SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

GEORGES RHIN

Équirépartition modulo 1 dans un corps de séries formelles sur un corps fini

Séminaire de théorie des nombres de Bordeaux (1970-1971), exp. n° 5, p. 1-12

<http://www.numdam.org/item?id=STNB_1970-1971____A5_0>

Séminaire de Théorie des Nombres 7-01
Année 1970-1971 , exposé n° 7 1er décembre 1970

EQUIREPARTITION MODULO 1 DANS UN CORPS DE SERIES FORMELLES SUR UN CORPS FINI

par

Georges RHIN

-:-:-:-

D'après [7], la suite $p\alpha$, où p décrit la suite croissante des nombres premiers, est équirépartie modulo 1 si, et seulement si, α est irrationnel. Nous généralisons ce théorème à un corps de séries formelles sur un corps fini.

1. - NOTATIONS ET RAPPELS

Soit F_q le corps fini à q éléments, de caractéristique $p \neq 2$. Nous désignerons par $\mathfrak{F}$ le corps des fractions $F_q(x)$. On munit $\mathfrak{F}$ de la valeur absolue ultramétrique discrète, dite "O-adique", en posant pour tout polynôme non nul A de $F_q[x]$, dont on désigne le degré par $d°A$,

$$|A| = q^{d°A} .$$

Le complété $\mathfrak{F}_o$ de $\mathfrak{F}$ pour la valeur absolue "O-adique" est le corps $F_q\{x^{-1}\}$ des séries formelles

$$\theta = \sum_{n=-\infty}^{\infty} a_n x^{-n} \quad , \quad a_n \in F_q \quad \text{et} \quad a_n = 0 \quad \text{pour} \quad n < n_\theta .$$

On désigne par $\mathfrak{P}$ l'idéal de valuation de $\mathfrak{F}_o$ qui est l'ensemble des séries formelles

$$\theta = \sum_{n=1}^{\infty} a_n x^{-n} \quad , \quad a_n \in F_q .$$

On définit l'homomorphisme $\mathfrak{K}_o$ du groupe additif $\mathfrak{F}_o^+$ sur le groupe addifit $\mathfrak{P}^+$ par

$$\mathfrak{K}_o\left(\sum_{n=-\infty}^{\infty} a_n x^{-n}\right) = \sum_{n=1}^{\infty} a_n x^{-n} .$$

$\mathfrak{K}_o(\theta)$ sera ici la "partie fractionnaire" de θ. Nous considèrerons la mesure de Haar du groupe additif localement compact $\mathfrak{F}_o^+$ normalisée par

$$\text{mes}\,\mathfrak{P} = 1 .$$

La mesure d'une boule $\mathfrak{B} = \alpha + \mathfrak{P}^d$ sera donc égale à q fois son rayon, c'est-à-dire,

$$\text{mes}\,\mathfrak{B} = q^{1-d} .$$

Carlitz [1] a donné la définition de l'équirépartition modulo 1 dans $\mathfrak{F}_o$.

Définition 1. - Une suite $(\alpha_n)_{n\geq 1}$ d'éléments de $\mathfrak{F}_o$ est dite équirépartie modulo 1 dans $\mathfrak{F}_o$ si la suite $(\mathfrak{K}_o(\alpha_n))_{n\geq 1}$ est équirépartie dans le groupe compact $\mathfrak{P}^+$.

Soit ψ un caractère différent de 1 du groupe additif F_q^+, et soit e_o le caractère de $\mathfrak{F}_o^+$, défini par

$$e_o\left(\sum_{n=-\infty}^{\infty} a_n x^{-n}\right) = \psi(a_1) .$$

Alors $e_o(H\,.)$ pour $H \in F_q[x]$ décrit l'ensemble des caractères e du groupe additif $\mathfrak{F}_o^+$ tels que

$$e(\theta) = e(\mathfrak{K}_o(\theta)) .$$

Ces caractères forment un sous-groupe du dual de $\mathfrak{F}_o^+$ isomorphe au dual de $\mathfrak{P}^+$.

On a alors le critère de Weyl [6] :

PROPOSITION 1. La suite $(\alpha_n)_{n\geq 1}$ d'éléments de $\mathfrak{F}_o$ est équirépartie modulo 1 dans $\mathfrak{F}_o$ si, et seulement si,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e_o(H\alpha_n) = 0 \quad , \quad \forall\, H \in F_q[x]^* .$$

2. - ENONCE DU THEOREME PRINCIPAL

Soit un ordre sur F_q. Nous définissons l'ordre Ω suivant sur $F_q[x]^*$.

Définition 2. - Soient $A = a_n x^n + \ldots + a_o$, et $B = b_m x^m + \ldots + b_o$, deux éléments de $F_q[x]^*$ tels que $a_n \neq 0$ et $b_m \neq 0$, alors

$$A \leq B \quad \text{pour } \Omega \text{ si } n < m \text{ ou si } n = m ,$$

et

$$(a_n, \ldots, a_o) \leq (b_n, \ldots, b_o)$$

pour l'orgre lexicographique à gauche sur F_q^{n+1} déduit de l'ordre sur F_q.

Soit $(P_n)_{n\geq 1}$ la suite croissante (pour l'ordre Ω) des polynômes unitaires irréductibles de $F_q[x]$. Nous démontrons alors le théorème suivant :

THEOREME 1. La suite $(P_n \alpha)_{n\geq 1}$ est équirépartie modulo 1 si, et seulement si, $\alpha \notin \mathfrak{F}$.

Si $\alpha \in \mathfrak{F}$, $\alpha = \frac{A}{B}$, où A et B sont deux éléments de $F_q[x]$, et $B \neq 0$, alors en prenant $H = B$ dans le critère de Weyl, il vient

$$\frac{1}{N} \sum_{n=1}^{N} e_o(B P_n \alpha) = 1 ,$$

car, d'après la définition de e_o , $e_o(F_q[x]) = 1$, et ici

$$B P_n \alpha \in F_q[x] \quad \text{pour tout } n .$$

Donc la suite $(P_n \alpha)_{n \geq 1}$ n'est pas équirépartie modulo 1 .

Si $\alpha \notin \mathfrak{F}$, pour tout $H \in F_q[x]^*$, $\beta = H\alpha \notin \mathfrak{F}$. En utilisant le développement en fraction continue de β [6], on montre que, pour tout τ entier assez grand, il existe deux éléments A et Q de $F_q[x]$ tels que

$$(A , Q) = 1 \qquad \text{(i. e. } A \text{ et } Q \text{ sont étrangers),}$$

$$0 < |Q| \leq q^{\tau} \quad \text{et} \quad |\beta - \frac{A}{Q}| < \frac{q^{-\tau}}{|Q|} .$$

Soit N un entier ; alors il existe γ entier tel que $|P_N| = q^{\gamma}$.

Nous prenons alors ε réel $(0 < \varepsilon \leq \frac{1}{100})$ et $\tau = \gamma - [\gamma^{\varepsilon}]$. La démonstration sera différente selon les trois cas suivants

$$q^{\gamma^{\varepsilon}} \leq |Q| \leq q^{\tau}$$

$$\gamma < |Q| < q^{\gamma^{\varepsilon}}$$

$$|Q| \leq \gamma .$$

Les deux premiers cas se traitent en adaptant à $\mathfrak{F}_o$ les techniques des sommes trigonométriques de I. M. Vinogradov [7]. Le dernier cas nécessite une généralisation à $\mathfrak{F}_o$ d'un théorème de Siegel [4].

3. - ENONCE DU THEOREME DE SIEGEL

Soient R , Q , L trois éléments de $F_q[x]^*$, et γ un entier, tels que : R soit unitaire de degré γ et $(L, Q) = 1$.

$\pi(\gamma)$ désigne le nombre de polynômes unitaires irréductibles de $F_q[x]$, et $\Phi(Q)$ l'indicateur d'Euler de Q, c'est-à-dire le nombre de polynômes unitaires A de $F_q[x]$, tels que $d°A = d°Q$ et $(A, Q) = 1$. Pour k entier, $\pi(R, Q, L, k)$ désigne le nombre de polynômes irréductibles unitaires P de $F_q[x]$ tels que

$$|P - R| < q^{\gamma - k},$$

et Q divise $P-L$ dans $F_q[x]$.

THEOREME 2 (Siegel). Soit $u > 0$, alors pour tout polynôme Q de $F_q[x]^*$, et k entier, tels que

$$|Q| \leq \gamma^u \qquad \text{et} \qquad k^4 \leq \gamma,$$

nous avons

$$\left|\pi(R, Q, L, k) - \frac{\pi(\gamma)}{q^k \Phi(Q)}\right| \leq c(u)\, q^{\gamma - \sqrt{\gamma}},$$

où $c(u)$ est une constante positive qui ne dépend que de u.

Nous montrerons successivement comment la démonstration du troisième cas se ramène au théorème 2, puis comment la démonstration du théorème 2 nécessite la recherche, dans le plan complexe, des régions où les fonctions $L(., \chi)$, introduites par D. R. Hayes [5], ne s'annulent pas.

4. - LE TROISIEME CAS SE RAMENE AU THEOREME 2

Soit $\mathfrak{M}$ l'ensemble des polynômes unitaires de $F_q[x]$. Nous définissons la relation d'équivalence suivante sur $\mathfrak{M}$:

Définition 3. - Soit k entier, et soient A et B deux éléments de $\mathfrak{M}$ de même degré γ

$$A \mathcal{R}_{(k)} B \Leftrightarrow |A - B| < q^{\gamma - k}.$$

$\Re_{(k)}$ partage des polynômes de $\mathfrak{M}$ de degré γ en q^k classes d'équivalence de cardinal $q^{\gamma-k}$. Nous avons la relation suivante entre $\Re_{(k)}$ et l'ordre Ω :

PROPOSITION 2. *Si R_1 et R_2 sont deux éléments de même degré tels que $R_1 < R_2$ pour Ω, alors quels que soient les polynômes A et B, tels que*

$$A \,\Re_{(k)}\, R_1 \quad \text{et} \quad B \,\Re_{(k)}\, R_2 ,$$

nous avons $A < B$ si $|R_1 - R_2| \geq q^{\gamma-k}$.

Nous pouvons donc ordonner les représentants des classes modulo $\Re_{(k)}$, et si $|P_N| = q^\gamma$, il existe ℓ entier, $1 \leq \ell \leq q^k$, tel que si $R_1 < R_2 < \ldots < R_{q^k}$ désignent les représentants de degré γ,

$$S_N = \sum_{n=1}^{N} e_o(P_n \beta) = \sum_{|P| \leq q^{\gamma-1}} e_o(P\beta) + \sum_{i=1}^{\ell-1} \sum_{P \,\Re_{(k)}\, R_i} e_o(P\beta)$$

$$+ 0\Big(\sum_{P \,\Re_{(k)}\, R_\ell} 1 \Big).$$

Il suffit alors de montrer que

$$\sum_{|P| \leq q^{\gamma-1}} e_o(P\beta) = 0\,(\pi(\gamma-1) + \pi(\gamma-2) + \ldots + \pi(1)),$$

$$S_N(R_i) = \sum_{P \,\Re_{(k)}\, R_i} e_o(P\beta) = 0(\pi(\gamma) q^{-k}) ,$$

et de prendre k tel que

$$\pi(R_\ell , 1 , 1 , k) = 0(\pi(\gamma)).$$

Pour vérifier la dernière propriété, nous prenons $k = [\gamma^\varepsilon]$, donc

$$|\pi(R_\ell , 1 , 1 , k) - \pi(\gamma) \times q^{-[\gamma^\varepsilon]}| \leq c\, q^{\gamma - \sqrt{\gamma}}$$

d'après le théorème 2. Ce choix de k convient, car $\pi(\gamma)$ est équivalent à $\gamma^{-1} q^\gamma$.

En partageant les polynômes de degré $\gamma-1$, $\gamma-2$, ... en classes d'équivalence modulo $\mathfrak{R}_{(k)}$, on se ramène à n'étudier que des sommes du type $S_N(R_i)$.

Posons $\beta = \frac{A}{Q} + \frac{\theta}{QT}$ où $|T| = q^{\tau}$ et $|\theta| < 1$. Alors, si $P \mathfrak{R}_{(k)} R_i$, nous avons

$$P_\beta = \frac{PA}{Q} + \frac{R_i\theta}{QT} + \frac{(P-R_i)\theta}{QT} \quad \text{et} \quad \frac{(P-R_i)\theta}{QT} \in \mathfrak{P}^2,$$

donc

$$S_N(R_i) = e_o\left(\frac{R_i\theta}{QT}\right) \sum_{P \mathfrak{R}_{(k)} R_i} e_o\left(\frac{PA}{Q}\right),$$

et

$$S_N(R_i) = e_o\left(\frac{R_i\theta}{QT}\right) \sum_{\substack{(L,Q)=1 \\ |L|<|Q|}} \sum_{\substack{P \mathfrak{R}_{(k)} R_i \\ Q \text{ divise } P-L}} e_o\left(\frac{AL}{Q}\right),$$

et, puisque $\left| e_o\left(\frac{R_i\theta}{QT}\right) \right| = 1$, il vient

$$|S_N(R_i)| = \left| \sum_{\substack{(L,Q)=1 \\ |L|<|Q|}} \pi(R_i, Q, L, k)\, e_o\left(\frac{AL}{Q}\right) \right|.$$

En utilisant le théorème 2,

$$|S_N(R_i)| \le \frac{\pi(\gamma)}{q^k \Phi(Q)} \left| \sum_{\substack{(L,Q)=1 \\ |L|<|Q|}} e_o\left(\frac{AL}{Q}\right) \right| + c\Phi(Q)\, q^{\gamma-\sqrt{\gamma}}.$$

Sachant que

$$\sum_{\substack{(L,Q)=1 \\ |L|<|Q|}} e_o\left(\frac{AL}{Q}\right) = \mu(Q),$$

où μ est la fonction de Möbius (et donc $|\mu(Q)| \le 1$) et que

$$|Q|^{1/2} \le |\Phi(Q)| \le |Q|,$$

on voit que

$$S_N(R_i) = O(\pi(\gamma)\, q^{-k}).$$

5. - INTRODUCTION DES FONCTIONS $L(.\ ,\ \chi)$

Soit $\mathfrak{R}$ une relation d'équivalence sur $\mathfrak{M}$, telle que le quotient $\mathfrak{M}/\mathfrak{R}$ soit un demi-groupe et que le groupe $\mathfrak{G}(\mathfrak{R})$ des éléments inversibles soit fini d'ordre $g(\mathfrak{R})$. Soit $\hat{\mathfrak{G}}$ le dual de $\mathfrak{G}(\mathfrak{R})$, et on définit [5] les caractères sur $\mathfrak{M}$.

Définition 4. Soit $x \in \hat{\mathfrak{G}}$, on définit l'homomorphisme χ de $\mathfrak{M}$ dans les nombres complexes de module 1 par

$$\chi(G) = x(\overline{G}) \quad \text{si la classe } \overline{G} \text{ est inversible,}$$
$$= 0 \quad \text{sinon.}$$

Soient $\chi_0 = 1, \chi_1, \ldots, \chi_{g-1}$ les caractères relatifs à $\mathfrak{R}$. On étend à $\mathfrak{M}$ la relation $\mathfrak{R}_{(k)}$:

Si A et B sont deux éléments de $\mathfrak{M}$ de degrés respectifs n et m, on pose

$$A\ \mathfrak{R}_{(k)}\ B \Leftrightarrow |x^m A - x^n B| < q^{m+n-k}.$$

Alors $g(\mathfrak{R}_{(k)}) = q^k$. Si $H \in \mathfrak{M}$, soit $\mathfrak{R}_H$ la relation

$$A\ \mathfrak{R}_H\ B \Leftrightarrow H \text{ divise } A - B.$$

Alors $\mathfrak{G}(\mathfrak{R}_H) = \Phi(H)$.

Nous définissons la relation $\mathfrak{R}_{(k)H} = \mathfrak{R}_{(k)} \cap \mathfrak{R}_H$.

Alors, si $(H, L) = 1$, $\overline{L}$ est inversible dans $\mathfrak{G}(\mathfrak{R}_{(k)H})$.

PROPOSITION 3. *Si $\chi_0, \chi_1, \ldots, \chi_{g-1}$ avec $g = g(\mathfrak{R}_{(k)H}) = q^k \Phi(H)$ sont les caractères relatifs à $\mathfrak{R}_{(k)H}$, nous avons*

$$\pi(R, H, L, k) = \sum_{|P| = q^\gamma} \frac{1}{g} \sum_{i=0}^{g-1} \overline{\chi}_i(L)\, \chi_i(P).$$

En effet, si P n'est pas inversible, $\chi_i(P) = 0$, et si $\overline{P}$ est inversible,

$$\frac{1}{g} \sum_{i=0}^{g-1} \overline{\chi}_i(L)\, \chi_i(P) = \frac{1}{g} \sum_{i=0}^{g-1} x_i(\overline{P} \cdot \overline{L}^{-1}),$$

et cette expression est l'intégrale de Haar sur $\hat{\mathfrak{G}}$ du caractère $x_i \to x_i(\overline{P} . \overline{L}^{-1})$ de $\hat{\mathfrak{G}}$. Cette intégrale est égale à 1 si Q divise P-L, et à 0 sinon. En posant,

$$\pi(\gamma , \chi_i) = \sum_{|P| = q^\gamma} \chi_i(P) ,$$

nous obtenons

$$\pi(R , H , L , k) = \frac{1}{g} \sum_{i=0}^{g-1} \overline{\chi}_i(L)\, \pi(\gamma , \chi_i) .$$

On démontre que

$$\pi(\gamma) - \pi(\gamma , \chi_o) = \sum_{\substack{P \\ P \text{ non inversible}}} 1 \leq 2g ,$$

et donc

$$\left| \pi(R , H , L , k) - \frac{\pi(\gamma)}{q^k \Phi(H)} \right| \leq 2 + \frac{1}{g} \sum_{i=1}^{g-1} |\pi(\gamma , \chi_i)| .$$

Il suffit alors de démontrer que, pour $1 \leq i \leq g-1$, $|\pi(\gamma, \chi_i)| \leq c(u) q^{\gamma - \sqrt{\gamma}}$.

Nous posons $L(s , \chi) = \sum_{G \in \mathfrak{M}} \frac{\chi(G)}{|G|^s}$ $\qquad s = \sigma + it$ et $\sigma > 1$,

et nous obtenons, si $a > 1$,

$$\pi(\gamma, \chi_i) = \frac{-1}{2\gamma\pi i \log^2 q} \int_{a-i\infty}^{a+i\infty} \frac{q^{(\gamma+1)s} - q^{\gamma s}}{s^2} \frac{L'(s , \chi)}{L(s , \chi)}\, ds + 0(\gamma\, q^{\gamma/2}) ,$$

ce qui ramène la démonstration du théorème 2 à l'étude des régions de $\underset{\sim}{C}$ où les fonctions $L(. , \chi)$ ne s'annulent pas.

6. - AUTRES RESULTATS

Nous démontrons aussi le théorème suivant :

THEOREME 3. Soit f un polynôme à coefficients dans $\mathfrak{F}_o$, de degré k $(2 \leq k < p)$,

$$f(X) = \alpha_o + \alpha_1 X + \ldots + \alpha_k X^k .$$

S'il existe un entier s $(2 \leq s \leq k)$ tel que $\alpha_s \notin \mathfrak{F}$ et tel que, si $(A_i)_{i \geq 1}$ désigne le développement en fraction continue de α_s, la suite A_i soit bornée, alors la suite $(f(P_n))_{n \geq 1}$ est équirépartie modulo 1 dans $\mathfrak{F}_o$.

Nous avons démontré depuis, le théorème

THEOREME 4. Soit k un entier $(2 \leq k < p)$, alors la suite $(\alpha P_n^k)_{n \geq 1}$ est équirépartie modulo 1 dans $\mathfrak{F}_o$ si et seulement si $\alpha \notin \mathfrak{F}$.

Si 0 est le plus petit élément de F_q dans la définition 2, A. Dijksma a démontré le théorème [3]

THEOREME 5. Soit $(G_n)_{n \geq 1}$ la suite des polynômes de $F_q[x]$ ordonnée selon l'ordre Ω. Soit f un polynôme de degré k $(1 \leq k < p)$

$$f(X) = \alpha_o + \alpha_1 X + \ldots + \alpha_k X^k \qquad \alpha_i \in \mathfrak{F}_o .$$

Alors la suite $(f(G_n))_{n \geq 1}$ est équirépartie modulo 1 dans $\mathfrak{F}_o$ si et seulement si l'un des α_i $(1 \leq i \leq k)$ est un élément de $\mathfrak{F}_o - \mathfrak{F}$.

Remarque. Nous ne pouvons pas supprimer la condition $k < p$ dans les théorèmes 3, 4 et 5 ; en effet, il existe des éléments α de $\mathfrak{F}_o - \mathfrak{F}$ tels que la suite $(\alpha H_n^p)_{n \geq 1}$ ne soit pas équirépartie modulo 1 quelle que soit la suite (H_n) de polynômes de $F_q[x]$.

Par exemple [3], $\alpha = \sum_{j=1}^{\infty} x^{-p^j}$ qui est algèbrique de degré p. En effet αH_n^p est une série formelle $\sum_{n}^{+\infty} a_n x^{-n}$ telle que $a_n = 0$ si $n \not\equiv 0$ mod p donc $a_1 = 0 \Rightarrow e_o(\alpha H_n^p) = 1^{-\infty}$ et $\frac{1}{N} \sum_{n=1}^{N} e_o(\alpha H_n^p) = 1$.

Dans le corps des réels I. M. Vinogradov [8] a démontré le théorème

THEOREME 6. Soit f un polynôme de degré $k \geq 2$ à coefficients réels tel qu'il existe un entier s $(k \geq s \geq 2)$ et un nombre réel $\chi > 0$ tels que

$$f(x) = \alpha_k x^k + \ldots + \alpha_1 x + \alpha_o$$

et pour $N \geq N_o$

$$\alpha_s = \frac{a}{q} + \frac{\theta}{q\tau} \qquad (a, q) = 1 \qquad |\theta| < 1$$

$$0 < q \leq \tau \ , \quad \tau = N^{0,5s} \quad \text{et} \quad N^{\chi} \leq q \leq \tau$$

alors la suite (f(p)) est équirépartie modulo 1 .

COROLLAIRE. Si f a un coefficient α_s $(k \geq s \geq 2)$ non rationnel dont le développement en fraction continue $\alpha_s = (a_o, a_1, \ldots, a_n, \ldots)$ est tel que la suite des $(a_i)_{i \geq 0}$ soit bornée, alors la suite (f(p)) est équirépartie modulo 1.

Contrairement à ce qu'ont affirmé Cigler et Helmberg dans [2] et Erdös dans [9], le théorème 6 n'implique pas le résultat suivant :

Si f est un polynôme de degré ≥ 1 à coefficients réels, la suite (f(p)) est équirépartie modulo 1 si le coefficient du monôme de plus haut degré de f est irrationnel.

-:-:-:-

BIBLIOGRAPHIE

[1] CARLITZ L. - Diophantine approximation in fields of characteristic p, Trans. Amer. Math. Soc. t. 72, 1952, p. 187-207.

[2] CIGLER J. and HELMBERG G. - Newer Entwicklungen in der theorie der Gleichverteilung. Jahr Deutsch Math. Vereinig, t. 64, 1962, p. 1-50.

[3] DIJKSMA A. - Uniform distribution of polynomials over GF {q, x} in GF[q, x]. Part. I, Nederl. Akad. Wetensch Proc. Ser. A, 72, 4, 1969, p. 376-383. - Part. II, Nederl. Akad. Wetensch. Ser. A, 73, 3, 1970, p. 187-195.

[4] ESTERMANN T. - Introduction to modern prime number theory. Cambridge Tracts in Mathematics and mathematical physics, 41.

[5] HAYES D. R. - The distribution of irreducibles in GF[q,x] . Trans. Amer. math. Soc. t. 117, 1965, p. 101-127.

[6] MATHAN (Bernard de). - Approximations diophantiennes dans un corps local. Bull. Soc. math. France, mémoire 21, 93 p., 1970 (Thèse Sc. math. Caen, 1968).

[7] VINOGRADOV I. M. - The method of trigonometrical sums in the theory of numbers. Translated from Russian. London, Interscience Publishers, 1954.

[8] VINOGRADOV I. M. - Sur l'évaluation de sommes trigonométriques avec des nombres premiers. Izv. Akad. Nank. S S S R Ser. Math., 1948-12, p. 225-248.

[9] Asymptotic distribution modulo 1. Nuffic international summer session in science. Nijenrode lectures P. Noordhoff. Groningen, 1962.

-:-:-:-

Georges RHIN
14, rue Leroy
14 - CAEN