ACTA ARITHMETICA
XV (1969)

Sur les diviseurs premiers des polynômes

par

T. NAGELL (Uppsala)

1. Introduction. Dans ce travail polynôme signifie, sauf avis contraire, un polynôme non constant à coefficients entiers rationnels.

Soit donné le polynôme $f(x)$ de x. Si p est un nombre premier, et si la congruence

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

admet (au moins) une solution x, on dit que p est un *diviseur premier du polynôme* $f(x)$. Il est bien connu que tout polynôme $f(x)$ admet une infinité de diviseurs premiers (théorème de Schur); voir Schur [8] (1) ou Nagell [6], théorème 45. D'autre part, si $f(x)$ est irréductible et d'un degré $\geqslant 2$, on peut montrer qu'il existe une infinité de nombres premiers, tels que la congruence (1) n'ait pas de solutions (théorème de Frobenius); ce résultat est une conséquence des lois de densité de Frobenius–Tchebotareff; voir p.ex. Hasse [4], §§ 23–24, et aussi [3].

Soit maintenant $g(x)$ un autre polynôme de x, et considérons la congruence

$$g(x) \equiv 0 \pmod{p}. \tag{2}$$

Alors on peut se demander s'il existe des nombres premiers p tels que toutes les deux congruences (1) et (2) soient résolubles. Dans un travail publié en 1923 j'ai montré qu'en effet il existe une infinité de tels nombres premiers quels que soient les deux polynômes. D'ailleurs dans ce travail-là, nous avons obtenu des résultats plus précis sur les diviseurs premiers communs aux deux polynômes. Les démonstrations reposent sur la théorie des corps algébriques; voir Nagell [5].

Dans les sections suivantes nous allons d'abord donner une démonstration très simple, sans recourir à la théorie des idéaux, de l'existence d'une infinité des nombres premiers en question. Notre premier but est donc d'établir le

(1) Les numéros figurant entre crochets renvoient à la bibliographie placée à la fin de ce mémoire.

THÉORÈME 1. *Il existe une infinité de diviseurs premiers communs à deux polynômes quelconques.*

Il suffit évidemment de supposer que les deux polynômes soient de degré $\geqslant 2$. Le théorème est évident si l'un des polynômes contient un facteur linéaire rationnel.

2. Lemmes. Soient donnés les deux polynômes $f(x)$ de degré $N \geqslant 2$ et $g(x)$ de degré $M \geqslant 2$. Nous avons besoin du résultat suivant:

LEMME 1. *Pour établir le Théorème 1 pour $f(x)$ et $g(x)$ il suffit de supposer que $N > M$.*

En effet, si $f(x)$ et $g(x)$ sont du même degré ($M = N$), nous pouvons déterminer trois entiers rationnels a, b et c tels qu'on ait

$$h(x) = af(x+c) - bg(x), \tag{3}$$

où le degré de $h(x)$ est $\leqslant N-1$. Le nombre c peut être choisi de façon que $h(x)$ ne soit pas constant. En effet, si l'on a pour $c \neq c_1$

$$af(x+c) - bg(x) = k, \qquad af(x+c_1) - bg(x) = k_1,$$

k et k_1 étant des constantes, on obtient

$$a[f(x+c) - f(x+c_1)] = k - k_1.$$

Or, cela est impossible vu que $f(x)$ n'est pas linéaire. Il en résulte que la congruence (2) peut être remplacée par la congruence

$$h(x) \equiv 0 \pmod{p}.$$

Cela démontre le Lemme 1.

Il est évident qu'on peut y ajouter le

LEMME 2. *Si a est le coefficient de x^N dans $f(x)$, et si b est le coefficient de x^M dans $g(x)$, on peut supposer que $a = b = 1$.*

Soit maintenant c un nombre entier rationnel, et divisons $f(x+c)$ par $g(x)$. Alors, nous aurons une relation

$$f(x+c) = g(x)h(x) + g_1(x), \tag{4}$$

où $h(x)$ et $g_1(x)$ sont des polynômes en x à coefficients entiers rationnels. Le degré de $h(x)$ est $= N-M$, et le degré de $g_1(x)$ est $\leqslant M-1$. Les coefficients de $h(x)$ et $g_1(x)$ sont des polynômes en c à coefficients entiers rationnels.

LEMME 3. *Si $M > 1$ il n'y a qu'un nombre limité de valeurs de c, pour lesquels le polynôme $g_1(x)$ dans (4) est une constante relativement à x.*

En effet, supposons que, pour une valeur donnée de c, $g_1(x)$ soit $= k(c)$, polynôme qui ne dépend que de c. Alors, si η est une racine de $g(x) = 0$, il résulte de (4), lorsqu'on y pose $x = \eta$,

$$f(\eta+c) = k(c).$$

On peut évidemment supposer que η soit d'un degré $\geqslant 2$. Si η' est un nombre conjugué à η, on a aussi

$$f(\eta'+c) = k(c).$$

On aura donc

$$f(\eta+c) - f(\eta'+c) = 0.$$

Or, cette relation ne peut subsister que pour un nombre fini de valeurs de c, $f(x)$ et η étant donnés. Donc, il y a un nombre infini de valeurs de c pour lesquels $g_1(x)$ n'est pas constant.

3. Démonstration du Théorème 1. Le théorème est vrai lorsque l'un des polynômes est linéaire. Considérons maintenant de nouveau la relation

$$f(x+c) = g(x)h(x) + g_1(x), \tag{5}$$

où $f(x)$, $g(x)$, $g_1(x)$ et c satisfont aux conditions données dans les lemmes du numéro précédent. On a donc $N > M \geqslant 2$, et c est choisi de façon que $g_1(x)$ ne soit pas constant.

Nous ferons la démonstration du Théorème 1 par induction complète. Supposons que le théorème soit vrai pour tous les polynômes de degré $< N$. Introduisons dans $g_1(x)$ au lieu de x la variable $y = x+c$. Alors $g_1(x)$ sera remplacé par le polynôme $g_2(y)$ dont les coefficients seront des polynômes en c à coefficients entiers rationnels. Le degré de $g_2(y)$ en y est > 0 et $< M$. Alors, d'après la supposition faite tout-à-l'heure sur la validité du Théorème 1 pour les polynômes de degré $< N$, celui-ci est vrai pour les polynômes $g(x)$ et $g_2(y)$. Si les nombres $g(x_0)$ et $g_2(y_0)$ sont divisibles par le nombre premier p, le nombre $f(x_0+c) = f(y_0)$ l'est aussi. Cela démontre notre assertion, vu qu'il y a une infinité de valeurs de c satisfaisant à la condition nécessaire.

4. Extensions du théorème de Schur. Soit n un nombre naturel $\geqslant 3$, et posons

$$F_n(x) = \prod_{\beta} (x - \varepsilon), \tag{6}$$

où le produit est étendu à toutes les $\varphi(n)$ racines n-ièmes primitives de l'unité ε. Alors il est bien connu que les diviseurs premiers de $F_n(x)$, qui ne divisent pas n, sont $\equiv 1 \pmod{n}$; voir p.ex. Nagell [6], théorème 94. Alors, si nous appliquons le Théorème 1 au cas où l'un des polynômes est $F_n(x)$, nous aurons le résultat:

THÉORÈME 2. *Tout polynôme $f(x)$ admet une infinité de diviseurs premiers congrus à 1 modulo n, lorsque n est un nombre naturel quelconque.*

Il y a lieu de comparer ce résultat avec le théorème suivant:

THÉORÈME 3. *Tout polynôme, possédant au moins un zéro réel, admet une infinité de diviseurs premiers qui ne sont pas congrus à* 1 *modulo* n, *où* n *est un nombre naturel quelconque* $\geqslant 3$.

Pour la démonstration voir Nagell [6], théorème 97; comparez aussi la remarque à la fin de ce numéro.

Ces deux résultats nous mènent à poser le problème suivant: Trouver les conditions nécessaires et suffisantes pour qu'un polynôme n'admette que des diviseurs premiers $\equiv 1 \pmod n$, où n est un nombre naturel $\geqslant 3$, abstraction faite d'un nombre fini de nombres premiers. Une condition nécessaire est évidemment que toutes les zéros du polynôme soient imaginaires.

Soit $F_n(x)$ le polynôme défini par (6), et posons

$$F_n(x, y) = y^{\varphi(n)} F_n\left(\frac{x}{y}\right).$$

Soit N un multiple de n. Alors, si $f(x)$ et $g(x)$ désignent des polynômes arbitraires, premiers entre eux, il est évident que les polynômes

$$F_N[f(x), g(x)],$$

aussi bien qu'un produit de polynômes de ce type, avec N, $f(x)$ et $g(x)$ variables, jouissent de la propriété en question.

Or, il est évident que cette observation ne donne pas la solution complète du problème.

Remarque. Dans mon livre [6] j'ai présenté le Théorème 3 sous le titre Théorème de Bauer. En réalité, Bauer a seulement établi le résultat suivant:

Soit $f(x)$ *un polynôme possédant au moins un zéro réel et jouissant de la propriété suivante: Les diviseurs premiers, excepté un nombre fini, sont congrus à* $+1$ *ou à* -1 *modulo* n, n *étant un nombre naturel* $\geqslant 3$. *Alors il y a une infinité de diviseurs premiers* $\equiv -1 \pmod n$.

Voir Bauer [1]. Cependant, j'ai trouvé qu'on peut, en modifiant la démonstration de Bauer, obtenir le meilleur résultat exprimé par le Théorème 3.

5. Une précision du Théorème 1. Dans le mémoire [5], cité plus haut, j'ai établi le résultat suivant:

THÉORÈME 4. *Soient donnés les deux polynômes* $f(x)$ *et* $g(x)$ *irréductibles dans le corps rationnel. Alors il existe une infinité de nombres premiers* p, *tels que le nombre de solutions incongrues de chacune des deux congruences*

$$f(x) \equiv 0 \pmod p \quad \text{et} \quad g(x) \equiv 0 \pmod p$$

soit égal au degré du polynôme entrant dans la congruence.

Vu que ce résultat est resté tout-à-fait inconnu je le juge nécessaire d'en recapituler la démonstration. Celle-ci est basée sur certains faits de la théorie des idéaux.

Soient $\boldsymbol{K}$ un corps algébrique du N-ième degré et $\boldsymbol{U}$ un sous-corps de $\boldsymbol{K}$ du n-ième degré. Soit encore $\mathfrak{p}$ un idéal premier du premier degré dans $\boldsymbol{K}$. La norme dans $\boldsymbol{K}$ de $\mathfrak{p}$ relativement au sous-corps $\boldsymbol{U}$ est un idéal $\mathfrak{j}$ dans $\boldsymbol{U}$, donc

$$N_{\boldsymbol{U}}(\mathfrak{p}) = \mathfrak{j}.$$

Si p est le nombre premier (rationnel) qui est divisible par $\mathfrak{p}$, la norme dans $\boldsymbol{U}$ de $N_{\boldsymbol{U}}(\mathfrak{p})$ relativement au corps rationnel est égal à p vu que $\mathfrak{p}$ est du premier degré, donc

$$N(\mathfrak{j}) = p.$$

Il en résulte que $\mathfrak{j}$ est un idéal premier du premier degré dans $\boldsymbol{U}$. Alors, à chaque idéal premier du premier degré $\mathfrak{p}$ dans $\boldsymbol{K}$ qui divise le nombre premier p, il correspond un idéal premier du premier degré $\mathfrak{j}$ dans $\boldsymbol{U}$ qui divise p. Encore, si le nombre premier p est le produit de N idéaux premiers du premier degré dans $\boldsymbol{K}$, il est le produit de n idéaux premiers du premier degré dans $\boldsymbol{U}$. En effet, supposons qu'on ait

$$p = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_N,$$

où $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_N$ sont des idéaux premiers du premier degré dans $\boldsymbol{K}$, et que

$$N_{\boldsymbol{U}}(\mathfrak{p}_i) = \mathfrak{j}_i,$$

où, d'après ce que nous venons de voir, $\mathfrak{j}_i$ est un idéal premier du premier degré dans $\boldsymbol{U}$. Alors, on obtient

$$N_{\boldsymbol{U}}(p) = \mathfrak{j}_1 \mathfrak{j}_2 \dots \mathfrak{j}_N = p^{N/n}.$$

Il en résulte que tous les idéaux premiers dans $\boldsymbol{U}$ qui divisent p sont du premier degré. Par conséquent p est un produit de tels idéaux premiers dans $\boldsymbol{U}$.

Supposons maintenant que $\boldsymbol{K}$ soit un corps de Galois. On sait que dans les corps de Galois on a la loi suivante: Si le nombre premier p est divisible par un idéal premier du premier degré, il est égal à un produit de tels idéaux premiers.

Soit $F(x)$ un polynôme irréductible du N-ième degré tel que le corps $\boldsymbol{K}$ soit engendré par une racine de l'équation $F(x) = 0$. Soit ensuite $f(x)$ un polynôme irréductible du n-ième degré tel que le corps $\boldsymbol{U}$ soit engendré par une racine de l'équation $f(x) = 0$.

Alors il résulte de ce qui précède: Si la congruence

$$F(x) \equiv 0 \pmod p, \tag{7}$$

où p est un nombre premier, est résoluble, la congruence

$$f(x) \equiv 0 \pmod{p} \tag{8}$$

l'est aussi. De plus, si la congruence (7) admet N solutions incongrues, la congruence (8) admet n solutions incongrues.

Soient maintenant $f(x)$ et $g(x)$ deux polynômes irréductibles dans le corps rationnel; et soient de plus $\boldsymbol{U}$ un corps algébrique de degré n engendré par une racine de l'équation $f(x) = 0$ et $\boldsymbol{U}_1$ un corps algébrique de degré m engendré par une racine de l'équation $g(x) = 0$. Soit enfin $\boldsymbol{K}$ un corps de Galois qui contient et $\boldsymbol{U}$ et $\boldsymbol{U}_1$; et supposons que $\boldsymbol{K}$ soit engendré par une racine de l'équation $F(x) = 0$, où $F(x)$ soit défini comme plus haut. Alors, si la congruence

$$F(x) \equiv 0 \pmod{p} \tag{9}$$

admet une solution pour le nombre premier p, il en est de même pour les congruences

$$f(x) \equiv 0 \pmod{p}, \tag{10}$$

$$g(x) \equiv 0 \pmod{p}. \tag{11}$$

De plus, il résulte de ce que nous venons de montrer: Si la congruence (9) admet N solutions incongrues, la congruence (10) admet n solutions incongrues et la congruence (11) m solutions incongrues.

Cela démontre le Théorème 4 vu que le polynôme $F(x)$ possède une infinité de diviseurs premiers.

6. Une précision du Théorème 2. A l'aide du Théorème 4 il est possible d'obtenir la précision suivante du Théorème 2:

THÉORÈME 5. *Soient $f(x)$ un polynôme irréductible de degré n et m un nombre naturel quelconque. Alors, il existe une infinité de nombres premiers $p \equiv 1 \pmod{m}$ tels que la congruence*

$$f(x) \equiv 0 \pmod{p}$$

possède n solutions incongrues.

Pour établir ce résultat on aura seulement à prendre, dans le Théorème 4, $g(x)$ égal au polynôme cyclotomique $F_m(x)$ définie par l'équation (6). Le Théorème 5 se trouve déjà dans le mémoire [5].

7. Remarques supplémentaires. Il est évident que le Théorème 4 est vrai même si le nombre de polynômes est > 2.

La généralisation suivante de ce théorème a été donnée par Fjellstedt:

THÉORÈME 6. *Soient Ω un corps algébrique, $f(x)$ et $g(x)$ des polynômes dans Ω n'admettant aucun zéro multiple. Soient de plus $f(x)$ de degré n et $g(x)$ de degré m. Alors, il y a une infinité d'idéaux premier* p *dans Ω tels que la congruence*

$$f(x) \equiv 0 \pmod{\mathfrak{p}}$$

ait n solutions incongrues, et que la congruence

$$g(x) \equiv 0 \pmod{\mathfrak{p}}$$

ait m solutions incongrues.

Pour la démonstration voir Fjellstedt [2], Satz 1.

Soit $f(x)$ un polynôme *irréductible* d'un degré $\geqslant 2$. Si p est un nombre premier tel que la congruence

$$f(x) \equiv 0 \pmod{p}$$

n'ait pas de solutions, nous dirons, pour raccourcir, que p est un *non-diviseur* de $f(x)$. D'après le théorème de Frobenius, cité plus haut, $f(x)$ admet une infinité de non-diviseurs; voir [3].

Soient maintenant $f(x)$ et $g(x)$ deux polynômes irréductibles, tous les deux d'un degré $\geqslant 2$. Alors on peut se demander s'il existe une infinité de nombres premiers p qui sont des non-diviseurs de tous les deux polynômes. Cela n'est pas toujours le cas ainsi qu'on le verra de l'exemple suivant. Choisissons les polynômes

$$f(x) = x^3 - 2 \quad \text{et} \quad g(x) = x^2 + x + 1.$$

Il est bien connu que la congruence

$$x^3 - 2 \equiv 0 \pmod{p} \tag{12}$$

est résoluble pour tous les nombres premiers $p \equiv -1 \pmod 3$ et pour tous les nombres premiers $p \equiv 1 \pmod 3$ représentables sous la forme

$$p = x^2 + 27y^2,$$

où x et y sont des nombres naturels. Pour tous les autres nombres premiers $p > 3$ la congruence (12) n'a pas de solutions. Donc, tous les non-diviseurs de $f(x)$ sont $\equiv 1 \pmod 3$, et leur densité est égale à 1/3. Pour la démonstration voir Nagell [7], théorème 4. D'autre part, les non-diviseurs de $g(x)$ sont tous les nombres premiers $\equiv -1 \pmod 3$. Donc, les polynômes $x^3 - 2$ et $x^2 + x + 1$ n'ont aucun non-diviseur commun. Les diviseurs premiers communs aux deux polynômes ont la densité 1/6.

Cependant, il est facile d'indiquer des cas dans lesquels il existe une infinité de non-diviseurs communs à deux polynômes. En effet, nous allons établir le résultat suivant:

THÉORÈME 7. *Soient $f(x)$ et $g(x)$ des polynômes quadratiques irréductibles, et tels que les corps quadratiques engendrés par les équations*

$f(x) = 0$ et $g(x) = 0$ soient distincts. Alors, il existe une infinité de non-diviseurs communs aux deux polynômes. La densité de ces nombres premiers est positive.

Démonstration. Il suffit évidemment de considérer les polynômes

$$f(x) = x^2 - D \quad \text{et} \quad g(x) = x^2 - D_1, \tag{13}$$

où D et D_1 signifient des nombres entiers rationnels, différents entre eux et différents de 1, qui ne sont divisibles par le carré d'aucun nombre premier. Les non-diviseurs p (sauf un nombre fini d'exceptions) de $f(x)$ sont caractérisés par des congruences du type $p \equiv r_i \pmod{4|D|}$, où r_i désigne $\frac{1}{2}\varphi(4|D|)$ nombres naturels dans l'intervalle $0 - 4|D|$ qui sont premiers avec $4|D|$. Les non-diviseurs p (sauf un nombre fini d'exceptions) de $g(x)$ sont caractérisés par des congruences du type $p \equiv s_j \pmod{4|D_1|}$, où s_j désigne $\frac{1}{2}\varphi(4|D_1|)$ nombres naturels dans l'intervalle $0 - 4|D_1|$ qui sont premiers avec $4|D_1|$. Pour la démonstration de ces faits voir p. ex. Nagell [6], pp. 149–153.

Ainsi, tout non-diviseur commun doit satisfaire aux congruences

$$p \equiv r_i \pmod{4|D|}, \quad p \equiv s_j \pmod{4|D_1|} \tag{14}$$

pour certaines valeurs de r_i et s_j. Posons maintenant $|D| = \delta d$ et $|D_1| = \delta d_1$, où d, d_1 et δ sont des nombres naturels, tels que $(d, d_1) = 1$. Soit ensuite $D^* = |DD_1|/\delta$. Alors les congruences (14) peuvent s'écrire

$$p \equiv q_i \pmod{4D^*}, \quad p \equiv t_j \pmod{4D^*}, \tag{15}$$

où q_i parcourt $\frac{1}{2}\varphi(4|D|)\varphi(d_1)$ nombres naturels dans l'intervalle $0 - 4D^*$, tels que $(q_i, 4D^*) = 1$, et où t_j parcourt $\frac{1}{2}\varphi(4|D_1|)\varphi(d)$ nombres naturels dans l'intervalle $0 - 4D^*$, tels que $(t_j, 4D^*) = 1$. Alors, on montre sans peine qu'il existe, au moins, une paire de valeurs i et j telle qu'on ait $q_i = t_j$. Cela démontre le Théorème 7. Par un raisonnement détaillé on peut évidemment obtenir un résultat plus précis et, en outre, montrer que la densité des non-diviseurs est égale à 1/4.

Lorsque $D \equiv D_1 \equiv 1 \pmod 4$ il suffit dans les congruences (14) et (15) de choisir les modules $2|D|$, $2|D_1|$ et $2D^*$.

Il est évident qu'on peut employer la même méthode pour déterminer les diviseurs premiers communs aux deux polynômes (13).

Exemples numériques. 1. Prenons les polynômes

$$x^2 - 2 \quad \text{et} \quad x^2 + 2.$$

Les non-diviseurs du premier polynôme sont les nombres premiers $\equiv \pm 3 \pmod 8$; les non-diviseurs de l'autre polynôme sont les nombres premiers $\equiv 5$ ou $\equiv 7 \pmod 8$. Donc, les non-diviseurs communs sont les nombres premiers $\equiv 5 \pmod 8$.

2. Prenons ensuite les polynômes

$$x^2 + x + 1 \quad \text{et} \quad x^2 - 5.$$

Les non-diviseurs du premier polynôme sont les nombres premiers $\equiv -1 \pmod 3$; les non-diviseurs de l'autre polynôme sont les nombres premiers $\equiv 3$ ou $\equiv 7 \pmod{10}$. On aura alors à comparer les deux series de congruences

$$p \equiv 11, 17, 23, 29 \pmod{30}, \quad p \equiv 7, 13, 17, 23 \pmod{30}.$$

Il en résulte que les non-diviseurs communs sont les nombres premiers $\equiv 17$ ou $\equiv 23 \pmod{30}$.

3. Comme troisième exemple prenons les polynômes

$$x^2 - 21 \quad \text{et} \quad x^2 + 15.$$

Les non-diviseurs du premier polynôme sont les nombres premiers safisfaisant aux congruences

$$p \equiv 11, 13, 19, 23, 29, 31 \pmod{42}.$$

Les non-diviseurs de l'autre polynôme sont caractérisés par les congruences

$$p \equiv 7, 11, 13, 29 \pmod{30}.$$

On aura alors à comparer les deux séries de congruences

$$p \equiv 11, 13, 19, 23, 29, 31, 53, 61, 71, 73, 97, 103, 107, 113,$$
$$137, 139, 149, 157, 179, 181, 187, 191, 197, 199 \pmod{210}$$

et

$$p \equiv 11, 13, 29, 37, 41, 43, 59, 67, 71, 73, 89, 97, 101, 103,$$
$$127, 131, 149, 157, 163, 179, 187, 191, 193, 209 \pmod{210}.$$

Il en résulte que les non-diviseurs communs sont les nombres premiers satisfaisant aux congruences

$$p \equiv 11, 13, 29, 71, 73, 97, 103, 149, 157, 179, 187, 191 \pmod{210}.$$

On montre sans peine que le Théorème 7 peut être étendu au cas où les équations $f(x) = 0$ et $g(x) = 0$ engendrent des corps abéliens de degré $\geqslant 2$.

Travaux cités

[1] M. Bauer, *Über die arithmetische Reihe*, Journal für Mathematik, Bd. 131, Berlin 1906.

[2] L. Fjellstedt, *Bemerkungen über gleichzeitige Lösbarkeit von Kongruenzen*, Ark. Mat. 3 (14), Stockholm 1955.

[3] G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Sitzungsber. Preuss. Akad. Wiss., Math.-Phys. Kl., Berlin 1896.

[4] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II: *Reziprozitätsgesetze*, Jahresber. der Deutschen Mathematischen Vereinigung, Bd. 36, Berlin 1930.

[5] T. Nagell, *Zahlentheoretische Notizen I, Ein Beitrag zur Theorie der höheren Kongruenzen*, Videnskapsselskapets Skrifter I, Matem.-Naturv. Klasse, No. 13, Kristiania 1923.

[6] — *Introduction to number theory*, New York 1951.

[7] — *Sur quelques problèmes dans la théorie des restes quadratiques et cubiques*, Ark. Mat. 3 (16), Stockholm 1955.

[8] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungsber. Berliner Math. Gesellsch., 11. Jahrg., Berlin 1912.

INSTITUT DE MATHÉMATIQUES DE L'UNIVERSITÉ D'UPPSALA

Reçu par la Rédaction le 2. 5. 1968

ACTA ARITHMETICA
XV (1969)

Remarque sur le travail précédent de T. Nagell

par

A. Schinzel (Varsovie)

Dans le travail [3] qui précède T. Nagell demande quels sont pour un nombre n donné quelconque les polynômes, dont tous les diviseurs premiers sont de la forme $nt+1$, abstraction faite d'un nombre fini des cas. Il suffit évidemment de résoudre ce problème pour les polynômes irréductibles. Nous allons démontrer

Théorème. *Soit n un nombre naturel quelconque, ζ_n une racine primitive de degré n de l'unité et soit $G(x)$ un polynôme irréductible. Afin que tous les diviseurs premiers de $G(x)$, abstraction faite d'un nombre fini des cas, soient de la forme $nt+1$ il faut et il suffit que*

$$(*) \qquad G(x) = aN\big(H(x)\big),$$

où $H(x)$ est un polynôme à coefficients du corps $Q(\zeta_n)$, N est la norme dans ce corps et a est un nombre rationnel.

Démonstration. Nécessité. Soit θ une racine de G et soit $k = Q(\theta)$ le corps engendré par θ. Les nombres premiers, qui ont un facteur premier idéal de degré 1 dans k sont des diviseurs de $G(x)$, donc étant de la forme $nt+1$ ils se décomposent complètement dans le corps $Q(\zeta_n)$. En vertu du théorème de Bauer ([1], voir [2], lemme 3) $Q(\zeta_n)$ est contenu dans k. La condition $(*)$ résulte maintenant du lemme 2 de [2] après la substitution $J = Q(\zeta_n)$.

Suffisance. Posons dans le lemme 1 de [2] $f(x) = G(x)/a$, $K = Q(\zeta_n)$. Les hypothèses étant satisfaites il en résulte que tous les diviseurs premiers suffisamment grands de $G(x)$ se décomposent dans K en facteurs premiers idéaux de degré 1. Ceci veut dire que ces diviseurs sont de la forme $nt+1$, q.e.d.

Dans le même ordre d'idées on peut démontrer le théorème plus général suivant:

Soit J un corps Bauerien (cf. [4], p. 333) *et soit $G(x)$ un polynôme irréductible. Afin que tous les diviseurs premiers de $G(x)$, abstraction faite*