SUJETS D'ARITHMÉTIQUE

Cours Maitrise Printemps 2008

Vadim Schechtman

Table des matières

Zeittafel

Pierre de FERMAT (1601 - 1665)

Leonard EULER (1707 - 1783)

Adrien Marie LEGENDRE (1752 - 1833)

Carl Friedrich GAUSS (1777 - 1855)

Pafnuty Lvovich CHEBYSHEV (1821 - 1894)

Évariste GALOIS (1811 - 1832)

Bernhard RIEMANN (1826 - 1866)

§1. Corps finis

1.1. *Théorème de Bezout.* Deux nombres entiers a, b sont premiers l'un à l'autre si et seulement si il existent des nombres entiers c, d tels que $ac + bd = 1$.

1.2. *Théorème.* Soit $p \in \mathbb{Z}$ un nombre premier. Alors $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ est un corps.

Preuve: exercice. Utiliser soit le théorème de Bezout, soit le lemme suivant.

1.3. *Lemme.* Un anneau commutatif fini est un corps ssi il est intègre (c'est-á-dire, ne contient pas de diviseurs de zéro).

(a) *Racines primitives*

1.4. Considérons le groupe multiplicatif $\mathbb{F}_p^*$. Celui-ci est un groupe abélien d'ordre $p-1$, d'où $a^{p-1} = 1$ pour chaque $a \in \mathbb{F}_p^*$.

En d'autres termes, pour chaque $b \in \mathbb{Z}$ premier à p, on a $b^{p-1} \equiv 1(p)$ (le "petit" théorème de Fermat).

Exemples d'applications.

1.4.1. *Exercice.* (a) Montrer que si $2^n - 1$ est premier alors n est premier.

(b) Si un premier p divise $2^{37} - 1$ alors p est de la forme $74k + 1$.

En effet, on cherche un premier p tel que $2^{37} \equiv 1(p)$. D'abord p est impair. D'un autre côté, $2^{p-1} \equiv 1(p)$, d'où $37|(p-1)$. Comme $2|(p-1)$, on a $74|(p-1)$, donc p est de la forme $74k + 1$.

(c) Donner des exemples de nombres premiers de la forme $74k + 1$.

($p = 149, 223$)

(d) Montrer que $223 \mid 2^{37} - 1$. Donc, $2^{37} - 1$ n'est pas premier.

En effet, on calcule: $2^8 \equiv 33 \pmod{223}$; $2^{16} \equiv -26 \pmod{223}$; $2^{32} \equiv 7 \pmod{223}$, d'où $2^{37} \equiv 7 \cdot 32 = 224 \equiv 1 \pmod{223}$.

1.4.2. *Exercice.* Nombres premiers de Fermat. (a) Montrer que si $2^m + 1$ est premier alors $m = 2^n$.

(b) Désignons $p_n = 2^{2^n} + 1$. Montrer que p_n est premier pour $n = 1, 2, 3, 4$.

(c) (Euler) Montrer que si un premier p divise p_5 alors $p = 64k + 1$.

En effet, ci c'est le cas, alors $2^{32} \equiv -1 \pmod{p}$, donc 2 est d'ordre 64 dans $\mathbb{F}_p^*$. Il s'en suit que $64|(p-1)$.

(d) (Euler) Montrer que $641 \mid p_5$, donc p_5 n'est pas premier.

1.5. Considérons le groupe $\mathbb{F}_5^*$. On a $\mathrm{Card}(\mathbb{F}_5^*)$, donc a priori ce groupe peut être isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Essayons le nombre 2: les restes 2^a modulo 5 pour $a = 1, 2, 3, 4$ sont $2, 4, 3, 1$, donc $\mathbb{F}_5^*$ est cyclique, avec un générateur $\bar{2} = 2 \bmod(5)$.

Cela est un phénomène général.

1.6. *Théorème* (Euler) Soient F un corps, $A \subset F^*$ un sous-groupe fini. Alors A est cyclique.

1.6.1. *Lemme.* Soient A un groupe abélien, $x, y \in A$ des éléments d'ordres a, b, tels que $(a, b) = 1$. Alors xy a l'ordre ab.

En effet, si B (resp. C) est un sous-groupe engendré par x (resp. y) alors l'ordre de $B \cap C$ divise l'ordres de B et de C, donc $B \cap C = \{1\}$. Si $(xy)^c = 1$ alors $x^c, y^c \in B \cap C$ donc $x^c = y^c = 1$, donc $a|c$ et $b|c$. Il s'en suit que $(ab)|c$, d'où l'assertion.

1.6.2. *Lemme.* Soient A un groupe abélien, $x, y \in A$ des éléments d'ordres a, b. Alors il existe un $z \in A$ d'ordre $c := \mathrm{ppcm}(a, b)$.

En effet, on peut trouver des décompositions $a = a'a''$, $b = b'b''$ avec $(a', b') = 1$ et $c = a'b'$ (vérifier!). Alors $x^{a''}$ (resp. $y^{b''}$ est de l'ordre a' (resp. b'), donc par le lemme précédent $z = x^{a''}y^{b''}$ est de l'ordre c.

1.6.3. *Corollaire.* Soit A un abélien groupe fini, d le maximal des ordres d'éléments de A. Alors l'ordre de chaque élément de A divise d, donc $x^d = 1$ pour chaque $x \in C$.

Revenons à notre théorème. Soit d le maximal des ordres d'éléments de A. D'après le corollaire précédent, $x^d = 1$ pour chaque $x \in A$. D'autre part, l'équation $t^d - 1 = 0$ ne peut pas avoir plus que d racines dans F, d'où $d = \mathrm{Card}(A)$, donc A est cyclique.

(b)

1.7. *Théorème* (Fermat) Soit F un corps de caractéristique $p > 0$.

Alors $(x + y)^p = x^p + y^p$ pour tous $x, y \in F$.

En effet,

$$(x + y)^p = \sum_{i=0}^{p} \binom{i}{p} x^i y^{p-i}$$

Mais

$$\binom{i}{p} \equiv 0(p)$$

pour $1 \leq i \leq p$ (vérifier!), d'où l'assertion.

Il s'en suit que l'application $\sigma : \ F \longrightarrow F$, $\sigma(x) = x^p$ est un morphisme de corps, necessairement injectif; de même pour ses itérés σ^f, $\sigma^f(x) = x^{p^f}$, $f \geq 1$.

Le sous-corps fixé $F_0 = \{x \in F \mid \sigma(x) = x\} \subset F$ contient $\mathbb{F}_p$ par le petit Fermat. Puisque l'équation $t^p - t = 0$ ne peut avoir plus que p racines dans F, Il s'en suit que $F_0 = \mathbb{F}_p$.

1.8. Soit F un corps fini. Sa caractéristique est necessairement un nombre premier p; on a $\mathbb{F}_p \subset F$. Si le degré $[F : \mathbb{F}_p]$ est égale à f, alors F est un espace vectoriel sur $\mathbb{F}_p$ de dimension f, donc $\mathrm{Card}(F) = p^f$.

Réciproquement, pour chaque $f \in \mathbb{Z},\ f \geq 1$, on peut construire un corps F qui ait $q = p^f$ éléments. Pour le faire, plongeons $\mathbb{F}_p$ dans un corps Ω algébriquement clos. Considérons le morphisme $\sigma^f :\ \Omega \longrightarrow \Omega$, $\sigma^f(x) = x^q$. Il est surjectif car Ω est algébriquement clos, donc σ^f est un automorphisme de Ω.

Considérons son sous-corps fixé $F = \{x \in \Omega \mid x^q = x\} \subset \Omega$; il coïncide avec l'ensemble de racines du polynôme $f(t) = t^q - t$ dans Ω.

1.9. *Lemme.* Toutes les racines de $f(t)$ sont distincts.

En effet, si $\alpha \in \Omega$ est une racine multiple de $f(t)$ alors $f'(\alpha) = 0$ (démontrer!). D'autre part,

$$f'(t) = qt^{q-1} - 1 = -1$$

n'a pas de racines, donc $f(t)$ n'a pas de racines multiples, cqfd.

Ce lemme implique que $\mathrm{Card}(F) = q$.

Soit $F' \subset \Omega$ un sous-corps à q éléments. On a $\mathrm{Card}(F'^*) = q - 1$, donc $x^{q-1} = 1$ pour chaque $x \in F',\ x \neq 0$, donc $x^q = x$ pour chaque $x \in F'$. Il s'en suit que $F' \subset F$, donc $F' = F$.

Enfin, soit K un corps arbitraire à q éléments. Celui-ci est une extension algébrique de $\mathbb{F}_p$ (de degré f). Par la propriété générale, il existe un plongement $\phi :\ K \hookrightarrow \Omega$ prolongeant l'inclusion $\mathbb{F}_p \subset \Omega$, puisque Ω est algébriquement clos. Son image $\phi(K)$ est un sous-corps à q éléments, donc $\phi(K) = F$. Donc $\phi :\ K \xrightarrow{\sim} F$.

On a prouvé

1.10. *Théorème.* Pour chaque nombre premier p et $f \in \mathbb{Z},\ f \geq 1$ il existe un corps à $q = p^f$ éléments. Ce corps est unique à isomorphisme près.

1.11. *Exercice.* Montrer que $\mathbb{F}_q \subset \mathbb{F}_{q'}$ ssi $q = p^f,\ q' = p^{f'}$ et $f | f'$ (cf. 1.22 (b)).

(c) *Fonction zeta de Riemann*

1.12. On définit:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

$s \in \mathbb{C}$.

Exemples. $\zeta(2) = \pi^2/6$ (Euler). Par contre, la série harmonique $\zeta(1)$ diverge (on a $\sum_{n=1}^{N} \frac{1}{n} \sim \log N$).

Exercice. Montrer que la série converge absolument et uniformement sur chaque compact dans le demi-plan $D = \{\Re(s) > 1\}$. Donc $\zeta(s)$ est une fonction holomorphe dans D.

1.13. *Exercice.* Montrer que

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1 - p^{-s}}$$

(produit d'Euler). En déduire, en posant $s = 1$, qu'il existe une infinité de nombres premiers.

(d) *Fonctions μ et ϕ*

1.14. Notation: $\mathbb{Z}_+ = \{n \in \mathbb{Z} \mid n > 0\}$. Un nombre $n \in \mathbb{Z},\ n > 1$, est dit *libre de carrés (square free)* si il est un produit de nombres premiers distincts.

On définit la *fonction de Moebius* $\mu :\ \mathbb{Z}_+ \longrightarrow \{-1, 0, 1\}$ par: $\mu(1) = 1$, pour $n > 1$ $\mu(n) = 0$ si n n'est pas libre de carrés et $\mu(n) = (-1)^r$ si $n = p_1 \cdot \ldots \cdot p_r$ avec p_i premiers et distincts.

1.15. *Exercice.* Montrer que

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

1.16. *Lemme.* Pour $n > 1$, on a $\sum_{d|n}\ \mu(d) = 0$.

En effet, si $n = \prod_{i=1}^{r}\ p_i^{a_i}$ alors

$$\sum_{d|n}\ \mu(d) = \sum_{(\epsilon_1,\ldots,\epsilon_r)\in\{0,1\}^r} \mu(p_1^{\epsilon_1} \cdot \ldots \cdot p_r^{\epsilon_r}) =$$

$$= \sum_{i=0}^{r} (-1)^i \binom{i}{r} = (1-1)^r = 0$$

1.17. Considérons l'ensemble $\mathbb{Z}_+^{\mathbb{C}} = \{f :\ \mathbb{Z}_+ \longrightarrow \mathbb{C}\}$. Introduisons sur cet ensemble une opération $\circ$ (*multiplication de Dirichlet*) par

$$f \circ g(n) = \sum_{d|n}\ f(d)g(n/d)$$

Elle est associative et commutative, avec l'unité $\mathbf{1}$, où $\mathbf{1}(1) = 1$, $\mathbf{1}(n) = 0$ pour $n > 1$ (vérifier!).

On définit $\nu :\ \mathbb{Z}_+ \longrightarrow \mathbb{C}$ par $\nu(n) = 1$ pour tous n. Évidemment,

$$f \circ \nu(n) = \sum_{d|n}\ f(d)$$

1.18. *Lemme.* $\mu \circ \nu = \mathbf{1}$

En effet, $\mu \circ \nu(1) = \mu(1)\nu(1) = 1$. D'autre part, pour $n > 1$

$$\mu \circ \nu(n) = \sum_{d|n}\ \mu(d) = 0,$$

d'après 1.16.

1.19. *Théorème* (formule d'inversion de Moebius) Pour $f \in \mathbb{Z}_+^{\mathbb{C}}$, soit $F(n) = \sum_{d|n}\ f(d)$. Alors

$$f(n) = \sum_{d|n}\ \mu(d)F(n/d)$$

Il s'agit de l'inversion d'une matrice triangulaire:

$$F(1) = f(1),$$

$$F(2) = f(1) + f(2),$$
$$F(3) = f(1) + f(3),$$
$$F(4) = f(1) + f(2) + f(4),$$

etc., d'où

$$f(1) = F(1),$$
$$f(2) = F(2) - F(1)$$
$$f(3) = F(3) - F(1),$$
$$f(4) = F(4) - F(2),$$

etc.

Démonstration du théorème: on a $F = f \circ \nu$, d'òu, par 1.18, $f = F \circ \mu$.

1.20. *Variante.* Soit $f : \mathbb{Z}_+ \longrightarrow G$ une application à valeurs dans un groupe abélien G, écrit multiplicativement. Si $F(n) = \prod_{d|n} f(d)$ alors

$$f(n) = \prod_{d|n} F(n/d)^{\mu(d)}$$

Preuve: exercice.

1.21. *Rémarque.* Dans tout le précédent, on peut aussi remplacer $\mathbb{Z}_+$ par l'ensemble de tous diviseurs d'un nombre fixé $N \in \mathbb{Z}_+$.

Fonction d'Euler.

1.22. Pour $n \in \mathbb{Z}_+$, on définit $\Phi(n) = \{a \in \mathbb{Z},\ 1 \leq a \leq n \mid (a, n) = 1\}$; $\phi(n) := \mathrm{Card}(\Phi(n))$.

Par exemple, $\phi(1) = 1$, $\phi(p) = p - 1$ si p est premier.

On peut identifier $\Phi(n)$ avec l'ensemble de générateurs de $\mathbb{Z}/n\mathbb{Z}$.

1.23. *Lemme.* $n = \sum_{d|n} \phi(n)$.

En effet, pour chaque $d|n$ soit Φ_d l'ensemble d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ = l'ensemble de générateurs de $\mathbb{Z}/d\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$. Alors $\mathbb{Z}/n\mathbb{Z} = \coprod_{d|n} \Phi_d$.

1.24. *Corollaire.* $\phi(n) = \sum_{d|n} d\mu(n/d)$

1.25. *Exercice.* Montrer, en employant 1.25, que si $n = \prod_{i=1}^{r} p_i^{a_i}$ est la décomposition en facteurs premiers (tous p_i étant distincts), alors

$$\phi(n)/n = \prod_{i=1}^{r} (1 - p_i^{-1})$$

Solution. On a

$$\phi(n) = \sum_{d|n} d\mu(n/d) =$$

$$= n - \sum_i n/p_i + \sum_{i<j} n/p_i p_j - \ldots = n \prod_{i=1}^{r} (1 - p_i^{-1})$$

1.26. *Exercice.* Combien y a-t-il de racines primitives modulo 37?

1.27. *Lemme.* $x^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (x - i)\ (p)$.

En effet, par le petit Fermat on connait $p-1$ racines: $1, \ldots, p-1$ du polynôme dans $\mathbb{F}_p[x]$.

1.28. *Corollaire* (théorème de Wilson) $(p-1)! \equiv -1\ (p)$.

Poser $x = 0$ dans 1.27.

1.29. *Corollaire.* Si $d \mid (p-1)$ alors le polynome $x^d - 1$ a d racines dans $\mathbb{F}_p$.

En effet, si $d \mid (p-1)$ alors $(x^d-1)|(x^{p-1}-1)$ dans $\mathbb{F}_p$ (prouver!), i.e. $x^{p-1}-1 = (x^d-1)g(x)$. Nous savons que $x^{p-1}-1$ a $p-1$ racines; mais si x^d-1 avait moins que d racines alors $x^{p-1}-1$ aurait moins que $p-1$ racines car $g(x)$ a au plus $\deg(g(x)) = p-1-d$ racines.

1.30. *Théorème.* Le groupe $\mathbb{F}_p^*$ est cyclique.

Soit $\psi(d)$ le nombre d'éléments d'ordre d dans $\mathbb{F}_p^*$. D'après 1.29, on a $d = \sum_{c|d} \psi(c)$. D'après la formule d'inversion de Moebius,

$$\psi(d) = \sum_{c|d} c\mu(d/c) = \phi(d)$$

(par 1.23). En particulier, $\psi(p-1) = \phi(p-1) > 0$ si $p > 2$. Pour $p = 2$ l'assertion est triviale.

(d) *Formule de Newton (Taylor discrét)*

1.31. *Coefficients binomiaux.* Pour $a \in \mathbb{C},\ i \in \mathbb{N}$, on définit

$$\binom{a}{i} = \frac{a(a-1)\ldots(a-i+1)}{i!}$$

De même, si x est une variable, on pose

$$\binom{x}{i} = \frac{x(x-1)\ldots(x-i+1)}{i!} \in \mathbb{Q}[x]$$

Ces polynômes pour $i = 0, 1, 2, \ldots$, forment une $\mathbb{Q}$-base de $\mathbb{Q}[x]$, et ils prennent de valeurs entiers en points entiers (démontrez!).

Exemples. $\binom{a}{0} = 1, \binom{a}{1} = a,\ \binom{-1}{i} = (-1)^i$. Calculez $\binom{-2}{i}$.

1.32. *Exercice.* Démontrez la formule binomielle:

$$(1+t)^a = \sum_{i=0}^{\infty} \binom{a}{i} t^i \in \mathbb{Z}[[t]]$$

$a \in \mathbb{Z}$. (Pour $a < 0$ commencer par $a = -1$, et faitez la récurrence en employant la dérivée.)

1.33. *Exercice.* Démontrer que $\binom{1/2}{i} \in \mathbb{Z}[1/2]$.

1.34. *Puissances discrètes.* Si x est une variable ou un nombre, et $i \in \mathbb{Z}$, on pose

$$x^{[i]} = x(x-1)\dots(x-i+1)$$

Donc $i^{[i]} = i!$, et

$$\binom{x}{i} = \frac{x^{[i]}}{i!}$$

1.35. *La dérivée discrète.* Pour $f(x) \in \mathbb{C}[x]$ on définit le polynôme Δf par

$$\Delta f(x) = f(x+1) - f(x)$$

Donc si $\deg f = d$, alors $\deg \Delta f = d - 1$.

Montrez que

$$\Delta x^{[i]} = i x^{[i-1]}$$

1.36. *Exercice.* (a) Pour chaque $f \in \mathbb{C}[x]$,

$$f(x) = \sum_{i=0}^{\infty} \Delta^i f(0) \cdot \frac{x^{[i]}}{i!} = \sum_{i=0}^{\infty} \Delta^i f(0) \cdot \binom{x}{i}$$

Idée: si l'on considère un développement limité

$$g(x)_{\le d} = \sum_{i=0}^{d} \Delta^i f(0) \cdot \binom{x}{i}$$

alors $f(i) = g(i)_{\le d}$ pour $i = 0, 1, \dots, d$.

(b) On définit:

$$\tilde{\Delta} f(x) = f(x) - f(x-1)$$

Montrer que pour chaque $f(x) \in \mathbb{C}[x]$,

$$f(x) = \sum_{i=0}^{\infty} \tilde{\Delta}^i f(-1) \binom{x+i}{i}$$

1.37. *Exercice.* Définissons un sous-anneau

$$P = \{f \in \mathbb{C}[x] \mid f(\mathbb{Z}) \subset \mathbb{Z}\}$$

Montrez que les polynômes $\binom{x}{i}$, $i \in \mathbb{Z}$, forment une $\mathbb{Z}$-base de P. Il s'ensuit que $P \subset \mathbb{Q}[x]$.

1.38. *Exercice*: Séries d'Hilbert. (i) Montrer que pour chaque $i \geq 0$,

$$\sum_{n=0}^{\infty} \binom{n+i}{i} x^n = \frac{1}{(1-x)^{i+1}}$$

(ii) En déduire que, $P(t)$ étant un polynôme arbitraire de degré d, on a:

$$H(P;x) := \sum_{n=0}^{\infty} P(n)x^n = \frac{Q(x)}{(1-x)^{d+1}},$$

où $Q(x)$ est le polynôme de degré d défini par son développement de Taylor en $x = 1$:

$$(-1)^i \frac{Q^{(i)}(1)}{i!} = \tilde{\Delta}^{d-i} P(-1)$$

(iii) En déduire que $P(x) \in P$ ssi $Q(x) \in \mathbb{Z}[x]$.

(iv) Faire un exemple:

$$\sum_{n=0}^{\infty} ((b+1)n+1)x^n = \frac{1+bx}{(1-x)^2}$$

(d) *Identité cyclotomique de Gauss*

Cf. [G], (e), no. 343 - 347, pp. 220 - 222.

1.39. *Polynômes des colliers.* On définit, avec Gauss

$$M_n(x) = \frac{1}{n} \sum_{d|n} \mu(d) x^{n/d}$$

Un collier c est un anneau de n perles; supposons que chaque perle peut avoir m couleurs. Un collier de la forme $c = dc'$ pour $d|n$ est appelé décomposable. Un collier qui n'est pas décomposable est appelé *primitif.*

1.40. *Exercice.* Prouver le *théorème de Moreau* (1872, cf. [M]; C.Moreau était un capitaine d'artillerie français): le nombre de colliers à n perles et à m couleurs est égal à $M_n(m)$.

Faire d'abord le cas $n = p$ un nombre premier.

1.41. *Exercice.* Montrer que chaque série $f(t) \in \mathbb{Z}[[t]]$ avec $f(0) = 1$ se décompose uniquement en produit

$$f(t) = \prod_{n=1}^{\infty} (1-t^n)^{a_n},\ a_n \in \mathbb{Z}$$

Trouver les premiers a_n pour $f(t) = 1 + 2t$.

Réponse:

$$1 + 2t = (1-t)^{-2}(1-t^2)^3(1-t^3)^{-2}(1-t^4)^3(1-t^5)^{-6}\dots$$

1.42. *Théorème.* Pour tous $b \in \mathbb{C}$

$$1 - bt = \prod_{n=1}^{\infty} (1-t^n)^{M_n(b)},$$

Preuve. On pose

$$1 - bt = \prod_{n=1}^{\infty} (1-t^n)^{a_n}$$

et l'on prend $td\log/dt$ de deux côtés:

$$-\sum_{i=1}^{\infty} b^i t^i = -\sum_{n=1}^{\infty} a_n \sum_{j=1}^{\infty} nt^{nj} = -\sum_{i=1}^{\infty}\Big(\sum_{n|i} na_n\Big)\cdot t^i,$$

d'où

$$b^i = \sum_{n|i} na_n,$$

et l'on finit par application de l'inversion de Moebius.

1.43. *Exercice.* Soit $f(q) \in \mathbb{C}[q, q^{-1}]$. On définit:

$$M_n(f;q) := \frac{1}{n}\sum_{d|n} \mu(d) f(q^d)^{n/d}$$

Par exemple, si $f(q)$ est une constante c, alors $M_n(c;q) = M_n(c)$.

(i) Montrez que

$$1 - f(q)t = \prod_{n=1}^{\infty}\prod_{i=-\infty}^{\infty} (1-q^i t^n)^{a_{in}}$$

où les exposants a_{in} sont définis par:

$$\sum_i a_{in}\cdot q^i = M_n(f;q)$$

(la somme est finie).

Solution. Prenons $-\log$ de deux côtés:

$$-\log(1-f(q)t) = \sum_{m=1}^{\infty} \frac{f(q)^m t^m}{m}$$

et

$$-\log(\prod_{i,n}(1-q^i t^n)^{a_{in}}) = \sum_i \sum_{n,k=1}^{\infty} a_{in}\frac{q^{ik}t^{nk}}{k} =$$

$$= \sum_{m=1}^{\infty} t^m \cdot \Big(\sum_{n|m} \sum_i a_{in} \frac{q^{im/n}}{m/n} \Big),$$

d'où

$$f(q)^m = \sum_{n|m} \sum_i n a_{in} q^{im/n}$$

pour chaque $m = 1, 2, \ldots$. On fait un changement de variable: $p = q^m$,

$$f(p^{1/m})^m = \sum_{n|m} \sum_i n a_{in} p^{i/n}$$

Maintenant on peut utiliser l'inversion de Moebius:

$$\sum_i n a_{in} p^{i/n} = \sum_{d|n} \mu(n/d) f(p^{1/d})^d,$$

et en faisant le retour: $q = p^{1/n}$, on obtient

$$\sum_i n a_{in} q^i = \sum_{d|n} \mu(n/d) f(q^{n/d})^d,$$

ce qui est la formule cherchée.

(ii) Faitez les cas: $f(q) = q^i$; $f(q) = -q$.

(e) *Fonction zeta de l'anneau* $\mathbb{F}_p[x]$

1.43. On pose $A := \mathbb{F}_p[x]$; cet anneau est tout à fait pareil à $\mathbb{Z}$.

Les idéaux non-nuls $I \subset A$ sont en bijection avec les polynômes unitares $f(x)$, $I = (f)$, et les idéaux premiers correspondent aux polynômes irréductibles. On pose

$$N(I) := \sharp(A/I) = p^{\deg f},$$

et l'on définit

$$\zeta(A; s) = \sum_{0 \neq I \subset A} N(I)^{-s} = \sum_{f \text{ unitaire}} p^{-s \deg f}$$

Il y a p^n polynômes unitaires de degré n, d'où

$$\zeta(A; s) = \sum_{n=1}^{\infty} p^n \cdot p^{-sn} = \frac{1}{1 - p \cdot p^{-s}} = \frac{1}{1 - pT}, \tag{1.43.1}$$

où l'on pose $T := p^{-s}$.

Le produit d'Euler pour $\zeta(A; s)$ s'ecrit sous une forme

$$\zeta(A; s) = \prod_{f \text{ unitaire, irréductible}} \frac{1}{1 - p^{-\deg f \cdot s}} =$$

$$= \prod_{d=1}^{\infty} \prod_{f \text{ un., irr.,} \deg f = d} \frac{1}{1-p^{-ds}} = \prod_{d=1}^{\infty} \frac{1}{(1-T^d)^{N_d(p)}},$$

où $N_d(p)$ désigne le nombre de polynômes unitaires irréductibles de degré d dans A.

De l'autre côté, en appliquant l'identité cyclotomique à (1.33.1),

$$\zeta(A;s) = \frac{1}{1-pT} = \frac{1}{\prod_{d=1}^{\infty} (1-T^d)^{M_d(p)}},$$

et l'on a démontré

1.44. *Théorème* (Gauss). Le nombre de polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[x]$ est égale à

$$N_d(p) = M_d(p) = \frac{1}{d} \sum_{l|d} \mu(l) p^{d/l}$$

1.45. *Corollaire.* Pour $d \geq 1$, $N_d(p) > 0$, i.e. pour chaque $d \geq 1$ il existe un polynôme irréductible de degré d.

En effet, l'ordre de croissance de $N_d(p)$ est exponentiel: $N_d(p)d^{-1} \sim p^d$ quand $d \to \infty$.

On a donc démontré en particulier encore une fois l'existence pour chaque $n \geq 1$ d'un corps fini à p^n éléments.

(f)

1.46. *Théorème* (Gauss). On a l'identité dans $\mathbb{F}_p[x]$

$$x^{p^n} - x = \prod_{d|n} F_d(x)$$

où $F_d(x)$ désigne le produit de tous polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[x]$.

La preuve suivra quelques lemmes.

1.47. *Lemme.* (a) Soit K un corps. Dans $K[x]$, le polynôme $x^n - 1$ divise $x^m - 1$ ssi $n|m$.

(b) Soit $a \in \mathbb{Z},\ a > 1$. Alors $a^n - 1$ divise $a^m - 1$ ssi $n|m$.

Exercice.

1.48. *Lemme.* Dans $\mathbb{F}_p[x]$, si un polynôme $f(x)$ divise $x^{p^n} - x$, alors $f(x)^2$ ne le divise pas.

Car si $x^{p^n} - x = f(x)^2 g(x)$, alors en prénant la dérivée,

$$-1 = 2f'(x)f(x)g(x) + f(x)^2 g'(x),$$

ce qui est impossible.

1.49. *Lemme.* Dans $\mathbb{F}_p[x]$, un polynôme irréductible de degré d divise $x^{p^n} - x$ ssi $d|n$.

Soit $f(x)$ un polynôme irréductible de degré d. Posons $K = \mathbb{F}_p[x]/(f) = \mathbb{F}_p(\alpha)$. On a $[K : \mathbb{F}_p] = d$, d'où $\mathrm{Card}(K) = p^d$, donc $\beta^{p^d} - \beta = 0$ pour tous $\beta \in K$.

Si $f(x)|(x^{p^n} - x)$ alors $\alpha^{p^n} - \alpha = 0$ puisque $f(\alpha) = 0$. Il s'en suit que $\beta^{p^n} - \beta = 0$ pour tous $\beta \in K$ (pourquoi?). Donc $(x^{p^d} - x)|(x^{p^n} - x)$ dans $K[x]$ (car le reste aura p^d racines). Donc $(x^{p^d-1} - 1)|(x^{p^n-1} - 1)$; par 1.37 (a), $(p^d - 1)|(p^n - 1)$, par 1.37 (b), $d|n$.

Réciproquement, puisque $\alpha^{p^d} = \alpha$, on a $f(x)|(x^{p^d} - x)$, $f(x)$ étant le polynôme irréductible pour α. Si $d|n$, alors $(x^{p^d} - x)|(x^{p^n} - x)$ d'après 1.47, donc $f(x)|(x^{p^n} - x)$, cqfd.

Notre théorème est une conséquence immédiate de 1.49.

(g) *Topologie t-adique*

1.50. Soit A un anneau commutatif; considérons l'anneau de séries formelles $A[[t]]$. Pour une série

$$f(t) = a_n t^n + a_{n+1} t^{n+1} + \dots, \ a_n \neq 0,$$

on définit $v(f) := n$; on pose $v(0) = \infty$, d'où l'apllication

$$v : \ A[[t]] \longrightarrow \mathbb{N} \cup \{\infty\}$$

qui a les propriétés suivantes:

(i) $v(1) = 0$; (ii) $v(fg) \leq v(f) + v(g)$ (avec l'égalité si A est intègre); (iii) $v(f + g) \leq \inf(v(f), v(g))$ (égalité si $v(f) \neq v(g)$).

1.51. Fixons un nombre réel c, $0 < c < 1$. On introduit une norme sur $A[[t]]$ par $||f|| = c^{v(f)}$. Alors:

(i) $||f|| = 0$ ssi $f = 0$; $||1|| = 1$; (ii) $||fg|| \leq ||f|| \cdot ||g||$ (égalité si A est intègre); (iii) $||f + g|| \leq \sup(||f||, ||g||)$ (égalité si $||f|| \neq ||g||$).

La norme définit la distance sur $A[[t]]$: $d(f, g) = ||f - g||$. La topologie corréspondante ne depend pas du choix de c.

1.52. *Exercice.* (a) Une série $\sum_n f_n$ converge ssi $||f_n|| \longrightarrow 0$.

(b) $A[[t]]$ est en espace métrique complét.

(c) $A[t]$ est dense dans $A[[t]]$.

§2. Réciprocité quadratique

2.1. *Définition* (Gauss) Soient $m \in \mathbb{Z}_{>1}$, $a \in \mathbb{Z}$, $(a, m) = 1$. a est appelé *résidu quadratique* modulo m si il existe une solution de la congruence $x^2 \equiv a\ (m)$. Sinon, a est appelé *non-résidu quadratique*.

En d'autres termes, a est résidu quadratique modulo m ssi sa classe $\bar{a} := a\mathrm{mod}(m) \in \mathbb{Z}/m\mathbb{Z}$ appartient à $(\mathbb{Z}/m\mathbb{Z})^{*2}$.

Considérons le cas $m = p$ en nombre premier. Le cas $p = 2$ étant trivial, nous supposerons que $p > 2$. Le groupe $\mathbb{F}_p^*$ est cyclique. Soit $u \in \mathbb{F}_p^*$ un générateur (une racine primitive). Alors $a \in \mathbb{F}_p^{*2}$ ssi $a = u^n$ avec n pair.

Il s'en suit que $a^{(p-1)/2} \in \{-1, 1\}$ et $a \in \mathbb{F}_p^{*2}$ ssi $a^{(p-1)/2} = 1$.

2.2. *Symbole de Legendre.* Soient p un nombre premier impair, a un nombre entier qui n'est pas divisible par p (ou un élément de $\mathbb{F}_p^*$). On définit $(a/p) := a^{(p-1)/2}\mathrm{mod}(p) = \pm 1$.

Donc on a $(-1/p) = (-1)^{(p-1)/2}$. En d'autres termes, $(-1/p) = 1$ si $p \equiv 1\ (4)$ et $(-1/p) = -1$ si $p \equiv 3\ (4)$.

Pour un entier n impair, définissons

$$\epsilon(n) = \frac{n-1}{2}\ (\mathrm{mod}\ 2) \in \mathbb{Z}/2\mathbb{Z}$$

Considérons le groupe multiplicatif $(\mathbb{Z}/4\mathbb{Z})^*$; il est cyclique, avec un générateur 3. On peut considérer ϵ comme un homomorphisme $\epsilon :\ (\mathbb{Z}/4\mathbb{Z})^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$.

On a $(-1/p) = (-1)^{\epsilon(p)}$.

2.3. Considérons le groupe $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$. On a

$$(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{1, 7\} \times \{1, 3\}$$

Pour un nombre entier impair n, posons

$$\omega(n) = \frac{n^2-1}{8}\ (\mathrm{mod}\ 2) \in \mathbb{Z}/2\mathbb{Z}$$

Donc $\omega(n) = 0$ si $n \equiv \pm 1\ (\mathrm{mod}\ 8)$ et $\omega(n) = 1$ si $n \equiv \pm 3\ (\mathrm{mod}\ 8)$.

On peut considérer ω comme un homomorphisme $(\mathbb{Z}/8\mathbb{Z})^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$.

2.4. *Théorème.* $(2/p) = (-1)^{\omega(p)}$

Démonstration. Soit α une racine primitive 8-ième de l'unité dans une clôture algébrique $\Omega \supset \mathbb{F}_p$, c'est-à-dire, un élément $\alpha \in \Omega$ satisfaisant l'équation $\alpha^4 = -1$. Posons $y = \alpha + \alpha^{-1}$. Alors

$$y^2 = \alpha^2 + 2 + \alpha^{-2} = 2$$

Donc

$$(\frac{2}{p}) = 2^{(p-1)/2} = y^{p-1}$$

D'un autre côté,

$$y^p = \alpha^p + \alpha^{-p}$$

Il s'en suit que si $p \equiv \pm 1 \pmod 8$, alors $y^p = y$, donc $y^{p-1} = 1$.

Par contre, si $p \equiv \pm 3 \pmod 8$, alors (comme $\alpha^4 = -1$)

$$y^p = \alpha^5 + \alpha^{-5} = -\alpha - \alpha^{-1} = -y,$$

donc $y^{p-1} = -1$, cqfd.

2.4.1. *Exercice.* Déterminer le degré $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$.

Solution. Considérons la tour $\mathbb{F}_p(\alpha) \supset \mathbb{F}_p(\beta) \supset \mathbb{F}_p$, où $\beta = \alpha^2$. On a $\beta^2 = -1$, $\beta^4 = 1$, donc $[\mathbb{F}_p(\beta) : \mathbb{F}_p] = 1$ ssi $\beta \in \mathbb{F}_p \Leftrightarrow 4|(p-1)$; si $p = 4k+3$, alors $[\mathbb{F}_p(\beta) : \mathbb{F}_p] = 2$.

De même, α est un élément d'ordre 8, donc $\alpha \in \mathbb{F}_q$ ssi $\mathbb{F}_q^*$ contient en élément d'ordre 8, donc $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$ où n est minimal tel que $8|(p^n - 1)$.

Il s'en suit que $[\mathbb{F}(\alpha) : \mathbb{F}_p] = 1$ si $p \equiv 1 \pmod 8$, sinon, ce degré est égal à 2.

Corollaire. Le polynôme $x^4 + 1$ est toujours réductible sur $\mathbb{F}_p$.

Rémarque. On a $x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$, donc si $\sqrt{2} \in \mathbb{F}_p$, i.e. $p \equiv \pm 1 \pmod 8$, la même décomposition est valable dans $\mathbb{F}_p[x]$.

2.5. *Variante de la démonstration.* Soit $\zeta = e^{\pi i/4}$. Alors $\zeta^4 = -1$. On va travailler dans l'anneau $A = \mathbb{Z}[\zeta]$. On rémarque que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subset A/pA$. En effet, $A \cong \mathbb{Z}[x]/(x^4+1)$, d'où $A/pA \cong \mathbb{F}_p[x]/(x^4+1)$.

2.5.1. *Exercice.* Prouver que $A \cong \mathbb{Z}[x]/(x^4+1)$.

Considérons l'élément $\tau = \zeta + \zeta^{-1} \in A$. On a

$$\tau^2 = \zeta^2 + 2 + \zeta^{-2} = 2, \tag{2.5.1}$$

car $\zeta^2 = -\zeta^{-2}$. Plus exactement,

$$\zeta = \cos(\pi/4) + i\sin(\pi/4) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},$$

d'où

$$\tau = \zeta + \zeta^{-1} = \sqrt{2} \tag{2.5.2}$$

(pour le moment, on n'aura pas besoin de ce résultat plus précis).

Il découle de (2.5.1) que

$$\tau^{p-1} = \tau^{2(p-1)/2} = 2^{p-1} \equiv \left(\frac{2}{p}\right) \pmod{p\mathbb{Z}},$$

d'où

$$\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{pA} \tag{2.5.3}$$

D'un autre côté, $\tau^p \equiv \zeta^p + \zeta^{-p} \pmod{pA}$ et $\zeta^p + \zeta^{-p} = \tau$ si $p \equiv \pm 1 (\mathrm{mod}\ 8)$ et $\zeta^p + \zeta^{-p} = -\tau$ si $p \equiv \pm 3 (\mathrm{mod}\ 8)$, i. e.

$$\tau^p \equiv (-1)^{\omega(p)} \tau \pmod{pA}$$

Donc

$$(\frac{2}{p})\tau \equiv (-1)^{\omega(p)} \tau \pmod{pA};$$

multipliant par τ,

$$2(\frac{2}{p}) \equiv 2(-1)^{\omega(p)} \pmod{pA};$$

Puisque 2 est inversible dans $\mathbb{F}_p \subset A/pA$, on en conclut que

$$(\frac{2}{p}) \equiv (-1)^{\omega(p)} \pmod{p},$$

ce qui entraîne $(2/p) = (-1)^{\omega(p)}$, cqfd.

2.6. *Exercice.* Montrer qu'il existe un nombre infini de nombres premiers p de la forme $8n + 7$.

Solution. Soient $p_1, \ldots, p_m$ des nombres premiers de la forme $8n+7$. Considérons le nombre $a = (4 \prod_{i=1}^m p_i)^2 - 2$. Si p est un nombre premier impair divisant a, alors 2 est résidu quadratique modulo p, donc $p \equiv \pm 1(8)$.

Par contre, $a/2 \equiv -1(8)$. Donc il existe un nombre premier p de la forme $8n + 7$ divisant a; évidemment, $p \notin \{p_1, \ldots, p_m\}$.

2.7. *Théorème* (Gauss) Soient p, q des nombres premiers impairs distincts. Alors

$$(\frac{p}{q}) = (-1)^{\epsilon(p)\epsilon(q)} (\frac{q}{p})$$

Dans la preuve on généralisera l'argument 2.5.

Sommes de Gauss quadratiques

2.8. On pose $\zeta = e^{2\pi i/p}$. On a

$$0 = \zeta^p - 1 = (\zeta - 1)(\zeta^{p-1} + \ldots + 1),$$

d'où

$$S_1 := \sum_{a=0}^{p-1} \zeta^a = 0 \tag{2.8.1}$$

Plus généralement, considérons la somme

$$S_a := \sum_{b=0}^{p-1} \zeta^{ab}$$

Il est clair que si $a \equiv 0(p)$, alors $S_a = p$.

Par contre, si $(a,p) = 1$ alors $\{ab \pmod p \mid 0 \leq b \leq p-1\} = \{0, ..., p-1\}$ d'où $S_a = S_1 = 0$.

On va travailler dans l'anneau $A = \mathbb{Z}[\zeta]$. Considérons le polynôme

$$f_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$$

D'après (2.8.1) on a l'homomorphisme surjectif d'anneaux

$$\phi : \ A' = \mathbb{Z}[x]/(f_p(x)) \longrightarrow A, \ \phi(x) = \zeta$$

2.9. *Théorème.* ϕ est un isomorphisme.

Pour une preuve voir 3.9.

D'ailleurs, on peut considérer (avec Gauss) tous ce qui se passe ci-dessous dans l'anneau A'.

2.10. Il est commode à poser $(0/p) = 0$.

2.10.1. *Lemme.* $\sum_{a \in \mathbb{F}_p} (a/p) = 0$.

Exercice.

On définit

$$g_a = \sum_{b \in \mathbb{F}_p} (\frac{b}{p}) \zeta^{ab} \ \in A$$

On désigne $g = g_1$.

2.11. *Lemme.* $g_a = (a/p)g$

Exercice.

Par exemple, puisque $\bar{\zeta} = \zeta^{-1}$, on trouve pour la conjuguée complexe

$$\bar{g} = g_{-1} = (-1/p)g = (-1)^{\epsilon(p)} g \tag{2.11.1}$$

2.11.1. *Exercice.* Montrer que

$$g = \sum_{a=0}^{p-1} e^{2\pi i a^2/p} \tag{2.11.2}$$

Solution. Soient $R, N \subset \{1, \ldots, p-1\}$ les sous-ensembles de résidus (resp. non-résidus) quadratiques,

$$g_R = \sum_{a \in R} \zeta^a, \ g_N = \sum_{a \in N} \zeta^a$$

On a $g_R + g_N = -1$ (pourquoi?). Donc

$$g = g_R - g_N = 1 + 2g_R = 1 + \sum_{a=1}^{p-1} e^{2\pi i a^2/p}$$

2.12. *Théorème* (Gauss)

$$|g|^2 = g\bar{g} = p \tag{2.12.1}$$

D'après (2.11.1), cela est équivalent à

$$g^2 = (-1)^{\epsilon(p)}p \tag{2.12.2}$$

Rémarquons que $g_a^2 = g^2$ pour tous $a,\ (a,p) = 1$.

Démonstration. Considérons le nombre $\sum_{a\in\mathbb{F}_p}\ g_a g_{-a} = \sum_{a\in\mathbb{F}_p^*}\ g_a g_{-a}$. D'un côté, on a pour $a \in \mathbb{F}_p^*$

$$g_a g_{-a} = (a/p)(-a/p)g^2 = (-1/p)g^2,$$

d'où

$$\sum_a\ g_a g_{-a} = (p-1)(-1/p)g^2$$

D'un autre côté,

$$g_a g_{-a} = \sum_{b,c}\ (\frac{b}{p})(\frac{c}{p})\zeta^{a(b-c)},$$

d'où

$$\sum_a\ g_a g_{-a} = \sum_{b,c}\ (\frac{b}{p})(\frac{c}{p})\sum_a\ \zeta^{a(b-c)} =$$

(cf. 2.8)

$$= p\sum_{b,c}\ (\frac{b}{p})(\frac{c}{p})\ \delta(b,c) = p\sum_b\ (\frac{b^2}{p}) = p(p-1),$$

ce qui entraîne (2.12.2).

2.13. Maintenant on peut prouver la loi de réciprocité quadratique 2.7. La preuve est pareille à 2.5, avec τ remplacée par g. On va utiliser des congruences dans A (ou dans A'). On pose

$$p^* := (-1)^{\epsilon(p)}p$$

Rappelons que q est un nombre premier impair distinct de p. On a

$$g^{q-1} = (g^2)^{(q-1)/2} = p^{*(q-1)/2} \equiv (\frac{p^*}{q})\ (\mathrm{mod}\ qA),$$

d'où

$$g^q \equiv (\frac{p^*}{q})g\ (\mathrm{mod}\ qA)$$

D'autre part,

$$g^q \equiv \sum_b\ (\frac{b}{p})^q\zeta^{bq}\ (\mathrm{mod}\ qA),$$

avec

$$\sum_b (\frac{b}{p})^q \zeta^{bq} = g_q = (\frac{q}{p})g$$

(q étant impair). Donc

$$(\frac{p^*}{q})g \equiv (\frac{q}{p})g \pmod{qA}$$

En multipliant par g,

$$(\frac{p^*}{q})p^* \equiv (\frac{q}{p})p^* \pmod{qA}$$

Mais p^* est inversible dans A/qA, donc

$$(\frac{p^*}{q}) \equiv (\frac{q}{p}) \pmod{qA},$$

d'où

$$(\frac{p^*}{q}) = (\frac{q}{p})$$

Cela est 2.7, car

$$(\frac{p^*}{q}) = (\frac{-1}{q})^{\epsilon(p)}(\frac{p}{q}) = (-1)^{\epsilon(p)\epsilon(q)}(\frac{p}{q})$$

2.13.1. *Exercice.* Calculer (13/17).

Sommes de Gauss à valeurs dans un corps fini

2.14. Soient p et ℓ deux nombres premiers distincts impairs. Dans une clôture algébrique $\Omega \supset \mathbb{F}_p$, choisissons une racine primitive ℓ-ième de l'unité, w. On définit la "somme de Gauss"

$$y = \sum_{a \in \mathbb{F}_\ell} (\frac{a}{\ell})w^a$$

2.15. *Théorème.* $y^2 = (-1)^{\epsilon(\ell)}\ell$.

Cf. 2.12.

En effet:

$$y^2 = \sum_{a,b} (\frac{ab}{\ell})w^{a+b} = \sum_{c \in \mathbb{F}_\ell} w^c \sum_{a \in \mathbb{F}_\ell} (\frac{a(c-a)}{\ell})$$

Or si $a \neq 0$:

$$(\frac{a(c-a)}{\ell}) = (\frac{-a^2}{\ell})(\frac{1-ca^{-1}}{\ell}) = (-1)^{\epsilon(\ell)}(\frac{1-ca^{-1}}{\ell}),$$

d'où

$$(-1)^{\epsilon(\ell)}y^2 = \sum_{c \in \mathbb{F}_\ell} A_c w^c,$$

où

$$A_c = \sum_{a \in \mathbb{F}_\ell^*} (\frac{1 - ca^{-1}}{\ell})$$

Si $c = 0$, $A_0 = \ell - 1$. D'un autre côté, si $c \neq 0$, l'application $a \mapsto 1 - ca^{-1}$ est une bijection $\mathbb{F}_\ell^* \xrightarrow{\sim} \mathbb{F}_\ell - \{1\}$. Donc

$$A_c = \sum_{d \in \mathbb{F}_\ell} (\frac{d}{\ell}) - (\frac{1}{\ell}) = -1$$

Il s'en suit:

$$\sum_{c \in \mathbb{F}_\ell} A_c w^c = \ell - 1 - \sum_{c \in \mathbb{F}_\ell^*} w^c = \ell,$$

ce qui démontre le théorème.

2.15.1. $y \in \Omega^*$.

2.16. *Lemme.* $y^{p-1} = (p/\ell)$.

En effet, puisque $\mathrm{char}(\Omega) = p$,

$$y^p = \sum_{a \in \mathbb{F}_\ell} (\frac{a}{\ell}) w^{ap} = (\frac{p}{\ell}) y,$$

ce qui entraîne le lemme, vu 2.15.1.

2.17. Maintenant on peut prouver 2.7, encore une fois. On a

$$y^{p-1} = (y^2)^{(p-1)/2} = ((-1)^{\epsilon(\ell)}\ell)^{(p-1)/2} = (\frac{(-1)^{\epsilon(\ell)}\ell}{p})$$

En combinant avec 2.16, cela implique le théorème.

Une démonstration d'Eisenstein

2.18. Soit p un nombre premier impair. Soit $S \subset \mathbb{F}_p^*$ un sous-ensemble tel que $\mathbb{F}_p^* = S \coprod (-S)$, par exemple, $S = \{1, \ldots, (p-1)/2\}$.

Pour $a \in \mathbb{F}_p^*,\ s \in S$, posons

$$as = e_s(a) s_a,\ e_s(a) = \pm 1,\ s_a \in S$$

On remarque que si $s \neq s'$ alors $s_a \neq s'_a$, car sinon, on aurait $s' = \pm s$, ce qui est impossible par hypothèse sur S. Donc $s \mapsto s_a$ est une bijection de S sur lui-même.

2.19. *Lemme* (Gauss) $(a/p) = \prod_{s \in S}\ e_s(a)$

En effet,

$$a^{(p-1)/2} \prod_{s \in S}\ s = \prod_{s \in S}\ (as) = \prod_{s \in S}\ e_s(a) s_a = \prod_{s \in S}\ e_s(a) \prod_{s \in S}\ s,$$

d'où

$$a^{(p-1)/2} = \prod_{s\in S} e_s(a),$$

ce qui entraîne le lemme.

2.20. *Exercice.* En déduire théorème 2.4.

Solution. Prenons $a = 2$, $S = \{1, \dots, (p-1)/2\}$. On a $e_s(2) = 1$ si $2s \leq (p-1)/2$ et $e_s(2) = -1$ si $2s > (p-1)/2$. Donc $(2/p) = (-1)^{n(p)}$ où $n(p)$ est le nombre d'entiers s tels que $(p-1)/4 < s \leq (p-1)/2$. Il reste à montrer que $n(p) \equiv \omega(p) \pmod 2$.

En effet, si $p = 4k+1$, la condition est $k < s \leq 2k$, d'où $n(p) = k$. De même, si $p = 4k-1$, $n(p) = k$ (vérifier!) Donc si $k = 2n$, c'est-à-dire, $p = 8n \pm 1$, alors $(2/p) = 1$.

Par contre, si $k = 2n+1$, i.e. $p = 8n + 4 \pm 1 = 8m \pm 3$, on a $(2/p) = -1$, cqfd.

Polynômes de Tchebycheff

2.21. *Lemme.* Soit m un nombre entier impair, $m \geq 1$. On a $\sin(mx) = f_m(\sin(x))$, où $f_m(t) \in \mathbb{Z}[t]$ est un polynôme de degré m, divisible par t, avec le terme supérieur égale à $(-4)^{(m-1)/2}$.

Démonstration par récurrence sur m. Le cas $m = 1$ est évident. Supposons que l'assertion est prouvée pour m. Nous avons

$$\sin(mx) = f_m(\sin(x)),$$

d'où, en faisant la dérivée,

$$m\cos(mx) = f'_m(\sin(x))\cos(x)$$

Donc

$$\sin((m+2)x) = \sin(mx)\cos(2x) + \cos(mx)\sin(2x) =$$

$$= f_m(\sin(x))(1 - 2\sin^2 x)) + 2m^{-1} f'_m(\sin(x))(1 - \sin^2 x)\sin(x) = f_{m+2}(\sin(x)),$$

où

$$f_{m+2}(t) = f_m(t)(1-2t^2) + 2m^{-1} f'_m(t)t(1-t^2) \tag{2.21.1}$$

Il s'en suit que $f_{m+2}(t) \in t\mathbb{Z}[t]$ et si $f_m(t) = a_m t^m + \dots$, alors $f_{m+2}(t) = -4a_m t^{m+2} + \dots$, ce qui implique le lemme.

Variante. On a

$$\sin((m-2)x) = \sin(mx)\cos(2x) - \cos(mx)\sin(2x),$$

donc

$$\sin((m+2)x) + \sin((m-2)x) = 2\sin(mx)(1 - 2\sin^2(x)),$$

d'où l'équation de récurrence

$$f_{m+2}(t) = 2f_m(t)(1-2t^2) - f_{m-2}(t) \tag{2.21.2}$$

(On a $f_1(t) = t,\ f_{-1}(t) = -t$.)

2.22. *Lemme.* Soit m en entier impair ≥ 1. Alors

$$\frac{\sin(mx)}{\sin(x)} = (-4)^{(m-1)/2} \prod_{a=1}^{(m-1)/2} (\sin^2 x - \sin^2(2\pi a/m))$$

En effet, d'après le lemme précédent,

$$(-4)^{-(m-1)/2} \frac{\sin(mx)}{\sin(x)} = g_m(\sin(x)),$$

où $g(t)$ est un polynôme unitaire de degré pair $m-1$. Or, il est très facile d'exhiber les $m-1$ racines distinctes de $g_m(t)$: ils sont $\pm\sin(2\pi a/m),\ a = 1, \ldots, (m-1)/2$ (on remarque que les nombres $\{\pm 2a \mid a = 1, \ldots, (m-1)/2\}$ décrivent tous les résidus possibles mod m sauf 0), d'où la formule désirée.

2.23. *Exercice* (Gauss, Eisenstein) (a) Montrer que $f_m(t)$ satisfait à l'équation différentielle

$$\frac{df_m(t)}{dt} = \frac{m\sqrt{1 - f_m(t)^2}}{\sqrt{1 - t^2}}$$

(b) Montrer que $f_m(t)$ satisfait à l'équation différentielle

$$(1 - t^2) f_m''(t) - t f_m'(t) + m^2 f_m(t) = 0$$

(c) En déduire que

$$f_m(t) = mt - \frac{m(m^2-1)}{3!}t^3 + \frac{m(m^2-1)(m^2-3^2)}{5!}t^5 - \ldots + (-1)^{(m-1)/2} 2^{m-1} t^m =$$

$$= \sum_{j=0}^{(m-1)/2} (-1)^j \cdot \frac{m(m^2-1^2)(m^2-3^2)\ldots(m^2-(2j-1)^2)}{(2j+1)!} \cdot t^{2j+1}$$

[En effet, soit

$$f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$$

une solution de (b). Alors:

$$0 = (1-t^2) \sum_{i=2}^{\infty} i(i-1) a_i t^{i-2} - t \sum_{i=1}^{\infty} i a_i t^{i-1} + m^2 \sum_{i=0}^{\infty} a_i t^i =$$

$$= \sum_{i=0}^{\infty} (i+2)(i+1) a_{i+2} t^i - \sum_{i=2}^{\infty} i(i-1) a_i t^i +$$

$$- \sum_{i=1}^{\infty} i a_i t^i + m^2 \sum_{i=0}^{\infty} a_i t^i =$$

$$= 2a_2 + m^2 a_0 + (6a_3 - a_1 + m^2 a_1) \cdot t +$$

$$+\sum_{i=2}^{\infty}\Big\{(i+2)(i+1)a_{i+2}-i(i-1)a_i-ia_i+m^2a_i\Big\}\cdot t^i,$$

d'où:

$$2a_2+m^2a_0=0,\ \text{i.e. } a_2=-m^2a_0/2;$$

$$6a_3+(m^2-1)a_1=0,\ \text{i.e. } a_3=-(m^2-1)a_1/6$$

et

$$(i+2)(i+1)a_{i+2}+\big(m^2-i^2)\big)a_i=0,$$

i.e.

$$a_{i+2}=-\frac{m^2-i^2}{(i+2)(i+1)}\cdot a_i,\ i\geq 2$$

Maintenant on rémarque que chez $f(t)=f_m(t)$, $a_0=f_m(0)=0$ et $a_1=f'_m(0)=m$, d'où la formule (c) est immédiate.]

(d) On note que si $m\in\mathbb{C}-\{0,\pm1,\pm3,\dots\}$ alors on obtient comme $f_m(t)$ une série infinie:

$$f_m(t)==\sum_{j=0}^{\infty}(-1)^j\cdot\frac{m(m^2-1^2)(m^2-3^2)\dots(m^2-(2j-1)^2)}{(2j+1)!}\cdot t^{2j+1}$$

Montrer que cette série converge absolument si $|t|<1$, uniformément sur chaque disque fermé $|t|\leq r<1$.

[Ceci est une conséquence immédiate du

Critère de d'Alembert. Si $\sum_{n=0}^{\infty}\ b_n$ est une série telle qu'il existent $r<1$ et n_0 tels que

$$\frac{|b_n|}{|b_{n+1}|}\leq r$$

pour $n\geq n_0$, alors cette série converge absolument.]

2.24. *Exercice.* Soit toujours m un entier impair, $m\geq 1$.

(a) Soit $\zeta=e^{2\pi i/m}$. Montrer que

$$u^m-v^m=\prod_{b=0}^{m-1}(\zeta^bu-\zeta^{-b}v)$$

(b) Soit $f(t)=e^{2\pi it}-e^{-2\pi it}$. Montrer que

$$f(mt)=f(t)\prod_{a=1}^{(m-1)/2}f(t-a/m)f(t+a/m)$$

(c) En déduire le lemme 2.22.

2.25. *Lemme.* Sous les hypothèses 2.18,

$$(\frac{a}{p})=\prod_{s\in S}\frac{\sin(2\pi as/p)}{\sin(2\pi s/p)}$$

En effet, pour chaque $s \in S$, $as = e_s(a)s_a$, d'où

$$\sin(2\pi as/p) = e_s(a)\sin(2\pi s_a/p)$$

En faisant le produit sur $s \in S$, on a, par le lemme de Gauss,

$$(\frac{a}{p}) = \prod_{s\in S} e_s(a) = \prod_{s\in S} \frac{\sin(2\pi as/p)}{\sin(2\pi s/p)},$$

en tenant compte de ce que $s \mapsto s_a$ est une bijection, cqfd.

2.26. *Une démonstration de 2.7.* Soient ℓ, p deux nombres premiers distincts impairs. Prenons $S = \{1, \dots, (p-1)/2\}$, $T = \{1, \dots, (\ell-1)/2\}$. On a

$$(\frac{\ell}{p}) = \prod_{s\in S} \frac{\sin(2\pi \ell s/p)}{\sin(2\pi s/p)} =$$

$$= \prod_{s\in S} (-4)^{(\ell-1)/2} \prod_{t\in T} (\sin^2(2\pi s/p) - \sin^2(2\pi t/\ell)) =$$

$$= (-4)^{(\ell-1)(p-1)/4} \prod_{s,t} (\sin^2(2\pi s/p) - \sin^2(2\pi t/\ell))$$

En permutant les rôles de ℓ et p, on obtient

$$(\frac{\ell}{p}) = (-1)^{(\ell-1)(p-1)/4} (\frac{p}{\ell}),$$

cqfd.

Un théorème de Fermat

2.27. *Exercice.* (a) Montrer que l'anneau de nombres gaussiens $A = \mathbb{Z}[i]$ est euclidien par rapport à la norme $N(a+bi) = a^2 + b^2$.

(b) Montrer que $x \in A$ est inversible ssi $N(x) = 1$. En conclure que $A^* = \{\pm 1, \pm i\}$.

(c) Un nombre $x \in A$ est dit *premier* si $x = yz$ implique que soit y, soit z est inversible. Si x est premier et $x \not| y$ alors $(x, y) = A$ ("théorème de Bezout"). Si x est premier et $x|(yz)$ alors $x|y$ ou $x|z$.

Soit p un nombre premier dans $\mathbb{Z}$ de la forme $4k+1$.

(d) Il existe $a \in \mathbb{Z}$ tel que $a^2 + 1 \equiv 0 (\mathrm{mod} p)$.

(e) p est n'est pas premier dans A.

En effet, si a est comme dans (d), alors $p|(a^2+1) = (a+i)(a-i)$. Si p etait premier alors il diviserait soit $a+i$, soit $a-i$. Par exemple, si $p|(a+i)$ alors $a + i = p(a' + b'i)$ ce qui est évidemment impossible.

(f) Il existent $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

En effet, d'après (e), $p = xy$ avec x, y non-inversibles. En prenant la norme, $p^2 = N(x)N(y)$ avec $N(x), N(y) > 1$, d'où $p = N(x) = N(y)$.

§3. Formule de produit de Gauss

3.1. Cf. [G]. On pose

$$(m,\mu)=\frac{(1-x^m)(1-x^{m-1})\cdot\ldots\cdot(1-x^{m-\mu+1})}{(1-x)(1-xx)\cdot\ldots(1-x^\mu)}\in\mathbb{C}(x)$$

("les coéfficients x-binomiaux"). Ici $\mu\in\mathbb{N},\ m\in\mathbb{Z}$.

Exemples: $(m,0)=1$;

$$(-1,\mu)=\prod_{i=1}^{\mu}\ \frac{1-x^{-i}}{1-x^i}=(-1)^\mu x^{-\mu(\mu+1)/2}$$

En géneral, $(-m,\mu)\in\mathbb{C}[x^{-1}]$, et à la limite

$$(-\infty,\mu):=\lim_{m\to\infty}(-m,\mu)=\frac{1}{(1-x)(1-xx)\cdot\ldots\cdot(1-x^\mu)}\in\mathbb{C}[[x^{-1}]]\qquad(3.1.1)$$

Si $m\in\mathbb{N}$, $(m,\mu)=0$ si $\mu>m$, et

$$(m,\mu)=(m,m-\mu)$$

3.2. On a

$$(m,\mu)=(m-1,\mu)+x^{m-\mu}(m-1,\mu-1)\qquad(3.2.1)$$

Il s'en suit que si $m\in\mathbb{N},\ m>\mu+1$, alors

$$(m,\mu+1)=\sum_{i=0}^{m-\mu-1}\ (\mu+i,\mu)x^i$$

On en déduit par recurrence sur μ que (m,μ) est un polynôme en x si $m\in\mathbb{N}$.

3.3. On pose

$$f(x,m)=1-\frac{1-x^m}{1-x}+\frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-xx)}-\ldots=\sum_{\mu=0}^{\infty}(-1)^\mu(m,\mu)$$

Si $m\in\mathbb{N}$, la somme est finie:

$$f(x,m)=\sum_{\mu=0}^{m}(-1)^\mu(m,\mu)\in\mathbb{C}[x]$$

Par contre, $f(x,-m)\in\mathbb{C}[[x^{-1}]]$, et

$$f(x,-\infty):=\lim_{m\leftarrow\infty}f(x,-m)=\sum_{\mu=0}^{\infty}\frac{1}{\prod_{i=1}^{\mu}(1-x^i)}\in\mathbb{C}[[x^{-1}]],\qquad(3.3.1)$$

cf. (3.1.1).

On a $f(x,0)=1,\ f(x,1)=0$.

3.4. Il découle de (3.2.1):

$$(m,0)=1$$
$$-(m,1)=-(m-1,1)-x^{m-1}$$
$$(m,2)=(m-1,2)+x^{m-2}(m-1,1),\ \text{etc.},$$

d'où

$$f(x,m)=\sum_{i=0}^{\infty}(-1)^i(1-x^{m-1-i})(m-1,i)$$

Par contre,

$$(1-x^{m-1-i})(m-1,i)=(1-x^{m-1})(m-2,i),$$

d'où

$$f(x,m)=(1-x^{m-1})f(x,m-2) \tag{3.4.1}$$

3.5. Supposons que $m\in\mathbb{N}$. Alors si m est pair (3.4.1) implique que

$$f(x,m)=(1-x)(1-x^3)\cdot\ldots\cdot(1-x^{m-1})=\prod_{j=0}^{(m-2)/2}(1-x^{2j+1}) \tag{3.5.1}$$

Par contre, si m est impair, $f(x,m)=0$ car $f(x,1)=0$.

3.6. Si $m=-2k,\ k\in\mathbb{Z},k>0$, on obtient

$$f(x,-2k)=\frac{1}{(1-x^{-1})(1-x^{-3})\cdot\ldots\cdot(1-x^{-2k+1})}\ \in\mathbb{C}[[x^{-1}]]$$

En passant à la limite pour $k\to\infty$ dans la topologie (x^{-1})-adique, on aura

$$\lim_{k\to\infty}f(x,-2k)=\sum_{i=0}^{\infty}\frac{1}{(x-1)(xx-1)\cdot\ldots\cdot(x^i-1)}=\frac{1}{\prod_{n=0}^{\infty}(1-x^{-2n-1})}$$

De même,

$$f(x,-2k-1)=\frac{f(x,-1)}{(1-x^{-2})(1-x^{-4})\ldots(1-x^{-2k})}$$

où

$$f(x,-1)=1+x^{-1}+x^{-3}+x^{-6}+\ldots=\sum_{n=0}^{\infty}x^{-n(n+1)/2},$$

d'où

$$\lim_{k\to\infty}f(x,-2k-1)=\frac{f(x,-1)}{\prod_{k=1}^{\infty}(1-x^{-2k})}$$

Or, les deux limites coïncident (cf. (3.3.1)):

$$\lim_{k\to\infty}f(x,-2k)=\lim_{k\to\infty}f(x,-2k-1)=\lim_{n\to\infty}f(x,-n)=:f(x,-\infty),$$

d'où

$$f(x,-1) = 1 + x^{-1} + x^{-3} + x^{-6} + \ldots = \frac{(1-x^{-2})(1-x^{-4})\cdot\ldots}{(1-x^{-1})(1-x^{-3})\cdot\ldots},$$

ou bien

$$\sum_{n=0}^{\infty} x^{n(n+1)/2} = 1 + x + x^3 + x^6 + \ldots = \frac{(1-xx)(1-x^4)\cdot\ldots}{(1-x)(1-x^3)\cdot\ldots} \in \mathbb{C}[[x]], \quad (3.6.1)$$

les deux cotés convergent pour $|x| < 1$.

On peut récrire

$$\sum_{n=0}^{\infty} x^{n(n+1)/2} = \frac{1}{2} \sum_{n=-\infty}^{\infty} x^{n(n+1)/2}$$

et

$$\frac{\prod_{i=1}^{\infty}(1-x^{2i})}{\prod_{i=1}^{\infty}(1-x^{2i-1})} = \frac{\prod_{i=1}^{\infty}(1-x^{2i})^2}{\prod_{i=1}^{\infty}(1-x^i)} =$$

$$= \frac{\prod_{i=1}^{\infty}(1+x^i)^2(1-x^i)^2}{\prod_{i=1}^{\infty}(1-x^i)} = \prod_{i=1}^{\infty}(1+x^i)^2(1-x^i),$$

donc

$$\frac{1}{2} \sum_{n=-\infty}^{\infty} x^{n(n+1)/2} = \prod_{i=1}^{\infty}(1+x^i)^2(1-x^i),$$

ce qui est une formule standarte de la théorie des fonctions theta, cf. Jacobi, Fund., no. 66, (4); [W], p. I, ch. IV, §9, (28).

Plus généralement, pour tous $m \in \mathbb{Z}$, on obtient

$$f(x,m) = f(x,-\infty)(1-x^{m-1})(1-x^{m-3})\cdot\ldots = \frac{(1-x^{m-1})(1-x^{m-3})\cdot\ldots}{(1-x^{-1})(1-x^{-3})\cdot\ldots}$$

3.7. Maintenant soit n un entier positif impair; posons $m = n-1$, et soit r une racine primitive de l'équation $x^n = 1$; posons $x = r$. On a

$$(n-1,\mu) = \frac{(1-r^{n-1})(1-r^{n-2})\cdot\ldots\cdot(1-r^{n-\mu})}{(1-r)(1-rr)\cdot\ldots\cdot(1-r^{\mu})}$$

Or:

$$\frac{1-r^{n-i}}{1-r^i} = \frac{1-r^{-i}}{1-r^i} = -r^{-i},$$

d'où

$$(n-1,\mu) = (-1)^{\mu} r^{-\mu(\mu+1)/2}$$

Donc

$$f(r,n-1) = 1 + r^{-1} + r^{-3} + r^{-6} + \ldots r^{-n(n-1)/2} = (1-r)(1-r^3)\cdot\ldots\cdot(1-r^{n-2}), \quad (3.7.1)$$

par (3.3.1).

3.8. On peut remplacer dans (3.7.1) r par n'importe quel r^λ où $(\lambda, n) = 1$; par exemple par r^{-2}:

$$\sum_{i=0}^{n-1} r^{i(i+1)} = 1 + r^2 + r^6 + r^{12} + \ldots + r^{n(n-1)} =$$

$$= (1 - r^{-2\cdot 1})(1 - r^{-2\cdot 3}) \cdot \ldots \cdot (1 - r^{-2(n-2)}) \tag{3.8.1}$$

Soit $n = 2k + 1$; on a

$$1 + 3 + 5 + \ldots + (2k - 1) = k^2,$$

i.e.

$$1 + 3 + \ldots + (n - 2) = \frac{(n-1)^2}{4}$$

Multiplions les deux côtés de (3.8.1) par

$$1 \cdot r \cdot r^3 \cdot \ldots \cdot r^{n-2} = r^{(n-1)^2/4}$$

Rémarquons que

$$i(i + 1) + \frac{(n-1)^2}{4} \equiv \frac{(n - 2i - 1)^2}{4} \pmod{n},$$

donc à gauche on obtient

$$r^{k^2} + r^{(k-1)^2} + \ldots + r + 1 + r + r^2 + \ldots + r^{k^2} = \sum_{i=0}^{n-1} r^{i^2}$$

car $i^2 \equiv (n - i)^2 \pmod{n}$. Il s'en suit que

$$1+r+r^2+\ldots+r^{(n-1)^2} = (r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\cdot\ldots\cdot(r^{n-2}-r^{-n+2}) \tag{3.8.2}$$

3.9. Soit p un nombre premier impair, $p = 2k + 1$, $\zeta = e^{2\pi i/p}$. Considérons la somme de Gauss

$$g(\zeta) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\zeta^a = \sum_{\rho \in R} \zeta^\rho - \sum_{\nu \in N} \zeta^\nu,$$

où R (resp. N) est l'ensemble des résidus (resp. des non-résidus) quadratiques. Puisque

$$1 + \sum_{\rho \in R} \zeta^\rho + \sum_{\nu \in N} \zeta^\nu = \sum_{a=0}^{p-1} \zeta^a = 0,$$

on a

$$g(\zeta) = 1 + 2\sum_{\rho \in R} \zeta^\rho = \sum_{n=0}^{p-1} \zeta^{a^2}$$

Donc

$$g(\zeta) = \prod_{s\in S} (\zeta^s - \zeta^{-s}) = (2i)^k \prod_{s\in S} \sin\ 2\pi s/p$$

où

$$S = \{1, 3, 5, \dots, 2k-1\}, \quad \mathrm{Card}(S) = k = (p-1)/2$$

Supposons que k est impair, $k = 2j+1$, i.e. $p = 4j+3$. On a

$$S = \{1, 3, 5, \dots, 2j+1\} \coprod \{k+2, k+4, \dots, k+2j\},$$

où $k+2 = p-k+1 \equiv -(k-1) \pmod p$, etc., d'où

$$\prod_{s\in S} \sin\ 2\pi s/p = (-1)^j \prod_{a=1}^{k} \sin\ 2\pi a/p,$$

donc

$$g(\zeta) = (2i)^{2j+1}(-1)^j \prod_{a=1}^{k} \sin\ 2\pi a/p = i2^{(p-1)/2} \prod_{a=1}^{(p-1)/2} \sin\ 2\pi a/p$$

De même, si $k = 2j$, i.e. $p = 4j+1$,

$$g(\zeta) = 2^{(p-1)/2} \prod_{a=1}^{(p-1)/2} \sin\ 2\pi a/p$$

3.9. Dans le produit $\prod_{a=1}^{(p-1)/2} \sin\ 2\pi a/p$, on a $0 < a < p/2$, donc $0 < 2\pi a/p < \pi$, d'où

$$\prod_{a=1}^{(p-1)/2} \sin\ 2\pi a/p > 0$$

D'autre part il est bien connu que $|g(\zeta)|^2 = p$. Il s'en suit que

$$g(\zeta) = \sqrt{p} \quad \text{si } p \equiv 1 \pmod 4$$

et

$$g(\zeta) = i\sqrt{p} \quad \text{si } p \equiv 3 \pmod 4$$

§4. Fonction Γ

4.1. On définit

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt = \int_0^\infty e^{-t}t^s\frac{dt}{t}, \quad \Re(s) > 0$$

Exercice. Montrer que $\Gamma(s+1) = s\Gamma(s)$ et $\Gamma(n) = (n-1)!$ si $n \in \mathbb{N}$.

A partir de l'équation fonctionelle (la première formule), définir le prolongement analytique de $\Gamma(s)$ à une fonction méromorphe sur le plan complexe avec les seuls pôles simples en $s = 0, -1, -2, \ldots$ Calculer les résidus en ces points.

La fonction Beta d'Euler est définie par

$$B(s,t) = \int_0^1 x^{s-1}(1-x)^{t-1}dx, \quad \Re(s), \Re(t) > 0$$

4.2. *Théorème.*

$$B(s,t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$$

Exercice. Démontrer cette formule pour $s, t \in \mathbb{N}$.

Démonstration du théorème (Jacobi, cf. [J]). On a

$$\Gamma(a)\Gamma(b) = \int_0^\infty \int_0^\infty e^{-x-y}x^{a-1}y^{b-1}dxdy$$

On fait le changement de variables $x + y = r,\ x = rw$, donc $0 \le r < \infty$, $0 \le w \le 1$ et $dxdy = rdwdr$, d'où

$$\Gamma(a)\Gamma(b) = \int_0^1 w^{a-1}(1-w)^{b-1}dw \int_0^\infty e^{-r}x^{a+b-1}dr = B(a,b)\Gamma(a+b)$$

4.3. *Exercice.* Rémarquons que

$$e^{-t} = \lim_{n\to\infty} \big(1 - \frac{t}{n}\big)^n,$$

d'où

$$\Gamma(s) = \lim_{n\to\infty} \int_0^n \big(1 - \frac{t}{n}\big)^n t^{s-1}dt \tag{4.3.1}$$

(pour une preuve, cf. 4.3.1 ci-dessous).

En déduire $\Gamma(s)$ comme une valeur limite de B.

En effet,

$$\int_0^n \big(1 - \frac{t}{n}\big)^n t^{s-1}dt =$$

$(u = t/n)$

$$= n^s \int_0^1 (1-u)^n u^{s-1} du$$

Pour $n \in \mathbb{N}$ on a

$$B(n+1,t) = \int_0^1 (1-v)^n v^{t-1} dv = \frac{n!}{t(t+1)\cdot \ldots \cdot (t+n)}$$

et cela est vrai pour tous $t \neq 0, -1, \ldots - n$ (prouver!)

Il en découle que

$$\Gamma(s) = \lim_{n\to\infty} n^s B(n+1,s) = \lim_{n\to\infty} n^s \frac{n!}{s(s+1)\cdot \ldots \cdot (s+n)} =$$

$$= \lim_{n\to\infty} n^s \frac{(n-1)!}{s(s+1)\cdot \ldots \cdot (s+n-1)} \qquad (4.3.2)$$

(*formule d'Euler - Gauss*).

4.3.1. *Exercice.* Preuve de (4.3.1), cf. [WW], 12.2.

(a) Pour tous $0 \leq y < 1$,

$$1 + y \leq e^y \leq (1-y)^{-1}$$

(b) Pour tous $0 \leq \alpha \leq 1$,

$$(1-\alpha)^n \geq 1 - n\alpha$$

(c) Déduire de (a) et (b) que

$$0 \leq e^{-t} - \left(1 - \frac{t}{n}\right)^n \leq n^{-1} t^2 e^{-t}$$

pour tous $0 \leq t < n$.

[En effet, en faisant $y = t/n$ dans (a), on obtient:

$$1 + t/n \leq e^{t/n} \leq (1 - t/n)^{-1},$$

d'où

$$(1 + t/n)^n \leq e^t \leq (1 - t/n)^{-n},$$

et

$$(1 + t/n)^{-n} \geq e^{-t} \geq (1 - t/n)^n,$$

Il s'en suit:

$$0 \leq e^{-t} - (1 - t/n)^n = e^{-t} \cdot \left(1 - e^t \cdot (1 - t/n)^n\right) \leq$$

$$\leq e^{-t} \cdot \left(1 - (1 - t^2/n^2)^n\right)$$

D'une autre part, d'après (b) avec $\alpha = t^2/n^2$, on aura

$$1 - (1 - t^2/n^2)^n \leq t^2/n,$$

d'où le résultat.]

(d) En déduire que

$$\left| \int_0^n \left\{ e^{-t} - \left(1 - \frac{t}{n}\right)^n \right\} \cdot t^{s-1} dt \right| \to 0$$

quand $n \to \infty$.

[En effet, d'après (c),

$$\left| \int_0^n \left\{ e^{-t} - \left(1 - \frac{t}{n}\right)^n \right\} \cdot t^{s-1} dt \right| \leq n^{-1} \int_0^n e^{-t} t^{s+1} dt <\leq n^{-1} \int_0^\infty e^{-t} t^{s+1} dt,$$

ce qui $\to 0$, puisque la dernière intégrale converge.]

(e) En déduire (4.3.1).

4.4. *Exercice.* Calculer $\Gamma(1/2)$.

Solution. On a

$$\Gamma(1/2)^2 = \frac{\Gamma(1/2)\Gamma(1/2)}{\Gamma(1)} = B(1/2, 1/2)$$

Par définition,

$$B(1/2, 1/2) = \int_0^1 x^{-1/2}(1-x)^{-1/2} dx =$$

$(x = u^2)$

$$= 2 \int_0^1 \frac{du}{\sqrt{1 - u^2}} = 2 \arcsin\ 1 = \pi,$$

d'où

$$\Gamma(1/2) = \int_0^\infty e^{-x} x^{-1/2} dx = \sqrt{\pi}$$

On rémarque que

$$\int_0^\infty e^{-x} x^{-1/2} dx = 2 \int_0^\infty e^{-u^2} du = \int_{-\infty}^\infty e^{-u^2} du,$$

donc

$$\int_{-\infty}^\infty e^{-u^2} du = \sqrt{\pi}$$

(l'intégrale de Poisson).

4.5. *Théorème.* On a

$$\Gamma(a)\Gamma(1-a) = \frac{\pi}{\sin\ \pi a}$$

Preuve. Supposons d'abord que $0 < \Re(a) < 1$. Par la formule d'Euler

$$\Gamma(a)\Gamma(1-a) = B(a, 1-a) = \int_0^1 x^{a-1}(1-x)^{-a}dx =$$

$(x = u/(u+1))$

$$= \int_0^\infty \frac{u^{a-1}}{u+1}du = I$$

Nous calculons la dernière intégrale par la formule de Cauchy, cf. [WW], 6.24, Example 1. En effet, considérons intégrale

$$I(r, R) = \int_{C(r,R)} \frac{z^{a-1}}{z+1}dz,$$

où $C(r, R)$ est le contour

$$C(r, R) = \{r \le z \le R\} \cup \{z = Re^{i\theta},\ 0 \le \theta \le 2\pi\} \cup$$

$$\cup\{R \ge z \ge r\} \cup \{z = re^{i\theta},\ 2\pi \ge \theta \ge 0\} =$$

$$= C_1 \cup C_2(R) \cup C_3 \cup C_4(r)$$

Alors

$$I(R, r) = \int_{C_2} + \int_{C_4} + (1-e^{2\pi i(a-1)}) \cdot \int_r^R \frac{u^{a-1}}{u+1}du = 2\pi i\ \mathrm{Res}_{z=-1}\frac{z^{a-1}}{z+1} = 2\pi i \cdot e^{\pi i(a-1)}$$

À la limite

$$\lim_{R\to\infty} \int_{C_2(R)} = \lim_{r\to 0} \int_{C_4(r)} = 0$$

grace à l'hypothèse $0 < \Re(a) < 1$, d'où

$$I = 2\pi i \cdot \frac{e^{\pi i(a-1)}}{1 - e^{2\pi i(a-1)}} = \frac{2\pi i}{e^{-\pi i(a-1)} - e^{\pi i(a-1)}} =$$

$$= \frac{2\pi i}{e^{\pi i a} - e^{-\pi i a}} = \frac{\pi}{\sin\ \pi a}$$

Ceci prouve 4.5 sous l'hypothèse $0 < \Re(a) < 1$; le cas général s'en suit, puisque les deux côtés sont des fonctions méromomorphes de a.

4.6. Soit

$$\omega = 4\int_0^1 \frac{dt}{\sqrt{1-t^4}}$$

Montrer que $\omega = \Gamma(1/4)^2/\sqrt{2\pi}$.

4.7. *Exercice: l'intégrale de Hankel.* Considérons l'intégrale

$$I(s) = \int_{\infty}^{(0+)} (-t)^{s-1} e^{-t} dt$$

Ici $\int_{\infty}^{(0+)} = \int_C$, où C désigne le chemin suivant:

$$C = \{\infty > t \geq \epsilon\} \cup \{t = \epsilon e^{i\theta},\ 0 \leq \theta \leq 2\pi\} \cup \{\epsilon \leq t < \infty\} =$$
$$= C_\epsilon^+ \cup C_\epsilon^0 \cup C_\epsilon^- \tag{4.7.1}$$

En plus,

$$(-t)^{s-1} = e^{(s-1)\log(-t)},$$

où $\log(-t)$ désigne la branche du logarithme qui prend les valeurs réels pour t réel négative.

(i) Montrer que

$$I(s) = -2i \sin \pi s \int_0^{\infty} t^{s-1} e^{-t} dt$$

si $\Re(s) > 0$. (Noter que $-t = te^{-i\pi}$ sur C_ϵ^+, $-t = te^{i\pi}$ sur C_ϵ^-).

Donc

$$\Gamma(s) = -\frac{1}{2i \sin \pi s} \int_{\infty}^{(0+)} (-t)^{s-1} e^{-t} dt$$

On note que $I(s)$ est bien définie pour tous $s \in \mathbb{C}$, c'est une fonction entière; donc on obtient (encore une fois) une définition de $\Gamma(s)$ comme une fonction méromorphe sur $\mathbb{C}$, avec les seules pôles simples en $s \in \mathbb{Z}_{\leq 0}$.

(ii) En déduire que

$$\frac{1}{\Gamma(s+1)} = -\frac{1}{2\pi i} \int_{\infty}^{(0+)} (-t)^{-s-1} e^{-t} dt$$

Prendre dans cette formule $s = n \in \mathbb{N}_+$, remplacer le contour $\int_{\infty}^{(0+)}$ par un cercle autour 0, et comparer avec le developpement taylorien de e^{-t}.

4.8. *Exercice:* formule de rédoublement (Legendre). En employant la formule d'Euler - Gauss (4.3.2), montrer que

$$\pi^{1/2} \Gamma(2s) = 2^{2s-1} \Gamma(s) \Gamma(s + 1/2)$$

Idée. Considérons la fonction

$$\phi(s) = \frac{2^{2s-1} \Gamma(s) \Gamma(s+1/2)}{\Gamma(2s)}$$

Remplacez $\Gamma(s)$ et $\Gamma(s+1/2)$ par l'expression (4.3.2), et $\Gamma(2s)$ — par

$$\lim_{n \to \infty} (2n)^{2s} \frac{(2n-1)!}{2s(2s+1)\dots(2s+2n-1)};$$

en déduisez que $\phi(s)$ ne depend pas de s. Faitez $s = 1/2$ pour conclure.

§5. Fonction ζ de Riemann

5.1. Cf. [R]. On a:

$$\Gamma(s) = \int_0^\infty e^{-x} x^s \frac{dx}{x} = \ (x = ty) \ = n^s \int_0^\infty e^{-ny} y^s \frac{dy}{y},$$

d'où

$$n^{-s} = \frac{1}{\Gamma(s)} \int_0^\infty e^{-ny} y^s \frac{dy}{y}$$

Il s'en suit:

$$\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s} = \frac{1}{\Gamma(s)} \sum_{n=1}^\infty \int_0^\infty e^{-ny} y^{s-1} dy =$$

$$= \frac{1}{\Gamma(s)} \int_0^\infty \sum_{n=1}^\infty e^{-ny} y^{s-1} dy = \frac{1}{\Gamma(s)} \int_0^\infty \frac{y^{s-1}}{e^y - 1} dy,$$

$\Re(s) > 1$. Pour justifier la permutation de la sommation et l'intégration, il suffit de montrer que: soit (a) $\int_0^\infty \sum_{n=1}^\infty |e^{-ny} y^{s-1}| dy < \infty$, soit (b) $\int_0^\infty \sum_{n=1}^\infty |e^{-ny} y^{s-1}| dy < \infty$. En effet, on voit facilement que les deux assertions soient vraies sous l'hypothèse $\Re(s) > 1$.

5.2. *Intégral de Hankel.* Considérons l'intégral

$$I(s) = \int_\infty^{(0+)} \frac{(-x)^{s-1}}{e^x - 1} dx,$$

où $(-x)^{s-1} = e^{(s-1)\log(-x)}$, la branche de $\log(-x)$ étant choisie de telle façon que pour $x \in \mathbb{R}_{<0}$, $\log(-x)$ est réel.

Alors il est facile à voir que

$$\int_\infty^{(0+)} \frac{(-x)^{s-1}}{e^x - 1} dx = (e^{i\pi(s-1)} - e^{-i\pi(s-1)}) \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx = -2i \sin \pi s \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx$$

si $\Re(s) > 1$. Autrement dit,

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx = \frac{I(s)}{2i \sin \pi s \Gamma(s)} =$$

(car $\Gamma(s)\Gamma(1-s) = \pi / \sin \pi s$)

$$= -\frac{\Gamma(1-s)}{2\pi i} \int_\infty^{(0+)} \frac{(-x)^{s-1}}{e^x - 1} dx \qquad (5.2.1)$$

Par contre, l'intégrale $I(s)$ est une fonction entière sur le plan complexe $s \in \mathbb{C}$; donc $\zeta(s)$ est bien définie comme une fonction méromorphe avec les seuls pôles possibles en $s = 1, 2, 3, \ldots$. La définition de $\zeta(s)$ par la série montre qu'elle n'a pas de pôles en $s = 2, 3, 4, \ldots$.

Par contre, pour $s \to 1$, $\zeta(s) \to \infty$, donc $\zeta(s)$ a un pôle simple en $s = 1$ (car $\Gamma(1-s)$ a un pôle simple en $s = 1$).

5.3. *Nombres de Bernoulli* sont définis par une série génératrice:

$$\frac{x}{e^x - 1} = \sum_{n=1}^{\infty} \frac{B_n}{n!} x^n,$$

Exercice. Montrer que $B_{2n+1} = 0$ pour $n > 0$.

Voici quelques premières valeurs:

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},$$

$$B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30},\ B_{10} = \frac{5}{66},\ B_{12} = -\frac{691}{2730}$$

5.4. *Polynômes de Bernoulli.* On définit les polynômes $B_n(t)$ ($n \geq 0$) par la série génératrice:

$$\frac{xe^{tx}}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n(t)}{n!} \cdot x^n$$

Exercice. Montrez que: (i)

$$B_n(t) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} t^k$$

(ii) $B_n'(t) = nB_{n-1}(t)$

(iii) $B_n(t+1) - B_n(t) = nt^{n-1}$. En déduire que

$$\sum_{i=1}^{k} i^n = \frac{B_{n+1}(k+1) - B_{n+1}(0)}{n+1} \tag{5.4.1}$$

Considérez les cas $n = 1, 2$ explicitement.

(iv) $\sum_{m=0}^{n-1} \binom{n}{m} B_m = 0$ pour $n > 1$, ce qui permet de calculer les B_n par recurrence. (Utilisez (iii) avec $t = 0$).

5.5. *Valeurs en entiers negatifs.* Maintenant mettons $s = -n$ dans (5.2.1), $n \in \mathbb{N}$. Alors le contour $\int_{\infty}^{(+0)}$ se ferme, d'où

$$\zeta(-n) = (-1)^n \Gamma(n+1) \int_{|x|=\epsilon} \frac{x^{-n-1}}{e^x - 1} dx =$$

$$= (-1)^n n! \cdot \mathrm{res}_{x=0} \left(\frac{1}{x^{n+2}} \cdot \frac{x}{e^x - 1} \right) = (-1)^n n! \cdot \frac{B_{n+1}}{(n+1)!} = (-1)^n \cdot \frac{B_{n+1}}{n+1}, \tag{5.5.1}$$

cf. (5.4.1). Voici quelques exemples:

$$\zeta(0) = \sum_{n=1}^{\infty} 1 = -\frac{1}{2},\ \zeta(-1) = \sum_{n=1}^{\infty} n = -\frac{1}{12},\ \zeta(-3) = \sum_{n=1}^{\infty} n^3 = \frac{1}{120}$$

(une sommation de séries divergentes...). Par contre, $\zeta(-2n) = 0$ si $n > 0$.

5.6. *Equation fonctionelle.* Ce qui est plus populaire (dépuis Euler...), ce sont les expressions de $\zeta(2n)$ pour n positif en termes de nombres de Bernoulli. Par exemple, tous le monde sait que $\zeta(2) = \sum n^{-2} = \pi^2/6$. Dans l'approche de Riemann ils sont des conséquences de l'équation fonctionelle pour la fonction $\zeta(s)$.

Fixons un petit $\epsilon > 0$. Pour $m \in \mathbb{Z}, m \geq 1$, considérons le contour (cf. 4.7.1)):

$$C(R_m) = \{R_m \geq x \geq \epsilon\} \cup \{x = \epsilon e^{i\theta},\ 0 \leq \theta \leq 2\pi\} \cup \{\epsilon \leq x \leq R_m\} \cup \{x = R_m e^{i\theta}, 2\pi \geq \theta \geq 0\} =$$

$$= C'(R_m) \cup C''(R_m),\ C''(R_m) = \{x = R_m e^{i\theta}, 2\pi \geq \theta \geq 0\},$$

où $R_m = \pi(2m + 1)$.

On considère l'intégrale (cf. (5.2.1)):

$$I(s; R_m) = -\frac{\Gamma(1-s)}{2\pi i} \int_{C(R_m)} f(x,s)dx,\ f(x,s) = \frac{(-x)^{s-1}}{e^x - 1},$$

la branche de $f(x, s)$ étant fixée comme en 5.2. D'après (5.2.1),

$$\lim_{m\to\infty} -\frac{\Gamma(1-s)}{2\pi i} \int_{C'(R_m)} f(x,s)dx = \zeta(s)$$

D'une autre part,

$$\left| \int_{C''(R_m)} f(x,s)dx \right| \leq \int_{C''(R_m)} \frac{|(-x)^{s-1}|}{|e^x - 1|} dx \leq C R_m^{\sigma} \int_{C''(R_m)} \frac{1}{|e^x - 1|} dx$$

où $\sigma = \Re(s)$.

5.6.1. *Lemme.* Il existe une constante $\epsilon > 0$ telle que

$$|e^x - 1| > \epsilon$$

pour tous $x \in C''_m$ et tous m.

Preuve. L'application exponentielle e^x définit un homéomorphisme $p : \mathbb{C}/2\pi i\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^*$. Choisissons $\delta > 0$ tel que

$$D_\delta + 2\pi i\mathbb{Z} \cap \left(\cup_{m=1}^{\infty}\ C''(R_m)\right) = \emptyset,$$

où $D_\delta = \{z|\ |z| < \delta\}$. Alors $p(D_\delta)$ est un voisinage de 1, donc il existe $\epsilon > 0$ tel que $D_\epsilon \subset p(D_\delta)$.

On a $p^{-1}(D_\epsilon) \subset D_\delta + 2\pi i_B Z$, donc $p(C''(R_m)) \subset \mathbb{C} - D_\epsilon$ pour tout m, i.e. pour tout m et tout $x \in C''(R_m)$, on a $|e^x - 1| > \epsilon$, QED.

Corollaire. Si $\Re(s) < 0$, alors

$$\lim_{m\to\infty} -\frac{\Gamma(1-s)}{2\pi i} \int_{C''(R_m)} f(x,s)dx = 0$$

D'autre part, on peut évaluer $I(s;R)$ par la formule des résidus de Cauchy: la fonction $f(x,s)$ a des pôles simples en $x = 2\pi in,\ n \in \mathbb{Z}$, avec les résidus

$$\mathrm{res}_{x=2\pi in}\frac{(-x)^{s-1}}{e^x-1} = (-2\pi in)^{s-1} = (2\pi n)^{s-1}e^{-\pi i(s-1)/2},$$

donc

$$I(s;R_m) = -\Gamma(1-s)\cdot\sum_{n=1}^{m}\{\mathrm{res}_{x=2\pi in}f(x;s) + \mathrm{res}_{x=-2\pi in}f(x;s)\} =$$

$$= (2\pi)^{s-1}\Gamma(1-s)2\sin(\pi s/2)\sum_{n=1}^{m} n^{s-1}$$

Il s'en suit que si $\Re(s) < 0$, alors

$$\lim_{m\leftarrow\infty} I(s;R_m) = 2^s\pi^{s-1}\Gamma(1-s)\sin(\pi s/2)\zeta(1-s)$$

On a démontré:

5.7. *Théorème* (Riemann). La fonction $\zeta(s)$ satisfait à l'eqüation fonctionelle

$$\zeta(s) = 2^s\pi^{s-1}\Gamma(1-s)\sin(\pi s/2)\zeta(1-s)$$

En effet, on a montré tout-à-l'heure que cette équation est satisfaite pour $\Re(s) < 0$ donc pour tous s car les deux côtés sont des fonctions méromorphes.

Des cas particuliers de 5.7 ont été connus déjà à Euler, [E], (a).

En utilisant les propriétés standartes de la fonction Γ, on peut donner, avec Riemann, une réformulation plus symétrique de 5.7. Rappelons que l'on a:

$$\frac{\sin(\pi s/2)}{\pi} = \frac{1}{\Gamma(s/2)\Gamma(1-s/2)}$$

et d'un autre côté,

$$\pi^{1/2}\Gamma(1-s) = 2^{-s}\Gamma((1-s)/2)\Gamma(1-s/2),$$

cf. 4.8. Il s'en suit:

5.8. *Théorème.* Définissons

$$\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$$

Alors

$$\xi(s) = \xi(1-s)$$

5.9. Si l'on met $s = 1-2n$ dans 5.7, et se rappelle (5.5.1), on obtient la formule celebre:

$$\zeta(2n) = (-1)^{n+1}\frac{2^{2n-1}B_{2n}}{(2n)!}\cdot\pi^{2n},$$

$n \geq 0$ (Euler).

Exercice. Montrer que

$$(-1)^{n-1} B_{2n} = 4n \int_0^\infty \frac{t^{2n-1}}{e^{2\pi t} - 1} dt$$

pour $n \geq 1$ (utiliser 5.1).

Formule sommatoire de Poisson

5.10. Considérons l'intégrale

$$\int_{C_N} \frac{e^{-\pi z^2 t}}{e^{2\pi i z} - 1} dz = \int_{C_N} \phi(z,t) dz$$

où C_N est le rectangle avec les sommets $\pm N + \frac{1}{2} \pm i$ orienté positivement, N étant un nombre entier, $N > 0$, t une variable complexe, $\Re(t) > 0$.

On a

$$\lim_{N\to\infty} \int_{C_N} \phi(z,t) dz = \left[\int_{-\infty-i}^{\infty-i} - \int_{-\infty+i}^{\infty+i} \right] \phi(z,t) dz =$$

par la formule de Cauchy

$$= \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t} =: \psi(t)$$

5.11. D'une autre part, sur la droite $z = u - i,\ -\infty < u < \infty$

$$\phi(z,t) = \frac{e^{-\pi z^2 t}}{e^{2\pi i z} - 1} = e^{-2\pi i z} \frac{e^{-\pi z^2 t}}{1 - e^{-2\pi i z}} =$$

$$= e^{-\pi z^2 t} \sum_{n=1}^{\infty} e^{-2\pi i n z} = \sum_{n=1}^{\infty} e^{-\pi z^2 t - 2\pi i n z} =$$

$$= \sum_{n=1}^{\infty} e^{-\pi t[(z+in/t)^2 - n^2/t^2]},$$

la série convergeant uniformement. Il s'en suit

$$\int_{-\infty-i}^{\infty-i} \phi(z,t) dz = \sum_{n=1}^{\infty} e^{-\pi n^2/t} \int_{-\infty-i}^{\infty-i} e^{-\pi t(z+in/t)^2} dz =$$

$$= \sum_{n=1}^{\infty} e^{-\pi n^2/t} \int_{-\infty-i}^{\infty-i} e^{-\pi t z^2} dz = \sum_{n=1}^{\infty} e^{-\pi n^2/t} \int_{-\infty}^{\infty} e^{-\pi t(u-i)^2} du =$$

$$= \sum_{n=1}^{\infty} e^{-\pi n^2/t} \int_{-\infty}^{\infty} e^{-\pi t u^2} du$$

Supposons que t et réel, $t > 0$. Alors (en posant $v = (\pi t)^{1/2}u$)

$$\int_{-\infty}^{\infty} e^{-\pi t u^2} du = (\pi t)^{-1/2} \int_{-\infty}^{\infty} e^{-v^2} dv = t^{-1/2},$$

donc ceci est vrai pout tous $t, \Re t > 0$. Donc

$$\int_{-\infty-i}^{\infty-i} \phi(z,t)dz = t^{-1/2} \sum_{n=1}^{\infty} e^{-\pi n^2/t}$$

De même,

$$\int_{-\infty+i}^{\infty+i} \phi(z,t)dz = -t^{-1/2} \sum_{n=0}^{\infty} e^{-\pi n^2/t};$$

on en déduit

$$\psi(t) = t^{-1/2} \sum_{n=-\infty}^{\infty} e^{-\pi n^2/t} = t^{-1/2}\psi(t^{-1})$$

5.12. Plus généralement, soit $f(z)$ une fonction entière qui satisfait à l'hypothèse suivante:

quelque soient $N \in \mathbb{Z}_{>0}$ et un sous-ensemble compact $K \subset \mathbb{R}$, en posant $z = x + iy$, on a: $\lim_{x\to\pm\infty} |x^N f(z)| = 0$ uniformement par rapport à $y \in K$.

Posons

$$\phi(z) = \frac{f(z)}{e^{2\pi i z} - 1}$$

Alors

$$\left[\int_{-\infty-i}^{\infty-i} - \int_{-\infty+i}^{\infty+i}\right] \phi(z)dz = \lim_{N\to\infty} \int_{C_N} \phi(z)dz = \sum_{n=-\infty}^{\infty} f(n)$$

par la formule de Cauchy.

D'un autre côté,

$$\frac{f(z)}{e^{2\pi i z} - 1} = e^{-2\pi i z} \frac{f(z)}{1 - e^{-2\pi i z}} = \sum_{n=1}^{\infty} f(z)e^{-2\pi i n z}$$

sur la droite $C_- = \{u - i,\ -\infty < u < \infty\}$, d'où

$$\int_{-\infty-i}^{\infty-i} \phi(z)dz = \sum_{n=1}^{\infty} \int_{-\infty}^{\infty} f(u)e^{-2\pi i n u} du = \sum_{n=1}^{\infty} \hat{f}(-n),$$

où l'on pose

$$\hat{f}(t) := \int_{-\infty}^{\infty} f(u)e^{2\pi i t u} du$$

De même,

$$\int_{-\infty+i}^{\infty+i} \phi(z)dz = -\sum_{n=0}^{\infty} \hat{f}(n)$$

Il s'en suit,

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n)$$

Deuxième preuve de Riemann de l'équation fonctionelle

5.13. On part de l'intégrale

$$\Gamma(s/2) = \int_0^\infty x^{s/2-1} e^{-x} dx =$$

$(x = \pi n^2 y)$

$$= \pi^{-s/2} n^s \int_0^\infty y^{s/2-1} e^{-\pi n^2 y} dy,$$

d'où:

$$\xi(s) = \pi^{-s/2}\Gamma(s/2) \sum_{n=1}^{\infty} n^{-s} = \int_0^\infty x^{s/2-1} \cdot \sum_{n=1}^{\infty} e^{-\pi n^2 x} dx = \int_0^\infty x^{s/2-1} \cdot \tilde{\psi}(x) dx, \tag{5.13.1}$$

où

$$\tilde{\psi}(x) = \sum_{n=1}^{\infty} e^{-\pi n^2 x},$$

donc

$$\psi(x) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 x} = 1 + 2\tilde{\psi}(x)$$

5.14. Maintenant on découpe l'intégrale (5.13.1) en deux:

$$\int_0^\infty x^{s/2-1} \cdot \tilde{\psi}(x) dx = \int_0^1 x^{s/2-1} \cdot \tilde{\psi}(x) dx + \int_1^\infty x^{s/2-1} \cdot \tilde{\psi}(x) dx,$$

où la première, après le changement de variable $x = 1/y$, deviendra:

$$\int_0^1 x^{s/2-1} \cdot \tilde{\psi}(x) dx = -\int_\infty^1 y^{-s/2-1} \tilde{\psi}(1/y) dy$$

Or, l'équation fonctionelle

$$x^{1/2}(1 + 2\tilde{\psi}(x)) = 1 + 2\tilde{\psi}(1/x)$$

fournit:

$$\tilde{\psi}(1/x) = x^{1/2}\tilde{\psi}(x) + \frac{x^{1/2} - 1}{2},$$

d'où:

$$-\int_\infty^1 y^{-s/2-1} \tilde{\psi}(1/y) dy = \int_1^\infty y^{-s/2-1/2} \tilde{\psi}(y) dy + \frac{1}{2} \int_1^\infty \left(y^{-s/2-1/2} - y^{-s/2-1}\right) dy$$

Ici:

$$\frac{1}{2}\int_1^\infty (y^{-s/2-1/2}-y^{-s/2-1})dy = \frac{1}{2}\left(\frac{y^{-s/2+1/2}}{-(s-1)/2}-\frac{y^{-s/2}}{-s/2}\right)\Big|_1^\infty = \frac{1}{s(s-1)}$$

si $\Re(s) < -1$.

Il s'en suit:

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) = -\frac{1}{s(1-s)} + \int_1^\infty \left(x^{s/2-1}+x^{(1-s)/2-1}\right)\cdot\tilde{\psi}(x)dx, \quad (5.14.1)$$

si $\Re(s) < -1$. Par contre, l'intégrale à droite est une fonction entière sur tout le plan complexe, donc (5.14.1) est vrai pour tous s.

Or, l'expression à droite ne change pas si l'on remplace s par $1-s$, d'où

$$\xi(s) = \xi(1-s)$$

Fonction $\Xi(t)$

5.15. *Fonction* $\tilde{\xi}(s)$ *et deux intégrations par parties.* On pose

$$\tilde{\xi}(s) = \frac{s(s-1)}{2}\xi(s) = (s-1)\Gamma(s/2+1)\pi^{-s/2}\zeta(s)$$

L'expression intégrale (5.14.1) entraine:

$$\tilde{\xi}(s) = \frac{1}{2} + \frac{s(s-1)}{2}\int_1^\infty \left(x^{s/2-1}+x^{(1-s)/2-1}\right)\cdot\tilde{\psi}(x)dx$$

Faisons l'intégration par parties:

$$I := \int_1^\infty \left(x^{s/2-1}+x^{(1-s)/2-1}\right)\cdot\tilde{\psi}(x)dx = \tilde{\psi}(x)\cdot\left(\frac{x^{s/2}}{s/2}+\frac{x^{(1-s)/2}}{(1-s)/2}\right)\Big|_1^\infty -$$

$$-\int_1^\infty \tilde{\psi}'(x)\cdot\left(\frac{x^{s/2}}{s/2}+\frac{x^{(1-s)/2}}{(1-s)/2}\right)dx =$$

(puisque $\tilde{\psi}(\infty) = 0$)

$$= \frac{2\tilde{\psi}(1)}{s(s-1)} - \int_1^\infty \tilde{\psi}'(x)\cdot\left(\frac{x^{s/2}}{s/2}+\frac{x^{(1-s)/2}}{(1-s)/2}\right)dx,$$

d'où

$$\tilde{\xi}(s) = \frac{1}{2} + \frac{s(s-1)}{2}I = \frac{1}{2} + \tilde{\psi}(1) + \int_1^\infty \tilde{\psi}'(x)\cdot\left((1-s)x^{s/2}+sx^{(1-s)/2}\right)dx$$

Faisons encore une fois une intégration par parties:

$$I' := \int_1^\infty \tilde{\psi}'(x)\cdot\big((1-s)x^{s/2}+sx^{(1-s)/2}\big)dx = \int_1^\infty x^{3/2}\tilde{\psi}'(x)\cdot\big((1-s)x^{s/2-3/2}+sx^{-s/2-1}\big)dx =$$

$$-x^{3/2}\tilde{\psi}'(x)\cdot\left(2x^{s/2-1/2}+2x^{-s/2}\right)\Big|_1^\infty +$$

$$+\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}\cdot\left(2x^{s/2-1/2}+2x^{-s/2}\right)dx =$$

$$= 4\tilde{\psi}'(1) + 2\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}x^{-1/4}\cdot\left(x^{s/2-1/4}+x^{-s/2+1/4}\right)dx$$

Il s'en suit:

$$\tilde{\xi}(s) = \frac{1}{2} + \tilde{\psi}(1) + 4\tilde{\psi}'(1) + 2\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}x^{-1/4}\cdot\left(x^{s/2-1/4}+x^{-s/2+1/4}\right)dx$$

5.16. *Exercice.* Montrer que $\frac{1}{2} + \tilde{\psi}(1) + 4\tilde{\psi}'(1) = 0$.

Il s'en suit que

$$\tilde{\xi}(s) = 2\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}x^{-1/4}\cdot\left(x^{s/2-1/4}+x^{-s/2+1/4}\right)dx$$

5.17. *Droite critique.* Posons maintenant $s = 1/2 + it$. Alors on aura:

$$x^{s/2-1/4} + x^{-s/2+1/4} = x^{it/2} + x^{-it/2} = 2\cos(t\log x/2),$$

d'où

$$\Xi(t) := \tilde{\xi}(\frac{1}{2} + it) = 4\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}x^{-1/4}\cdot\cos(t\log x/2)dx$$

§6. Développements eulériens de sin et de cotg

6.1. On suit Bourbaki, [B], Chapitre VI, §2.

Lemme. On a pour $n \in \mathbb{Z}$, $n > 0$:

$$\sin nz = 2^{n-1} \prod_{k=0}^{n-1} \sin(z + k\pi/n)$$

En effet,

$$\sin nz = \frac{1}{2i}(e^{inz} - e^{-inz}) = \frac{e^{-inz}}{2i}(e^{2inz} - 1) =$$

$$= \frac{e^{-inz}}{2i} \prod_{p=0}^{n-1} (e^{2iz} - e^{-2\pi ip/n}) = \frac{1}{2i} \prod_{p=0}^{n-1} (e^{iz} - e^{-iz-2\pi ip/n}) =$$

$$= (2i)^{n-1} \prod_{p=0}^{n-1} e^{-\pi ip/n} \prod_{p=0}^{n-1} \frac{e^{iz+\pi ip/n} - e^{-iz-\pi ip/n}}{2i}$$

Or,

$$(2i)^{n-1} \prod_{p=0}^{n-1} e^{-\pi ip/n} = (2i)^{n-1} e^{-\pi i/n \cdot \sum_{p=0}^{n-1} p} = (2i)^{n-1} e^{-\pi i(n-1)/2} = 2^{n-1},$$

d'où l'assertion.

6.2. En divisant par $\sin z$ et en faisant tendre z vers 0, on obtient:

$$\prod_{p=0}^{n-1} \sin(p\pi/n) = n2^{1-n}$$

6.3. Supposons que $n = 2m + 1$ est impair. Alors 6.1 peut s'écrire

$$\sin nz = (-1)^m 2^{n-1} \prod_{p=-m}^{m} \sin(z - p\pi/n) =$$

$$= (-1)^m 2^{n-1} \sin z \prod_{p=1}^{m} \sin(z - p\pi/n) \sin(z + p\pi/n)$$

Or, on vérifie aisément la formule suivante:

$$\sin^2(a + b) - \sin^2(a - b) = \sin 2a \sin 2b,$$

d'où

$$\sin a \sin b = \sin^2((a + b)/2) - \sin^2((a - b)/2)$$

Il s'en suit,

$$\sin(z - p\pi/n)\sin(z + p\pi/n) = \sin^2 z - \sin^2(p\pi/n),$$

d'où

$$\sin nz = 2^{n-1}\sin z \prod_{p=1}^{m} (\sin^2(p\pi/n) - \sin^2 z)$$

Or, d'après 6.2,

$$\prod_{p=1}^{m} \sin^2(p\pi/n) = \frac{n}{2^{n-1}},$$

d'où

$$\sin nz = n\sin z \prod_{p=1}^{m} (1 - (\sin^2 z/\sin^2(p\pi/n)))$$

En remplaçant z par z/n, on arrive au

6.4 *Théorème.* Si $n = 2m + 1$ est impair alors

$$\sin z = n\sin(z/n) \prod_{k=1}^{m} \left(1 - \frac{\sin^2(z/n)}{\sin^2(k\pi/n)}\right)$$

Maintenant si l'on fait m tendre vers l'infini, on obtient

6.5. *Théorème.*

$$\sin z = z \cdot \prod_{k=1}^{\infty} \left(1 - \frac{z^2}{k^2\pi^2}\right)$$

(Convergence uniforme dans des sous-ensembles compacts.)

Preuve (cf. *op. cit.*). On réecrit 6.4 sous une forme

$$\sin z = n\sin(z/n) \prod_{k=1}^{\infty} (1 - w_k(n, z)) \tag{6.5.1}$$

où $w_k(n, z) = \sin^2(z/n)/\sin^2(k\pi/n)$ si $1 \le k \le m$ et $w_k(n, z) = 0$ si $k > m$.

Lemme. Pour tout z contenu dans une partie compacte $K \subset \mathbb{C}$ et pour tous n impaire, la série $\sum_{k=1}^{\infty} w_k(n, z)$ est *normalement convergente* (uniformément par rapport à n et z).

Démonstration. On a

$$\lim_{n\to\infty} n\sin(z/n) = z$$

uniformement dans K, donc il existe $M > 0$ tel que $|n\sin(z/n)| \le M$ pour tout n et tout $z \in K$.

Sous-lemme. Pour $1 \le k \le m$ on a $n\sin(k\pi/n) \ge k\pi/2$.

En effet, pour $4 \ge x \ge 0$ on a $(\sin x)/x \ge 1 - x^2/6$, donc pour $0 \le x \le \pi/2$ on a $(\sin x)/x \ge 1/2$, d'où l'assertion de sous-lemme.

Il s'en suit de sous-lemme que $|w_k(n,z)| \leq 4M^2/k^2\pi^2$ pour tous k et $z \in K$, d'où le lemme en découle.

Le lemme implique qu'on peut faire tendre $n \longrightarrow \infty$ dans (6.5.1); comme pour k fixé, $w_k(n,z)$ tend (uniformément dans K) vers $z^2/k^2\pi^2$, on obtient l'assertion du théorème.

6.6. Prenons la dérivée logarithmique:

$$\text{cotg}z = \frac{1}{z} + \sum_{p=1}^{\infty} \frac{2z}{z^2 - p^2\pi^2} = \frac{1}{z} + \sum_{p=1}^{\infty} \left(\frac{1}{z - p\pi} + \frac{1}{z + p\pi} \right)$$

l'égalité est vraie pour tout $z \in \mathbb{C}$ dinstinct d'un multiple entier de π, la série étant normalement convergente dans tout ensemble compact $K \subset \mathbb{C} - \mathbb{Z}\pi$.

Application aux nombres de Bernoulli

6.7. *Exercice.* Montrer que

$$\frac{z}{e^z - 1} = -\frac{z}{2} + \frac{iz}{2}\text{cotg}(iz/2)$$

On rappelle que le nombres de Bernoulli sont définis par:

$$\frac{z}{e^z - 1} = 1 - \frac{z}{2} + \sum_{n=1}^{\infty} B_{2n} \frac{z^{2n}}{(2n)!}$$

6.8. Le développement de cotg nous dit:

$$\text{cotg } z - \frac{1}{z} = \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2\pi^2}$$

Maintenant:

$$\frac{2z}{z^2 - n^2\pi^2} = -\frac{2z}{n^2\pi^2} \cdot \frac{1}{1 - z^2/n^2\pi^2} = -\frac{2z}{n^2\pi^2} \cdot \sum_{k=0}^{\infty} \frac{z^{2k}}{n^{2k}\pi^{2k}} =$$

$$= -2\sum_{k=1}^{\infty} \frac{z^{2k-1}}{n^{2k}\pi^{2k}}$$

($|z| < \pi$).

Lemme. La série double

$$\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \frac{-2z^{2k-1}}{n^{2k}\pi^{2k}} \tag{6.8.1}$$

est absolument convergente dans le disque ouvert $D = \{|z| < \pi\}$ normalement convergente dans tout compact $K \subset D$, et a pour somme cotg $z - 1/z$.

En effet, pour $|z| \leq a < \pi$, on a

$$\left| \frac{-2z^{2k-1}}{n^{2k}\pi^{2k}} \right| \leq \frac{2a^{2k-1}}{n^{2k}\pi^{2k}}$$

et la somme d'un nombre fini quelconque de termes à droite est $\leq \sum_{n=1}^{\infty} 2a/(n^2\pi^2 - a^2) < \infty$, d'où la convergeance normale. Pour trouver la somme, on fait d'abord la sommation par rapport à k, puis par rapport à n, et l'on trouve

$$\sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2\pi^2} = \operatorname{cotg}\, z - \frac{1}{z}$$

En échangeant l'ordre de sommations, il s'en suit:

$$\operatorname{cotg} z = \frac{1}{z} - 2\sum_{k=1}^{\infty} \frac{\zeta(2k)}{\pi^{2k}} z^{2k-1},$$

où

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$$

Donc

$$\frac{z}{e^z - 1} = -\frac{z}{2} + \frac{iz}{2} \cdot \left(\frac{2}{iz} + 2\sum_{k=1}^{\infty} \frac{\zeta(2k)}{\pi^{2k}} (-1)^k i \frac{z^{2k-1}}{2^{2k-1}} \right) =$$

$$= 1 - \frac{z}{2} + \sum_{k=1}^{\infty} (-1)^{k-1} \frac{\zeta(2k)}{2^{2k-1}\pi^{2k}} z^{2k}$$

6.9. En comparaisant avec 6.7,

$$B_{2n} = (-1)^{n-1}(2n)! \frac{2\zeta(2n)}{(2\pi)^{2n}},$$

ou

$$\zeta(2n) = (-1)^{n-1} \frac{(2\pi)^{2n}}{2(2n)!} B_{2n},$$

$n \geq 1$.

§7. Fonction η de Dedekind et formule de Schlömilch - Ramanujan

7.1. Étant donné un nombre réel $a > 0$, on pose $q := e^{-2\pi a}$; considérons une fonction réelle

$$h(a) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) = e^{-\pi a/12} \prod_{n=1}^{\infty} (1 - e^{-2\pi n a})$$

Il est clair que le produit converge normalement dans chaque compact $K \subset \mathbb{R}_{>0}$.

Notre but principal dans ce chapitre sera une preuve du

Théorème (Dedekind). On a

$$h(1/a) = \sqrt{a} h(a) \tag{7.1.1}$$

Démonstration, d'après Carl Ludwig Siegel, [Sie].

7.2. En prenant le logarithme naturel,

$$-\frac{\pi a}{12} - \log h(a) = -\sum_{n=1}^{\infty} \log(1 - q^n) = \sum_{n,m=1}^{\infty} \frac{q^{nm}}{m} = \sum_{m=1}^{\infty} \frac{1}{m(q^{-m} - 1)}$$

Prenons le logarithme de (7.1.1):

$$\log h(1/a) = \frac{1}{2} \log\ a + \log h(a),$$

ou

$$-\frac{\pi a}{12} - \log h(a) = -\frac{\pi a^{-1}}{12} - \log h(1/a) + \frac{1}{2} \log\ a + \frac{\pi(-a + a^{-1})}{12}$$

Donc (7.1.1) est équivalente à:

$$\frac{1}{2} \log\ a + \frac{\pi(-a + a^{-1})}{12} = \sum_{m=1}^{\infty} \frac{1}{m} \left(\frac{1}{e^{2\pi m a} - 1} - \frac{1}{e^{2\pi m/a} - 1} \right) \tag{7.2.1}$$

7.3. *Une fonction intéressante:* $\operatorname{cotg} z$. On pose $y = e^{iz}$. Alors:

$$\operatorname{cotg} z = \frac{\cos z}{\sin z} = -\frac{(y^{-1} + y)/2}{(y^{-1} - y)/2i} = -i \cdot \frac{y^{-1} + y}{y^{-1} - y} = i \cdot \frac{y + y^{-1}}{y - y^{-1}} =$$

$$= -i \cdot \left(1 + \frac{2}{y^{-2} - 1} \right) = i \cdot \left(1 + \frac{2}{y^2 - 1} \right) \tag{7.3.1}$$

Donc $\lim_{y \to 0} \operatorname{cotg} z = -i$ et $\lim_{y \to \infty} \operatorname{cotg} z = i$. De là:

$$\lim_{n \to \infty} \operatorname{cotg}((n + 1/2)z) = -i \text{ si } \Im z > 0 \tag{7.3.2a}$$

et

$$\lim_{n\to\infty} \operatorname{cotg}((n+1/2)z) = i \text{ si } \Im z < 0 \qquad (7.3.2b)$$

7.4. Posons $\tau = ai$. On définit une fonction $f(z) = \cot z \cot z/\tau$ et on considère la fonction $g_n(z) = z^{-1} f(\nu z)$ où $\nu = (n+1/2)\pi$, $n = 0, 1, \ldots$. Soit C le contour du parallelogramme avec les sommets $1, \tau, -1, -\tau$.

Quels sont les poles de $g_n(z)$? On a:

$$g_n(z) = \frac{\cos \nu z}{z \sin \nu z} \cdot \frac{\cos \nu z/\tau}{\sin \nu z/\tau}$$

Donc on a:

(a) des poles simples en $z = \pm \pi m/\nu$, $m = 1, 2, \ldots$, avec les résidus

$$\operatorname{res}_{z=\pm\pi m/\nu}\ g_n(z) = \frac{\cot(\pi m/\tau)}{\pi m};$$

(b) des poles simples en $z = \pm \pi m\tau/\nu$, $m = 1, 2, \ldots$, avec les résidus

$$\operatorname{res}_{z=\pm\pi m\tau/\nu}\ g_n(z) = \frac{\cot(\pi m\tau)}{\pi m}$$

(c) Enfin, en $z = 0$ on a:

$$g_n(z) = \frac{1}{z} \cdot \frac{1}{\nu z} \cdot \frac{\tau}{\nu z} \cdot \frac{1 - \nu^2 z^2/2 + \ldots}{1 - \nu^2 z^2/6 + \ldots} \cdot \frac{1 - \nu^2 z^2/2\tau^2 + \ldots}{1 - \nu^2 z^2/6\tau^2 + \ldots} =$$

$$= \frac{\tau}{\nu^2 z^3} \cdot \left(1 - \frac{\nu^2 z^2}{3} + \ldots\right) \cdot \left(1 - \frac{\nu^2 z^2}{3\tau^2} + \ldots\right) =$$

$$= \frac{\tau}{\nu^2 z^3} \cdot \left(1 - \frac{\nu^2 z^2}{3} \cdot (1 + \tau^{-2}) + \ldots\right),$$

d'où

$$\operatorname{res}_{z=0}\ g_n(z) = -\frac{\tau + \tau^{-1}}{3}$$

Par la formule des résidus de Cauchy,

$$\frac{1}{2\pi i} \int_C f(\nu z) \frac{dz}{z} = -\frac{\tau + \tau^{-1}}{3} + \frac{2}{\pi} \sum_{m=1}^{n} \frac{1}{m} (\cot \pi m\tau + \cot \pi m/\tau)$$

On rémarque que

$$\cot \pi m\tau + \cot \pi m/\tau = -2i \left(\frac{1}{e^{-2\pi i m\tau} - 1} - \frac{1}{e^{2\pi i m/\tau} - 1} \right),$$

cf. (7.3.1), d'où

$$\int_C f(\nu z) \frac{dz}{z} = -\frac{2\pi i(\tau + \tau^{-1})}{3} + 8 \sum_{m=1}^{n} \frac{1}{m} \left(\frac{1}{e^{-2\pi i m\tau} - 1} - \frac{1}{e^{2\pi i m/\tau} - 1} \right) \quad (7.4.1)$$

7.5. Maintenant faisons n tendre à l'infini dans (7.4.1). Soit $\ell_1 = \{\Im z = 0\}$ et ℓ_2 la droite qui passe à travers 0 et τ. D'après (1.3.2a,b),

$\lim_{n\to\infty} \cot \nu z = -i$ si z est au-dessus de ℓ_1; $\lim_{n\to\infty} \cot \nu z = i$ si z est au-dessous de ℓ_1 et

$\lim_{n\to\infty} \cot \nu z/\tau = i$ si z est à droite de ℓ_2; $\lim_{n\to\infty} \cot \nu z/\tau = -i$ si z est à gauche de ℓ_2.

Il s'en suit que sur le côté $(1, \tau)$ de C (sans les sommets) la valeur limite $\lim_{n\to\infty} \cot \nu z \cot \nu z/\tau = -i \cdot i = 1$.

De même, sur les côtés $(\tau, -1)$, $(-1, -\tau)$ et $(-\tau, 1)$ les valeurs limites sont $-1, 1, -1$.

De là,

$$\lim_{n\to\infty} \int_C f(\nu z)\frac{dz}{z} = \left(\int_1^\tau - \int_\tau^{-1} + \int_{-1}^{-\tau} - \int_{-\tau}^{1}\right)\frac{dz}{z} =$$

$$= \log\tau - \pi + \log\tau + \log(-\tau) - \pi - 2\pi + \log(-\tau) = 4\log\tau - 2\pi = 4\log(\tau/i) \quad (7.5.1)$$

Donc en passant à la limite $n \to \infty$ dans (7.4.1), on obtient:

$$4\log(\tau/i) + \frac{2\pi i(\tau + \tau^{-1})}{3} = 8\sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{1}{e^{-2\pi i m\tau} - 1} - \frac{1}{e^{2\pi i m/\tau} - 1}\right)$$

En divisant cela par 8, on obtient la formule cherchée (7.2.1), QED.

7.6. *Théorème*, [Sch], [Ram].

$$\sum_{n=1}^{\infty} \frac{n}{e^{2\pi n} - 1} = \frac{1}{24} - \frac{1}{8\pi} \tag{7.6.1}$$

7.7. *Démonstration* de Srinivasa Ramanujan, [Ram], (18), p. 32. L'identité (7.1.1) s'écrit:

$$e^{-\pi/12a}\prod_{n=1}^{\infty}(1 - e^{-2\pi n/a}) = \sqrt{a}\cdot e^{-\pi a/12}\prod_{n=1}^{\infty}(1 - e^{-2\pi na})$$

En prénant le logarithme,

$$-\frac{\pi}{12a} + \sum_{n=1}^{\infty}\log(1 - e^{-2\pi n/a}) = \frac{\log a}{2} - \frac{\pi a}{12} + \sum_{n=1}^{\infty}\log(1 - e^{-2\pi na})$$

En prénant la dérivée,

$$\frac{\pi}{12a^2} - \sum_{n=1}^{\infty}\frac{(2\pi n/a^2)\cdot e^{-2\pi n/a}}{1 - e^{-2\pi n/a}} = \frac{1}{2a} - \frac{\pi}{12} + \sum_{n=1}^{\infty}\frac{2\pi n e^{-2\pi n/a}}{1 - e^{-2\pi na}},$$

ou bien

$$\frac{\pi}{12}(a^{-2} + 1) - \frac{1}{2a} = 2\pi\sum_{n=1}^{\infty} n\cdot\left(\frac{a^{-2}}{e^{2\pi n/a} - 1} + \frac{1}{e^{2\pi na} - 1}\right) \tag{7.7.1}$$

Sous une forme plus symétrique,

$$\frac{\pi(a^{-1}+a)}{12}-\frac{1}{2}=2\pi\sum_{n=1}^{\infty}\left(\frac{n/a}{e^{2\pi n/a}-1}+\frac{na}{e^{2\pi na}-1}\right) \tag{7.7.2}$$

Maintenant, si l'on pose $a=1$, on arrive à (7.6.1).