des caractéristiques principales mis à part, il n'y a que les deux alternatives suivantes pour la constitution des systèmes réduits du tableau (40)-(41):

ou les systèmes ne contiennent que des triples (40), si n est de la forme $3m$,

ou les systèmes contiennent des triples (40) et des éléments (41).

2° Tant que les systèmes réduits ne contiennent qu'*un* triple par colonne (40) ou qu'*un* élément (41), ils appartiennent à n.

3° Les systèmes réduits suivants, appartenant à n, ont une construction *immédiate:*

a) un triple d'une colonne (40) et les $n-3$ éléments (41) qui complètent le système,
b) deux triples pris dans deux colonnes (40) et les $n-6$ éléments (41) qui complètent le système,
c) trois triples pris dans trois colonnes (40) et les $n-9$ éléments (41) qui complètent le système.

Et ainsi de suite. Le résultat est:

a) $n-2$ systèmes réduits *différents*, puisqu'il y a $n-2$ colonnes (40).
b) Les éléments d'un triple a, b, c d'une colonne se retrouvent *au plus* dans 9 triples d'une autre colonne. Il reste *au moins* $n-9$ triples

dans chaque autre colonne sans élément commun avec $\boldsymbol{a, b, c}$. En prenant les $n-2$ colonnes deux à deux, nous obtenons *au moins* $\frac{(n-2)(n-3)}{2}(n-9)$ systèmes réduits *différents*.

c) Les éléments de deux triples sans élément commun pris dans deux colonnes, $\boldsymbol{a, b, c}$ et $\boldsymbol{a', b', c'}$ se retrouvent *au plus* dans 18 triples d'une autre colonne. Il reste *au moins* $n-18$ triples dans chaque autre colonne sans élément commun avec $\boldsymbol{a, b, c}$ et $\boldsymbol{a', b', c'}$. En prenant les $n-2$ colonnes trois à trois, nous obtenons *au moins* $\frac{(n-2)(n-3)(n-4)}{3!}(n-9)(n-18)$ systèmes réduits *différents*.

Et ainsi de suite.

B. Ensuite, concernant les systèmes *contenant des éléments (41)* et leur appartenance à n ou à un diviseur de n, nous remarquerons ce qui suit. En vertu d'un théorème général, rappelé déjà dans la note 25) et démontré dans *T.*, p. 32, le groupe $\{|\mathbf{x}, \mathbf{1}+\mathbf{x}|\}$ (mod n) répartit les $\frac{n(n-1)(n-2)\ldots\ldots(n-i+1)}{i!}$ *i-uples* (combinaisons i à i) des n éléments $\mathbf{0, 1, 2, \ldots, n-1}$, en:

$\frac{(n-1)(n-2)\ldots\ldots(n-i+1)}{i!}$ col. cycliques de n i-uples chacune, si i n'est pas diviseur de n; (42)

$\frac{1}{n}\left\{\frac{n(n-1)(n-2)\ldots\ldots(n-i+1)}{i!} - \frac{n}{i}\right\}$ col. cycliques de n i-uples chacune,

plus *une* colonne cyclique de $\frac{n}{i}$ i-uples, si i est diviseur de n.

Il en résulte pour les systèmes réduits contenant des éléments (41):

1° Les systèmes réduits *différents* qui n'ont qu'*un* élément (41) appartiennent à n (2°, ci-dessus). Il en existe probablement, si n est assez grand de la forme $3m+1$. Il suffit d'obtenir ceux contenant l'élément **0**, par exemple.

2° Les systèmes réduits *différents* qui ont *deux* éléments (41) appartiennent à n, excepté ceux dont le couple des éléments (41) appartiendrait à la colonne cyclique de $\frac{n}{2}$ couples, dans le cas où n est *pair*.

Ces derniers, s'il en existe, appartiendront au diviseur $n' = \frac{n}{2}$ de n.

Il existe probablement de tels systèmes, du moins de la première sorte, si n est assez grand de la forme $3m + 2$. Il suffit d'obtenir ceux contenant les couples de tête des colonnes cycliques différentes de *couples* des éléments $\mathbf{0, 1, 2, \ldots, n-1}$, soit (42):

$$\frac{n-1}{2} \text{ col. cycliques de couples, si } n \text{ est impair}$$

$$\frac{1}{n}\left\{\frac{n(n-1)}{2} - \frac{n}{2}\right\} + 1 \text{ col. cycl. de couples, si } n \text{ est pair.}$$

3° Les systèmes réduits *différents* qui ont *trois* éléments (41) appartiennent à n, excepté ceux dont le triple des éléments (41) appartiendrait à la colonne cyclique de $\frac{n}{3}$ triples, dans le cas où n est *multiple de 3*.

Ces derniers, s'il en existe, appartiendront au diviseur $n' = \frac{n}{3}$ de n.

Il existe probablement de tels systèmes, du moins de la première sorte, si n est assez grand de la forme $3m$. Il suffit d'obtenir ceux contenant les triples de tête des colonnes cycliques différentes de *triples* des éléments $\mathbf{0, 1, 2, \ldots, n-1}$, soit (42):

$$\frac{(n-1)(n-2)}{6} \text{ col. cycliques de triples, si } n \text{ est premier à 3.}$$

$$\frac{1}{n}\left\{\frac{n(n-1)(n-2)}{6} - \frac{n}{3}\right\} + 1 \text{ col. cycl. de triples, si } n \text{ est multiple de 3.}$$

Et ainsi de suite.

C. Enfin, concernant les systèmes contenant *plus d'un triple au moins dans l'une des colonnes (40)* et leur appartenance à n ou à un diviseur de n, la même répartition des i-uples des éléments $\mathbf{0, 1, 2, \ldots, n-1}$ en colonnes cycliques nous donne le résultat suivant.

Représentons les triples d'une colonne (40) par *leurs premiers éléments*. Par les substitutions du groupe $\{|\, x, 1 + x \,|\}$ (mod n), les triples de cette colonne permutent entre eux comme leurs premiers éléments (§ 37), les combinaisons i à i de ces triples permutent entre elles (ou non) comme les i-uples des éléments $\mathbf{0, 1, 2, \ldots, n-1}$, qui représentent ces combinaisons permutent entre eux (ou non).

Il résulte de là, pour les triples qu'un système réduit a dans une même colonne (40), le fait analogue à celui que nous venons d'établir pour les éléments (41):

Les systèmes réduits *différents* qui ont i triples dans une colonne (40), $i = 2, 3, \ldots$, appartiennent à n, excepté ceux pour qui le i-uple des éléments $\mathbf{0, 1, 2, \ldots, n-1}$ représentant ces i triples, appartiendrait à la colonne cyclique singulière de $\frac{n}{i}$ i-uples, dans le cas où n est multiple de i. Ces derniers systèmes appartiendront au diviseur $n' = \frac{n}{i}$ de n. Il existe certainement de tels systèmes et des deux sortes si n est assez grand et i assez petit. Il suffit d'obtenir ceux contenant les ensembles de i triples d'une même colonne, représentés par les i-uples de tête des colonnes cycliques différentes de *i-uples* des éléments $\mathbf{0, 1, 2, \ldots, n-1}$, dont le nombre est donné par (42).

Des considérations établies sous les points A, B et C, il résulte essentiellement ceci: *le* ***grand nombre*** *des systèmes réduits différents du tableau (40)-(41), c'est-à-dire des systèmes de caractéristiques différents possédant le diviseur* $\{|\underline{x}, \underline{\alpha^n x}|\}$, ***appartient à n***; ceux qui appartiennent à un diviseur de n sont les *exceptions.*

42. Nous prendrons ensuite *le cas du diviseur d de n,* $< n$.

Dans ce cas les colonnes réduites (mod d) (35), qui peuvent servir à former des systèmes de caractéristiques appartenant à d ou à un diviseur de d, ne peuvent évidemment provenir que des colonnes de $3n$ caractéristiques (29), dont les colonnes réduites (mod n) sont dans le tableau (40). D'ailleurs si $\boldsymbol{a, b, c}$ sont différents (mod d), ils le sont aussi (mod n). Le rectangle (31) se décompose en $\frac{n}{d}$ carrés (39); l'élément réduit (mod d) $\boldsymbol{a}$ représente ce que représentent les $\frac{n}{d}$ éléments réduits (mod n): $\boldsymbol{a, a+d, \ldots, a+n-d,}$ soit les éléments:

$$\underline{\alpha^a}, \underline{\alpha^{a+n}}, \underline{\alpha^{a+2n}}; \underline{\alpha^{a+d}}, \underline{\alpha^{a+d+n}}, \underline{\alpha^{a+d+2n}}; \ldots\ldots, \underline{\alpha^{a+n-d}}, \underline{\alpha^{a+2n-d}}, \underline{\alpha^{a+3n-d}}.$$

Ce sont là aussi les $\frac{n}{d}$ caractéristiques principales de la série (37), qui se représente donc également par le seul élément réduit (mod d) $\boldsymbol{a}$.

Par conséquent il suffit de *réduire (mod d)* le tableau complet (40)-(41) et de conserver du résultat de (40) les seules colonnes dont les triples ont trois éléments différents. *Obtenir tous les systèmes de caractéristiques possédant le diviseur* $\{\{x, \underline{\alpha^d x}\}\}$, *équivaudra à trouver dans les nouvelles colonnes réduites et les éléments* $\mathbf{0, 1, \ldots, d-1}$, *tous les ensembles de m triples et de l éléments pour lesquels* $3m\frac{n}{d} + l\frac{n}{d} = n$ ou $3m + l = d$, *et qui ne contiennent pas deux fois le même élément.* Nous obtiendrons ainsi tous les systèmes de caractéristiques appartenant à d ou à un diviseur de d. Le cas $m = 0$, $l = d$ nous donnera encore une fois le système des caractéristiques principales.

Tout le contenu du § 41 est maintenant valable sans changement pour ce nouveau tableau (40)-(41) réduit (mod d); il suffit d'y remplacer le groupe $\{\{\mathbf{x, 1 + x}\}\}$ (mod n) par le groupe $\{\{\mathbf{x, 1 + x}\}\}$ (mod d), les éléments $\mathbf{0, 1, \ldots, n-1}$ par les éléments $\mathbf{0, 1, \ldots, d-1}$, n et n' diviseur de n, par d et d' diviseur de d. En particulier, le *grand nombre* des systèmes de caractéristiques *différents*, qui possèdent le diviseur $\{\{x, \underline{\alpha^d x}\}\}$, *appartient à d;* ceux qui appartiennent à un diviseur de d sont les *exceptions.*

Il est à peine nécessaire de faire ici l'observation suivante. Bien que le premier tableau (40)-(41) réduit (mod n) nous donne déjà théoriquement tous les systèmes de caractéristiques différents appartenant à d diviseur de n, les considérations de ce § 42 ont cependant tout leur intérêt. Le tableau (40)-(41) réduit (mod d), du moins pour les petites valeurs de N et du diviseur d, sera considérablement réduit (au sens propre du mot) par rapport au tableau (mod n). Il fournira bien plus aisément les systèmes de caractéristiques différents appartenant à d ou à un diviseur de d, sans compter les autres résultats pour N et d plus grands, par exemple les systèmes de caractéristiques différents appartenant à d que l'on peut construire *immédiatement* par le procédé sous A, 3°, § 41.

43. *Cas du diviseur 3n lui-même.*

Malheureusement, comme nous venons de le voir encore dans le cas de d diviseur de n, ce problème de l'obtention des systèmes de caractéristiques différents, abordé par la méthode exposée dans cette étude, est tel que l'échelon supérieur comporte réunies avec ses propres solu-

tions celles de l'échelon inférieur. Le cas du diviseur $d = 3n$ ne sera donc guère simplifié du fait que l'on aura obtenu tous les systèmes de caractéristiques appartenant aux diviseurs $d < 3n$. Il présente le maximum de difficultés et nous ne l'aborderons pas ici sous sa forme générale.

Nous ne ferons que l'énoncer. Il y a $n-1$ colonnes cycliques de $3n$ caractéristiques et une colonne cyclique singulière des n caractéristiques principales. Les exposants de α dans ces colonnes forment autant de colonnes cycliques de *triples* des éléments $0, 1, 2, \ldots, 3n-1$. Il s'agit de trouver dans le tableau de ces colonnes cycliques (mod $3n$):

$$\begin{array}{llllllll}
a, & b, & c, & a', & b', & c', & \ldots\ldots, \\
a+1, & b+1, & c+1, & a'+1, & b'+1, & c'+1, & \ldots\ldots, \\
a+2, & b+2, & c+2, & a'+2, & b'+2, & c'+2, & \ldots\ldots, \\
\ldots\ldots\ldots\ldots\ldots\ldots, & & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & & \ldots\ldots, \\
a+3n-1, & b+3n-1, & c+3n-1, & a'+3n-1, & b'+3n-1, & c'+3n-1, & \ldots\ldots,
\end{array} \tag{43}$$

$$\begin{array}{lll}
0, & n, & 2n, \\
1, & n+1, & 2n+1, \\
\ldots\ldots\ldots\ldots\ldots\ldots, & & \\
n-1, & 2n-1, & 3n-1,
\end{array}$$

tous les ensembles de n triples qui ne contiennent pas deux fois le même élément, ou qui contiennent donc les $3n$ éléments $0, 1, 2, \ldots, 3n-1$. Ils donneront tous les systèmes de caractéristiques appartenant à $3n$ ou à un diviseur de $3n$, autrement dit *tous les systèmes de caractéristiques.*

Nous ajouterons seulement les remarques immédiates.

1° Les $\frac{3n(3n-1)(3n-2)}{6}$ triples des $3n$ éléments $0, 1, 2, \ldots, 3n-1$ forment d'après (42), 3 étant diviseur de $3n$, $\frac{1}{3n}\left\{\frac{3n(3n-1)(3n-2)}{6} - \frac{3n}{3}\right\} = \frac{3n(n-1)}{2}$ col. cycliques de $3n$ triples et une col. cyclique de $\frac{3n}{3} = n$ triples qui est la suivante: $0+x, n+x, 2n+x$, $(x = 0, 1, \ldots, 3n-1)$ (théorème de la note 25). Les $n-1$ col. cycliques à $3n$ triples ci-dessus ne sont qu'une partie des $\frac{3n(n-1)}{2}$ col. cycliques de triples des $3n$ éléments; mais il est intéressant de constater que la colonne cyclique

de triples singulière 0, n, $2n$, se trouve aussi dans ce tableau des colonnes qui donnent les systèmes de caractéristiques.

2° Le problème posé par ce tableau (43) n'est pas le même que celui du tableau (40)-(41) réduit (mod n) ou (mod d). Dans ces deux derniers cas, on disposait de *triples* et d'éléments *isolés* pour constituer un système des n ou des d éléments du tableau; ici on ne dispose que de *triples*. Le problème serait analogue à celui posé par les *seules* colonnes (40) dans le cas de n ou d multiples de 3 (ici $3n$ est multiple de 3), s'il n'y avait la colonne singulière 0, n, $2n$, dont les triples joueront évidemment pour la constitution des systèmes un rôle particulier.

3° Il y a n colonnes dans le tableau (43). Si un système de caractéristiques doit avoir une caractéristique dans chaque colonne, il en aura exactement *une* par colonne. Il existe probablement de tels systèmes pour N assez grand; ils appartiendront à $d = 3n$.

4° Tant que le système de caractéristiques Σ n'a qu'*une* caractéristique au plus par colonne de $3n$ caractéristiques, il appartient à $d = 3n$. Admettons qu'il en ait plus d'une et que la colonne (43) a, b, c corresponde à une colonne de $3n$ caractéristiques dans laquelle Σ a i caractéristiques. Représentons les triples de a, b, c correspondants à ces caractéristiques par leurs premiers éléments $a_1, a_2, \ldots, a_i$. Σ appartiendra encore à $d = 3n$, à moins que le i-uple $a_1, a_2, \ldots, a_i$ appartienne à la colonne cyclique *singulière* de $\frac{3n}{i}$ i-uples, dans le cas où $3n$ est multiple de i. C'est dire de nouveau que le *grand nombre* des systèmes de caractéristiques différents pour N, *appartient à* $d = 3n$; ceux qui appartiennent à $d < 3n$ sont le petit nombre.

44. *Enfin,* en reprenant les quatre cas du § 39, il reste encore seul *le quatrième cas,* qui n'a pas encore été touché, *celui où d et n ont un p. g. c. d.* $\delta > 1$, *autre que d ou n.* Alors $d = 3\delta$, $n = n'\delta$ où 3 et n' sont premiers entre eux. Le rectangle (31) contient $\frac{3n}{d} = \frac{n}{\delta} = n'$ caractéristiques; si le système de caractéristiques Σ contient la caractéristique principale $\underline{\alpha^a}$ $\underline{\alpha^{a+n}}$ $\underline{\alpha^{a+2n}}$, il contient les n' caractéristiques principales (38).

Dans les deux cas $d = n$ et d diviseur de n, $< n$, les caractéristiques des colonnes et les caractéristiques principales entrant dans la constitution d'un système Σ, y entrent par ensembles *inégaux* de $\frac{3n}{d}$ et $\frac{n}{d}$ caractéristiques (§ 36 et 39); par suite, dans ces deux cas, *n doit être* de la forme $3m$ pour que Σ puisse être constitué uniquement de caractéristiques des colonnes. Dans ce cas-ci $d = 3\delta$, et le cas précédent $d = 3n$, au contraire, les caractéristiques des colonnes et les caractéristiques principales entrant dans la constitution de Σ, y entrent par ensembles *égaux* de n' caractéristiques (1 caractér. pour $d = 3n$); par suite Σ peut être constitué uniquement de caractéristiques des colonnes, *quel que soit n.*

I. *Une première partie des systèmes de caractéristiques, possédant le diviseur* $||\underline{x}, \underline{\alpha^d x}||$, *s'obtient donc en construisant dans le tableau (35) des colonnes réduites (mod d), dont les triples ont trois éléments différents, tous les ensembles de* δ *triples contenant les* $d = 3\delta$ *éléments* **0, 1, ..., d—1.**

Mais nous pouvons avoir aussi un système Σ constitué de rectangles (31) et d'ensembles (38). Pour cela il *faut* et il *suffit* que les m rectangles (31), entrant dans la constitution de Σ, contiennent exactement les éléments des $n - (\delta - m)\, n' = m\, n'$ caractéristiques principales *manquantes* dans les $(\delta - m)$ ensembles (38) qui complètent la constitution de Σ.

On a $n = n'\delta$, $3n = n'd$ et $3n - d = (n' - 1)\, d$. Les éléments de la première rangée verticale du rectangle (31) sont aussi les premiers éléments des caractéristiques principales (38). Les n' entiers:

$$a,\ a + d,\ a + 2d,\ \ldots\ldots,\ a + (n' - 1)\, d \qquad (44)$$

sont incongrus entre eux (mod n), puisque les caractéristiques principales (38) sont différentes. Soit a' le plus petit reste positif ou nul de l'entier a (mod δ); a' est un des entiers 0, 1, 2, ..., $\delta - 1$. Les entiers (44) sont $\equiv a'$ (mod δ). Leurs plus petits restes positifs ou nul (mod n) sont donc:

$$a',\ a' + \delta,\ a' + 2\delta,\ \ldots\ldots,\ a' + n - \delta = a' + (n' - 1)\, \delta. \qquad (45)$$

Conformément à la notation adoptée jusqu'ici (§ 36), a' est *l'élément réduit (mod* δ*)* a; il représente l'ensemble des éléments:

$$\underline{\alpha^{a'}},\ \underline{\alpha^{a'+\delta}},\ \underline{\alpha^{a'+2\delta}},\ \ldots\ldots,\ \underline{\alpha^{a'+n-\delta}},\ \underline{\alpha^{a'+n}},\ \underline{\alpha^{a'+n+\delta}},\ \ldots\ldots$$

$$\ldots\ldots,\ \underline{\alpha^{a'+2n-\delta}},\ \underline{\alpha^{a'+2n}},\ \underline{\alpha^{a'+2n+\delta}},\ \ldots\ldots,\ \underline{\alpha^{a'+3n-\delta}}. \quad (46)$$

Ce sont là, d'après ce qui est dit ci-dessus des entiers (44), les éléments des caractéristiques principales (38). Nous pouvons donc représenter l'ensemble des caractéristiques principales (38) par le *seul élément réduit* (*mod* δ) $\boldsymbol{a}$, comme au § 42 nous avons pu représenter l'ensemble correspondant (37) par le *seul élément réduit* (*mod d*) $\boldsymbol{a}$. Les δ éléments réduits (mod δ) $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{\delta}-\mathbf{1}$ représenteront bien ainsi les $\delta . 3n' = 3n$ éléments $\underline{\alpha^0}$ à $\underline{\alpha^{3n-1}}$ et les $\delta n' = n$ caractéristiques principales.

Les n' éléments de la première rangée verticale du rectangle (31), représentés par l'élément réduit (mod d) $\boldsymbol{a}$, sont une partie, le tiers, des $3n'$ éléments représentés par l'élément réduit (mod δ) $\boldsymbol{a}$. Pour que les $2n'$ éléments des deux autres rangées verticales du rectangle, représentées par les éléments réduits (mod d) $\boldsymbol{b}$ et $\boldsymbol{c}$, soient les deux autres tiers des éléments (46), il *faut* et il *suffit* que, $\boldsymbol{b}$ et $\boldsymbol{c}$ étant différents et différents de $\boldsymbol{a}$, réduits (mod δ), ils donnent tous deux $\boldsymbol{a}$ (mod δ). La condition est nécessaire d'après ce qui est établi à l'alinéa précédent; elle est suffisante, puisqu'alors les $3n'$ éléments différents du rectangle appartiennent aux éléments (46). D'ailleurs si les trois éléments $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, différents (mod d), donnent le même élément réduit (mod δ) $\boldsymbol{a}$, ils ne peuvent être évidemment que les trois éléments $\boldsymbol{a}$, $\boldsymbol{a}+\boldsymbol{\delta}$, $\boldsymbol{a}+2\boldsymbol{\delta}$ (mod d).

II. *La seconde partie des systèmes de caractéristiques, possédant le diviseur* $\{|\underline{x}, \underline{\alpha^d x}|\}$, *s'obtient donc en ajoutant au tableau* (35) *des colonnes réduites (mod d) dont les triples ont trois éléments différents, les éléments réduits (mod* δ*):*

$$\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{\delta}-\mathbf{1}, \quad (47)$$

et en construisant tous les ensembles de m triples (35) *et de l éléments* (47) *remplissant les conditions suivantes:*

1° $m . 3n' + l . 3n' = 3n$, ou puisque $n = n'\delta$, $m + l = \delta$;

2° l'ensemble ne contient pas deux fois le même élément;

3° aucun élément des triples n'est congru à un des l éléments (47) (mod δ); dans ce cas en effet les éléments des triples ne peuvent être que trois à trois congrus au même élément (mod δ).

Dans les deux cas I et II, nous ne retenons de nouveau que les systèmes de caractéristiques *différents*, c'est-à-dire dans le cas I, ceux qui ne se déduisent pas l'un de l'autre par une substitution du groupe $|(0\ 1\ 2\ \ldots\ \overline{d-1})|$, dans le cas II, ceux dont les parties constituées des triples (35) ne se déduisent pas l'une de l'autre par une substitution du même groupe; il est clair qu'alors les parties restantes, constituées d'éléments isolés (47), ne se déduiront pas l'une de l'autre par une substitution du groupe $|(0\ 1\ 2\ \ldots\ \overline{\delta-1})|$ et inversement.

Le cas I est contenu dans le cas II; c'est celui où $l=0$. De nouveau, en suite de ce qui vient d'être dit et du théorème de la note 25), (42), les systèmes différents appartenant *à un diviseur de d* seront le petit nombre.

Chapitre V

Les systèmes cycliques de triples différents

45. Chacune des n caractéristiques d'un système de caractéristiques Σ détermine une paire de colonnes cycliques de triples conjuguées (§ 15, avant-dernier alinéa). Par le fait Σ lui-même, avec ce choix libre entre deux colonnes par caractéristique, représente (§ 14, II) 2^n systèmes cycliques de triples de Steiner. Nous les appellerons *les systèmes de triples déterminés* par Σ, ou plus court, les *systèmes de triples* de Σ. 2^{n-1} de ces systèmes sont éventuellement *différents* (§ 14, II). Nous représenterons par S l'un quelconque d'entre eux. Inversement Σ sera dit *le système des caractéristiques de* S.

Lorsque la substitution $u=|x,\ \beta x|$ change une colonne cyclique de triples en une colonne cyclique de triples, la substitution $\sigma=|\underline{x},\ \underline{\beta x}|$ change la caractéristique de la première colonne dans la caractéristique de la seconde (§ 26). Inversement lorsque σ change une caractéristique en une caractéristique, u change la paire de colonnes conjuguées déterminée par la première caractéristique en la paire déterminée par la seconde; en effet u change une colonne cyclique de triples en une colonne cyclique de triples et la caractéristique *détermine* sa paire de colonnes conjuguées.

Théorème 8. Donc, lorsque $t=|x,\ \alpha x|$ change le système de triples S en un système S_1, $\tau=|\underline{x},\ \underline{\alpha x}|$ change le système de caractéristiques

Σ dans le système Σ_1 des caractéristiques de S_1. Inversement, lorsque τ change le système de caractéristiques Σ en un système Σ_1, t change le système de triples S en un système S_1 déterminé par Σ_1; en particulier la paire de systèmes conjugués S et S', dans la paire de systèmes conjugués S_1 et S_1'.

Il résulte de là, des définitions données aux § 2 et 34, du fait que le groupe métacyclique est engendré par les deux substitutions $s = |x, 1 + x|$ et $t = |x, \alpha x|$ et que seule la seconde de ces substitutions agit sur un système cyclique de triples, enfin du théorème 6 (§ 22), que, pour $N = 6n + 1$ *premier, les systèmes de triples sont équivalents ou différents, selon que les systèmes de caractéristiques, qui les déterminent, sont équivalents ou différents.*

Les systèmes de caractéristiques *différents* nous suffisent donc pour obtenir tous les systèmes de triples *différents*. Il reste à déterminer pour *chacun* de ces systèmes de caractéristiques différents, *combien* des 2^n systèmes de triples qu'il détermine, sont encore éventuellement *différents*. Nous savons déjà que ce nombre est au plus 2^{n-1}.

46. Le théorème 8 a une autre conséquence, qui nous permettra de répondre partiellement à la question qui vient d'être posée.

Si ω est la première puissance positive de t qui change S en lui-même, la série des systèmes déduits de S par les puissances de t est la suivante (§ 23, (16)), S_i' désignant le conjugué de S_i:

$$S = S_0, S_1, S_2, \ldots, S_{\frac{\omega}{2}-1}, S_0', S_1', S_2', \ldots, S'_{\frac{\omega}{2}-1}, S_0, S_1, \ldots . \quad (48)$$

Si d est la première puissance positive de τ qui change Σ, le système des caractéristiques de S, en lui-même, (autrement dit, si Σ appartient au diviseur d de $3n$), la série des systèmes déduits de Σ par les puissances de τ est (§ 34):

$$\Sigma = \Sigma_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_{d-1}, \Sigma_0, \Sigma_1, \ldots . \quad (49)$$

D'après le théorème 8, chaque système (49) est le système des caractéristiques du système de triples (48) du même rang. Il en résulte, puisque $\Sigma_d = \Sigma_0$ est le système des caractéristiques de $S_{\frac{\omega}{2}} = S_0'$, que d est diviseur de $\frac{\omega}{2}$ ou $\omega = 2\mu d$, μ entier positif. μ et d étant fixés, ω est

donc fixé; *il y a alors dans la série (48) 2μ systèmes de triples dont le système des caractéristiques est Σ. Ces 2μ systèmes sont équivalents; chacun d'eux possède le diviseur métacyclique* $\{|x, 1+x|, |x, \alpha^{\omega}x|\}$ (§ 23, 3°)[44]; *en vertu du théorème 6 les autres systèmes de triples déterminés par Σ en seront différents.*

ω est diviseur de $6n$ (§ 23, théorème 7) et $\frac{6n}{\omega}$ est un entier impair (§ 23, 2°). Donc $\frac{6n}{2\mu d} = \frac{3n}{\mu d}$ est un entier *impair* et μ, diviseur de $\frac{3n}{d}$, doit contenir tous les facteurs 2 contenus dans $\frac{3n}{d}$. Soit $\frac{3n}{d} = 2^a . n_1$, n_1 entier impair $\geqq 1$, a entier $\geqq 0$. Soit $\mu_1' = 1, \mu_2', \mu_3', \ldots, \mu_{k-1}', \mu_k' = n_1$, les diviseurs de n_1. Les valeurs de μ sont $\mu_i = 2^a \mu_i', i = 1, 2, \ldots, k$. Soit x_i le nombre des systèmes de triples *différents* déterminés par Σ, pour lesquels $\omega_i = 2\mu_i d = 2^{a+1} \mu_i' d$. Nous avons l'équation indéterminée suivante, qui nous renseigne partiellement, complètement dans quelques cas, sur le nombre des systèmes de triples *différents* déterminés par le système de caractéristiques Σ appartenant au diviseur d de $3n$:

$$2^n = 2^{a+1} \mu_1' x_1 + 2^{a+1} \mu_2' x_2 + \ldots + 2^{a+1} \mu_k' x_k$$

$$\text{ou} \qquad 2^{n-a-1} = \mu_1' x_1 + \mu_2' x_2 + \ldots + \mu_k' x_k . \tag{50}$$

47. 1°. *Pour $d = 3n$:*

$$a = 0, \; n_1 = 1 ; \; \mu_k' = \mu_1' = 1 ; \; \omega_k = \omega_1 = 2d = 6n.$$

L'équation se réduit à: $x_1 = 2^{n-1}$.

Les systèmes de caractéristiques appartenant à $d = 3n$ donnent chacun 2^{n-1} systèmes de triples différents. Chacun de ces systèmes de triples possède uniquement le groupe cyclique $\{|x, 1+x|\}$ (note 44).

---

[44]) ω est ***la plus petite*** puissance positive de t qui change ces systèmes de triples en eux-mêmes. Le groupe donné est donc aussi le diviseur métacyclique d'ordre ***le plus élevé*** que possèdent ces systèmes. Par contre le groupe qui ***appartient*** (§ 3) à chacun de ces 2μ systèmes équivalents peut être plus étendu et contenir des substitutions qui ne sont pas métacycliques. Cependant le cas où un système ***cyclique*** de triples possède un groupe de substitutions sortant du groupe métacyclique doit être ***l'exception.*** Nous reviendrons sur ce point. En tout cas il semble que la proposition suivante ait lieu:

Un système ***cyclique*** de triples qui ne possède dans le groupe métacyclique que le diviseur cyclique $\{|x, 1+x|\}$, ***n'est invariant par aucune autre substitution;*** autrement dit, $\{|x, 1+x|\}$ est alors le groupe qui ***appartient*** au système.

2° *Pour* $d = \frac{3n}{2}$ (dans le cas où n est *pair*):

$$a = 1,\ n_1 = 1\ ;\ \mu'_k = \mu_1' = 1\ ;\ \omega_k = \omega_1 = 4d = 6n.$$

L'équation se réduit à: $x_1 = 2^{n-2}$.

Les systèmes de caractéristiques appartenant à $d = \frac{3n}{2}$ *(n pair) donnent chacun* 2^{n-2} *systèmes de triples différents. Chacun de ces systèmes possède encore uniquement le groupe cyclique* $\{\{x,\ 1+x\}\}$ (note 44).

3° *Pour* $d = n$: $\quad a = 0,\ n_1 = 3\ ;\ \mu_1' = 1,\ \mu'_k = \mu_2' = 3\ ;$
$\omega_1 = 2d = 2n,\ \omega_k = \omega_2 = 6d = 6n.$

L'équation devient: $x_1 + 3x_2 = 2^{n-1}$. (51)

Le nombre $x_1 + x_2$ est *pair*; il a sa plus grande valeur pour $x_2 = 0$ et sa plus petite valeur pour x_1 minimum. On a $2^{n-1} \equiv \pm 1 \pmod 3$, selon que $n - 1$ est pair ou impair. Donc si $n - 1$ est pair, l'égalité $1 + 3x_2 = 2^{n-1}$ est possible; si $n - 1$ est impair, c'est la suivante, $2 + 3x_2 = 2^{n-1}$, qui est possible. Le nombre $x_1 + x_2$ est donc *au plus* 2^{n-1} et *au moins:*

$$\begin{aligned} &\frac{2^{n-1}-1}{3} + 1, \text{ si } n-1 \text{ est pair, } n \text{ impair;} \\ &\frac{2^{n-1}-2}{3} + 2, \text{ si } n-1 \text{ est impair, } n \text{ pair.} \end{aligned} \qquad (52)$$

$x_1 + 3x_2 = (x_1 + 3) + 3(x_2 - 1)$; les nombres $x_1 + x_2$ intermédiaires sont donc en progression arithmétique de raison 2. Pour les premières valeurs de N étudiées jusqu'ici, pour lesquelles il existe des systèmes de caractéristiques appartenant à $d = n$, soit $N = 19,\ 31,\ 37,\ 43$, les solutions trouvées de l'équation (51) sont celles du cas du *minimum* (52), du cas de *l'égalité* $x_1 = x_2 = 2^{n-3}$ et déjà pour $N = 43$, pour 10 de ces systèmes de caractéristiques appartenant à $d = 7$, une solution *autre* que les deux précédentes, la solution $4 + 3.20 = 64$. Pour $N = 19$ l'équation est $x_1 + 3x_2 = 4$ et n'a que la solution $x_1 = 1,\ x_2 = 1$, qui est à la fois celle du minimum et celle de l'égalité. Nous donnerons ces résultats au chapitre suivant.

Les systèmes de caractéristiques appartenant à $d = n$ donnent chacun un nombre pair de systèmes de triples différents, au plus 2^{n-1}, au moins le nombre (52). Ces systèmes de triples possèdent uniquement le groupe cyclique $\{|x, 1+x|\}$ ou bien le diviseur métacyclique $\{|x, 1+x|, |x, \alpha^{2n}x|\}$; il en existe au moins un qui possède ce dernier diviseur.

48. *Dans le cas $d = 1$ et dans ce seul cas, le nombre des indéterminées de l'équation (50) peut être réduit.*

La première puissance positive de τ qui change *une caractéristique* (non principale) en elle-même est $\tau^{3n} = |\underline{x}, \underline{\alpha^{3n}x}| = |\underline{x}, \underline{x}|$. La substitution correspondante $t^{3n} = |x, \alpha^{3n}x| = |x, -x|$ est la première puissance positive de t qui change *sûrement* une colonne cyclique de triples dans sa conjuguée et un système de triples dans son conjugué. Ce fait a pour conséquence que: ω est diviseur de $6n$ (§ 23), $\frac{6n}{\omega}$ est un entier impair (§ 23), d est diviseur de $3n$ (§ 34), ω et d ayant le sens qui leur a été fixé. La comparaison des séries (48) et (49) exige que d soit diviseur de $\frac{\omega}{2}$ et de là et des faits précédents est résultée l'équation (50).

Or la première puissance positive de τ qui change une caractéristique *principale* en elle-même est $\tau^n = |\underline{x}, \underline{\alpha^n x}|$ (§ 31, dernier alinéa) et *n est diviseur de $3n$*. La substitution correspondante $t^n = |x, \alpha^n x|$ est donc la première puissance positive de t qui change *sûrement* un système de triples S, déterminé par le système des caractéristiques principales, en son conjugué S'[45]). Ce fait a évidemment pour conséquence que pour S, ω est diviseur de $2n$ et $\frac{2n}{\omega}$ est un entier impair; d est d'ailleurs déjà diviseur de n et de $\frac{\omega}{2}$ puisqu'il est 1.

$\omega = 2\mu$; $\frac{2n}{2\mu} = \frac{n}{\mu}$ est un entier impair. Soit $n = 2^a . n_1'$, n_1' entier impair $\geqq 1$, a entier $\geqq 0$[46]). Soit ici $\mu_1' = 1$, μ_2', μ_3', ..., $\mu_{k'-1}'$, $\mu_{k'}' = n_1'$, les diviseurs de n_1'. Les valeurs de μ sont $\mu_i = 2^a \mu_i'$, $i = 1, 2, \ldots, k'$. Soit x_i le nombre des systèmes de triples *différents* déterminés par le

[45]) $|x, \alpha^n x|$ ne peut changer S en lui-même, puisque n est diviseur de $3n$ et $|x, \alpha^{3n}x|$ change S dans le conjugué S'.

[46]) Au § 46 nous avons posé $\frac{3n}{d} = 2^a . n_1$; pour $d = 1$ l'égalité devient $3n = 2^a . n_1$. C'est la raison pour laquelle nous posons ici: $n = 2^a . n_1'$ où $3n_1' = n_1$.

système des caractéristiques principales, pour lesquels $\omega_i = 2\,\mu_i = 2^{a+1}\,\mu_i'$. L'équation (50) vient remplacée par la suivante :

$$2^{n-a-1} = \mu_1'\,x_1 + \mu_2'\,x_2 + \ldots + \mu'_{k'}\,x_{k'} \qquad (53)$$

où le nombre des termes k' est le nombre des diviseurs de n_1', alors que si nous avions pris simplement $d = 1$ dans l'équation (50), le nombre des termes k aurait été le nombre des diviseurs de $n_1 = 3\,n_1'$.

49. Des considérations précédentes, des équations (50) et (53) et des valeurs correspondantes de ω, nous pouvons encore rendre explicites les résultats suivants. Il suffit de remarquer, d'une part, que le nombre $x_1 + x_2 + \ldots + x_\varkappa$, $\varkappa = k$ ou k', a sa plus grande valeur pour $x_2 = x_3 = \ldots = x_\varkappa = 0$, $x_1 = 2^{n-a-1}$ et n'est pas inférieur à $\frac{2^{n-a-1}}{\mu_\varkappa'} = x_\varkappa$, pour $x_1 = x_2 = \ldots = x_{\varkappa-1} = 0$; d'autre part, que $\omega_i = 2^{a+1}\,\mu_i' d$ est minimum pour le diviseur $\mu_1' = 1$ et maximum pour le diviseur $\mu_\varkappa' = n_1$ resp. n_1' et que le diviseur métacyclique $\{s,\ t^\omega\}$ d'ordre $N\frac{6n}{\omega}$ est d'autant plus étendu que ω est plus petit.

I. Le *nombre* des systèmes de triples *différents* déterminés par un système de caractéristiques Σ appartenant à $d > 1$ est $\geqq \frac{2^{n-a-1}}{n_1} = \frac{2^{n-1}.d}{3n}$ et $\leqq 2^{n-a-1}$. Chacun de ces systèmes de triples possède *au moins* le groupe cyclique $\{|x,\ 1+x|\}$ et *au plus* le diviseur métacyclique $\{|x,\ 1+x|,\ |x,\ \alpha^\omega x|\}$ où $\omega = 2^{a+1}.d$, a étant le nombre des facteurs 2 qui restent dans le quotient $\frac{3n}{d}$.

II. Le *nombre* des systèmes de triples *différents* déterminés par le système des caractéristiques principales est $\geqq \frac{2^{n-a-1}}{n_1'} = \frac{2^{n-1}}{n}$ et $\leqq 2^{n-a-1}$. Chacun de ces systèmes de triples possède *au moins* le diviseur métacyclique $\{|x,\ 1+x|,\ |x,\ \alpha^{2n} x|\}$ et *au plus* le diviseur métacyclique $\{|x,\ 1+x|,\ |x,\ \alpha^\omega x|\}$ où $\omega = 2^{a+1}$, a étant le nombre des facteurs 2 contenus dans n.

n_1 et n_1' sont des entiers impairs; dans la première partie de I et II, le premier signe d'égalité ne vaut que pour $n_1 = 1$, resp. $n_1' = 1$. Mais alors dans I, resp. dans II, les deux limites données sont égales et 2^{n-a-1} est le nombre *exact* des systèmes de triples différents déterminés par le système de caractéristiques en question.

Prenons ici le cas où $n_1' = 1$. Alors $n = 2^a$ et $N = 6.2^a + 1$. Il y a des nombres premiers de cette forme: 13, 97, 193, 769, 12 289, etc. Les diviseurs de n sont 1, 2, 2^2, ..., 2^a. Ceux de $3n$ sont: 1, 2, ..., 2^a; 3, 3.2, ..., 3.2^a. Le système des caractéristiques principales détermine exactement 2^{n-a-1} systèmes de triples différents. Un système de caractéristiques appartenant à $d = 3.2^i$, $i = 0, 1, \ldots, a$, détermine exactement $2^{n-a+i-1}$ systèmes de triples différents. Par contre pour un système de caractéristiques appartenant à $d = 2^i$, $i = 2, 3, \ldots, a$, le nombre des systèmes de triples différents reste $> \frac{2^{n-a+i-1}}{3}$ et $\leqq 2^{n-a+i-1}$.

50. *Le cas* $d = 3$, déduit de l'équation (50), donnera *la même équation* (53), que le cas $d = 1$ tel que nous venons de le traiter (§ 48). En effet pour $d = 3$, $\frac{3n}{d} = 2^a . n_1 = n = 2^a . n_1'$ (§ 46 et 48). Donc $n_1 = n_1'$ et les coefficients de l'équation (50) sont dans ce cas les mêmes que ceux de l'équation (53).

51. Pour les premières valeurs de N, premier de la forme $6n + 1$, étudiées jusqu'ici et pour lesquelles j'ai le nombre exact des systèmes de triples différents, soit $N = 7$, 13, 19, 31, 37, 43, les diviseurs d de $3n$ sont uniquement des formes 1, 3, n, $\frac{3n}{2}$, $3n$. Pour $d = 3n$ et $d = \frac{3n}{2}$, le nombre exact des systèmes de triples différents est déterminé (§ 47). Pour $d = n$, j'ai indiqué les solutions de l'équation (51) que j'ai obtenues pour $N = 19$, 31, 37 et 43. Je donnerai encore ici l'équation (50)-(53) *commune* aux cas $d = 1$ et $d = 3$ pour $N = 19$, 31, 37 et 43, et les solutions obtenues; pour $N = 7$ et 13 il n'existe que le système des caractéristiques principales et la résolution de l'équation correspondante est immédiate.

$N = 19$; $n = 2^0 . 3$; diviseurs de n_1': $\mu_1' = 1, \mu_2' = 3$; équation $x_1 + 3x_2 = 2^2$
$N = 31$; $n = 2^0 . 5$; „ „ „ : $\mu_1' = 1, \mu_2' = 5$; „ $x_1 + 5x_2 = 2^4$
$N = 37$; $n = 2^1 . 3$; „ „ „ : $\mu_1' = 1, \mu_2' = 3$; „ $x_1 + 3x_2 = 2^4$
$N = 43$; $n = 2^0 . 7$; „ „ „ : $\mu_1' = 1, \mu_2' = 7$; „ $x_1 + 7x_2 = 2^6$

Pour les quatre équations, la solution (x_1, x_2) pour laquelle $x_1 + x_2$ est *minimum* est celle fixée par $x_1 = 1$; *c'est celle que nous avons trouvée dans les quatre cas, soit pour le système des caractéristiques principales, soit pour l'unique système de caractéristiques qui appartient à* $d = 3$ *dans chacun des quatre cas,* c'est-à-dire: pour $N = 19$, $x_1 = 1$, $x_2 = 1$; pour $N = 31$, $x_1 = 1$, $x_2 = 3$; pour $N = 37$, $x_1 = 1$, $x_2 = 5$; pour $N = 43$, $x = 1$, $x_2 = 9$.

Lorsque l'équation (50) - (53) commune aux cas $d = 1$ et $d = 3$ n'a que *deux* termes au second membre, ce qui a lieu et uniquement pour $n = 2^a . p$ (p premier impair), le système des caractéristiques principales et chaque système de caractéristiques appartenant à $d = 3$ *déterminent des systèmes de triples qui possèdent le diviseur d'étendue maximale* $\{ | x, 1 + x |, | x, \alpha^{\omega} x | \}$ où $\omega = 2^{a+1}$ resp. $2^{a+1} . 3$, puisque dans ce cas une solution ne saurait comprendre $x_1 = 0$. En particulier, lorsque $n = 2^0 . p = p$, l'équation est $2^{p-1} = x_1 + p x_2$. On a $2^{p-1} \equiv 1 \bmod p$. La solution (x_1, x_2) pour laquelle $x_1 + x_2$ est *minimum* est alors $x_1 = 1$, $x_2 = \dfrac{2^{p-1} - 1}{p}$; c'est la solution trouvée plus haut dans les cas $N = 19$, 31 et 43.

Pour les valeurs suivantes de $N = 6n + 1$ premier, jusqu'à 100, l'équation en question est encore à deux termes:

$$\begin{array}{llll} N = 61 ; & n = 2^1 . 5 ; & \text{l'équation est:} & x_1 + 5 x_2 = 2^8, \\ N = 67 ; & n = 2^0 . 11 ; & \text{„} \quad \text{„} & x_1 + 11 x_2 = 2^{10}, \\ N = 73 ; & n = 2^2 . 3 ; & \text{„} \quad \text{„} & x_1 + 3 x_2 = 2^9, \\ N = 79 ; & n = 2^0 . 13 ; & \text{„} \quad \text{„} & x_1 + 13 x_2 = 2^{12}. \end{array} \tag{54}$$

Resterait le cas $N = 97$, mais sur ce cas nous sommes fixés (§ 49, dernier alinéa): son système des caractéristiques principales et ses quatre systèmes de caractéristiques différents qui appartiennent à $d = 3$, déterminent chacun 2^{11} systèmes de triples différents.

Pour $N = 61$, 67 et 79, il y a deux systèmes de caractéristiques différents qui appartiennent à $d = 3$; pour $N = 73$, il y en a trois. Il serait intéressant de déterminer si la solution de l'équation (54) correspondante est toujours, soit pour le système des caractéristiques principales, soit pour ces systèmes appartenant à $d = 3$, celle du *minimum* pour $x_1 + x_2$, comme dans les quatre cas étudiés jusqu'ici.

(Reçu le 18 avril 1931)