33. *Sommes de Gauss modulo p^α. I*

Par J.-L. MAUCLAIRE
C.N.R.S. et Université Waseda

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1983)

1. Soit p un nombre premier, α un entier >1, χ un caractère primitif modulo p^α. On définit la somme de Gauss $\tau(\chi)$ mod p^α par

$$\tau(\chi)=\sum_{x\in(\boldsymbol{Z}/p^\alpha\boldsymbol{Z})^\times}\chi(x)\exp\left(2i\pi\frac{x}{p^\alpha}\right).$$

On se propose de donner ici le résultat suivant:

Théorème 1. *p étant un nombre premier impair, et α un entier >1, χ un caractère primitif modulo p^α, alors*

1. *Si $\alpha=2k$, on pose $\chi(1+p^k)=\exp(-2i\pi(h/p^k))$, où $0<h<p^k$ (et $(h,p)=1$ puisque χ est primitif). Alors, pour tout $L\equiv h \bmod p^k$, on a*

$$\tau(\chi)=p^k\chi(L)\exp\left(2i\pi\frac{L}{p^{2k}}\right).$$

2. *Si $\alpha=2k+1$, on détermine de façon unique un entier h par les relations*

$$\chi(1+p^k+2^*p^{2k})=\exp\left(-2i\pi\frac{h}{p^{k+1}}\right),$$

$0\leq h\leq p^{k+1}$ (et $(h,p)=1$ car χ est primitif), où $2^*2\equiv 1$ modulo p. Alors, pour tout $L\equiv h \bmod p^{k+1}$, on a

$$\tau(\chi)=p^{k+1/2}\exp\left(2i\pi\frac{L}{p^{2k+1}}\right)\cdot\chi(L)\cdot\varepsilon_p\left(\frac{2L}{p}\right)$$

où $\varepsilon_p=1$ si $p\equiv 1$ (4), i si $p\equiv 3 \bmod 4$, et $(\cdot/p)$ est le symbole de Legendre.

On peut donner une formulation qui condense le Théorème 1 de la façon suivante:

Théorème 1. bis. *Soient p premier impair, $k>1$, χ un caractère primitif modulo p^k, Z_p^* le groupe multiplicatif des unités de Z_p, Γ_{p-1} le sous-groupe cyclique d'ordre $p-1$ de Z_p^*, ce qui fait que χ, considéré comme caractère sur Z_p^* trivial sur $(1+p^kZ_p)$ s'identifie pour $\varepsilon\in\Gamma_{p-1}$, $u\in Z_p$ à $\chi(\varepsilon(1+pu))=\psi(\varepsilon)\exp(-2i\pi(h/p^k))\log(1+pu)$, où $(h,p)=1$, h fixé, $0<h<p^{k-1}$, ψ est un caractère* mod p *fixé,* $\log(\cdot)$ *est le logarithme p-adique usuel. Comme $h\in Z_p$, h s'écrit:*

$$h=\eta(1+p\tilde{h}),\quad \eta\in\Gamma_{p-1},\quad \eta\equiv h \bmod p,\quad \tilde{h}\in Z_p.$$

Alors on a pour la somme de Gauss $\tau(\chi)$ mod p^k

$$\tau(\chi)=p^{k/2}\cdot\left(\frac{2h}{p}\right)^k\cdot\varepsilon_p^{k^2}\cdot\psi(h)\cdot\exp\left(-2i\pi\frac{h}{p^k}\right)\log\left(\frac{1+p\tilde{h}}{e_p}\right),$$

où $(\cdot/p)$ *est le symbole de Legendre,* $\log e_p=1$, $\varepsilon_p=1$ *si* $p\equiv 1 \bmod 4$, *i si* $p\equiv 3 \bmod 4$.

2. Démonstration pour le cas de $Z/p^{2k}Z$. Ici, p sera un nombre premier impair ou 2. On remarque que tout élément x de $(Z/p^{2k}Z)^\times$ s'écrit modulo p^{2k} sous la forme

$$x=\theta\cdot y,$$

où $(\theta,p)=1$, $0\leq\theta\leq p^k$, et $y=1+p^km$, $0\leq m\leq p^k-1$, de façon unique. On a donc, en posant $G=(Z/p^{2k}Z)^\times$, $G'=(Z/p^kZ)^\times$,

$$\tau(\chi)=\sum_{x\in G}\chi(x)\exp\left(2i\pi\frac{x}{p^{2k}}\right)=\sum_{x\in G'}\sum_{m=0}^{p^k-1}\chi(\theta(1+p^km))\exp\left(2i\pi\frac{(1+p^km)}{p^{2k}}\right)$$

$$=\sum_{x\in G'}\chi(\theta)\exp\left(2i\pi\frac{\theta}{p^{2k}}\right)\cdot\sum_{m=0}^{p^k-1}\chi(1+p^km)\exp\left(2i\pi\frac{p^km\theta}{p^{2k}}\right).$$

Or, $\{y=1+p^km,\ 0\leq m\leq p^k-1\}$, muni de la loi interne $\times$, est un sous-groupe multiplicatif de G isomorphe à Z/p^kZ ; on remarque que

$$1+p^km=(1+p^k)m,$$

et en posant

$$\chi(1+p^k)=\exp\left(-2i\pi\frac{h}{p^k}\right),$$

on obtient

$$\sum_{m=0}^{p^k-1}\chi(1+p^km)\exp\left(2i\pi\frac{p^km\theta}{p^{2k}}\right)=\begin{cases}p^k & \text{si}\quad \theta=h\\ 0 & \text{sinon}\end{cases},$$

d'où $\tau(\chi)=p^k\chi(h)\exp 2i\pi(h/p^{2k})$.

Remarques. 1) Si $(h,p)>1$, la formule est encore vraie et correspond à un caractère χ non primitif.

2) Si $L\equiv h \bmod p^k$, alors $L=h\cdot(1+p^kl)$ et

$$\chi(L)\exp\left(2i\pi\frac{L}{p^{2k}}\right)=\chi(h)\chi(1+p^kl)\exp\left(2i\pi\frac{h+p^khl}{p^{2k}}\right)$$

$$=\chi(h)\cdot\exp\left(-2i\pi\frac{h}{p^k}l\right)\exp\left(2i\pi\frac{h}{p^{2k}}\right)\exp\left(2i\pi\frac{h}{p^k}l\right)=\tau(\chi),$$

d'où le 1) du Théorème 1.

3. Démonstration pour le cas de $Z/p^{2k+1}Z$, p impair. On remarque que tout x de $(Z/p^{2k+1}Z)^\times$ s'écrit de façon unique sous la forme $x=\theta\cdot(1+p^km)$, où $0\leq\theta\leq p^k$, $(\theta,p)=1$ et $0\leq m\leq p^{k+1}-1$.

On considère le sous-groupe Γ_{k+1} de $(Z/p^{2k+1}Z)^\times$ dont les éléments s'écrivent sous la forme $1+p^km$, $0\leq m\leq p^{k+1}-1$. On détermine son dual $\hat{\Gamma}_{k+1}$ comme suit :

$$\psi\in\hat{\Gamma}_{k+1}\quad\text{si}\quad\psi((1+p^km)\cdot(1+p^kn))=\psi(1+p^km)\cdot\psi(1+p^kn).$$

On vérifie que l'on a

$$\psi(1+p^km)=\psi_h(1+p^km)=\exp\left(2i\pi\frac{h}{p^{2k+1}}(-p^km+p^{2k}2^*m^2)\right),$$

où $0\leq h\leq p^{k+1}-1$, et $2^*2\equiv 1 \bmod p$. En effet :

Si $h\not\equiv l \bmod p^{k+1}$, alors $\psi_h\neq\psi_l$.

En outre:

$$\psi_h(1+p^h m)\psi_h(1+p^k n) = \exp 2i\pi\frac{h}{p^{2k+1}}(-p^k m+p^{2k}2^*m^2-p^k n+p^{2k}2^*n^2)$$
$$= \exp 2i\pi\frac{h}{p^{2k+1}}(-(p^k(m+n)+p^{2k}mn) +2^*p^{2k}(m+n)^2)$$
$$= \exp 2i\pi\frac{h}{p^{2k+1}}(-(p^k(m+n)+p^k mn)) +2^*p^{2k}((m+n)+p^k mn)^2)$$
$$= \psi_h((1+p^k m)\cdot(1+p^k n)).$$

Donc, $\{\psi_h, 0\leq h\leq p^{k+1}-1\}=\hat{\Gamma}_{k+1}$, puisque chaque ψ_h est un caractère et que le nombre de tels ψ_h distincts est le cardinal de Γ_{k+1}.

On a alors, en posant $G=(\boldsymbol{Z}/p^{2k+1}\boldsymbol{Z})^\times$, $G'=(\boldsymbol{Z}/p^k\boldsymbol{Z})^\times$,

$$\tau(\chi)=\sum_{x\in G}\chi(x)\exp\left(2i\pi\frac{x}{p^{2k+1}}\right)$$
$$=\sum_{\theta\in G'}\sum_{0\leq m\leq p^{k+1}-1}\chi(\theta(1+p^k m))\exp\left(2i\pi\frac{\theta(1+p^k m)}{p^{2k+1}}\right)$$
$$=\sum_{\theta\in G'}\chi(\theta)\exp\left(2i\pi\frac{\theta}{p^{2k+1}}\right)\cdot\sum_{0\leq m\leq p^{k+1}-1}\chi(1+p^k m)\exp\left(2i\pi\frac{\theta p^k m}{p^{2k+1}}\right).$$

Or χ, restreint à Γ_{k+1}, est un élément de $\hat{\Gamma}_{k+1}$. Il existe donc h tel que $\chi=\psi_h$. On a donc:

$$\sum_{0\leq m\leq p^{k+1}-1}\chi(1+p^k m)\exp\left(2i\pi\frac{\theta p^k m}{p^{2k+1}}\right)$$
$$=\sum_{0\leq m\leq p^{k+1}-1}\exp 2i\pi\left(\frac{h}{p^{2k+1}}(-p^k m+p^{2k}m^2 2^*)+\frac{1}{p^{2k+1}}\theta p^k m\right)$$
$$=\sum_{r=0}^{p-1}\sum_{v=0}^{p^k-1}\exp 2i\pi\left(\frac{1}{p^{k+1}}(\theta-h)(r+pv)+2^*\frac{r^2 h}{p}\right)$$
$$=\left(\sum_{r=0}^{p-1}\exp 2i\pi\left(\frac{1}{p^{k+1}}(\theta-h)r+\frac{2^*r^2h}{p}\right)\right)\left(\sum_{v=0}^{p^k-1}2i\pi\frac{(\theta-h)v}{p^k}\right).$$

Mais

$$\sum_{v=0}^{p^k-1}\exp\left(2i\pi\frac{\theta-h}{p^k}v\right)=\begin{cases}p^k & \text{si } \theta-h\equiv 0 \bmod p^k\\ 0 & \text{sinon.}\end{cases}$$

Comme h vérifie $0\leq h\leq p^{k+1}-1$, et que θ vérifie $0\leq\theta\leq p^k-1$, on a une seule valeur de θ vérifiant $\theta-h\equiv 0 \bmod p^k$ (pourvu que $h\not\equiv 0 \bmod p$, ce qui signifie que χ est primitif). On écrit $\theta=h+up^k$, où $0\leq -u<p$, et notre somme devient, en posant $h^{-1}h\equiv 1 \bmod p$,

$$\sum_{r=0}^{p-1}\exp 2i\pi\left(\frac{up^k r}{p^{k+1}}+\frac{2^*r^2h}{p}\right)p^k=p^k\sum_{r=0}^{p-1}\exp\left(\frac{2i\pi}{p}2^*h((r+uh^{-1})^2-(uh^{-1})^2)\right)$$
$$=p^k\exp\left(-2i\pi\frac{2^*u^2h^{-1}}{p}\right)\cdot\sum_{x=0}^{p-1}\exp\left(2i\pi\frac{2^*hx^2}{p}\right),$$

d'où

$$\tau(\chi)=\chi(h+up^k)\cdot\exp\left(-2i\pi\frac{2^*u^2h^{-1}}{p}\right)\cdot\sum_{x=0}^{p-1}\exp\left(2i\pi\frac{2^*hx^2}{p}\right)$$
$$\cdot\exp\left(2i\pi\frac{h+up^k}{p^{2k+1}}\right)\cdot p^k.$$

On définit $\tilde{h}$ par $h\tilde{h}\equiv 1 \bmod p^{k+1}$, et l'on voit que

$$\chi(h+up^k)=\chi(h(1+\tilde{h}up^k))=\chi(h)\psi_h(1+\tilde{h}up^k)$$
$$=\chi(h)\exp 2i\pi\frac{h}{p^{2k+1}}\left(-\tilde{h}up^k+2^*\frac{\tilde{h}^2u^2p^{2k}}{p}\right)$$
$$=\chi(h)\exp 2i\pi\left(-\frac{u}{p^{k+1}}+\frac{h^{-1}u^2 2^*}{p}\right),$$

d'où

$$\tau(\chi)=p^k\chi(h)\exp\left(2i\pi\frac{h}{p^{2k+1}}\right)\sum_{x=0}^{p-1}\exp\left(2i\pi\frac{2^*hx^2}{p}\right).$$

D'où, en utilisant la valeur connue de la "somme de Gauss" historique $\varepsilon_p\cdot p^{1/2}$, on a

$$\tau(\chi)=p^{k+(1/2)}\chi(h)\exp\left(2i\pi\frac{h}{p^{2k+1}}\right)\varepsilon_p\left(\frac{2h}{p}\right)$$

où $(\cdot/p)$ est le symbole de Legendre.

Or, si $L\equiv h \bmod p^{k+1}$, on a $L=h(1+p^{k+1}l)$ et

$$\chi(L)\exp\left(2i\pi\frac{L}{p^{2k+1}}\right)=\chi(h)\chi(1+p^{k+1}l)\exp\left(2i\pi\frac{h}{p^{2k+1}}\right)\exp\left(2i\pi\frac{hl}{p^k}\right)$$
$$=\chi(h)\exp\left(-2i\pi\frac{l}{p^k}\right)\exp\left(2i\pi\frac{h}{p^{2k+1}}\right)\exp\left(2i\pi\frac{hl}{p^k}\right)$$
$$=\chi(h)\exp\left(-2i\pi\frac{h}{p^{2k+1}}\right),$$

d'où le 2) du Théorème 1, car

$$\chi(1+p^k+p^{2k}2^*)=\exp\left(-2i\pi\frac{h}{p^{k+1}}\right).$$

Addendum. Après présentation de cette note, l'auteur a été informé du fait que les sommes de Gauss modulo p^α, p impair, $\alpha>1$, avaient déjà été déterminées par R. Odoni: On Gauss sums mod $p^n\geq 2$, Bull. London Math. Soc. **5** (1973), 325–327. Les méthodes suivies ici ainsi que la formulation des résultats sont cependant entièrement différentes.