ATS FERMAT

(11) $\beta = 1 - c = 1 - \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = \frac{3}{2} + i\frac{\sqrt{3}}{2}$. $N(\beta) = \left(\frac{3}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{9}{4} + \frac{3}{4} = \frac{12}{4} = \underline{3}$

(12) Si $z \in \mathbb{Z}[c]$, alors $z = a + cb$ où a et $b \in \mathbb{Z}$.

$$N(z) = \left|a + \left(-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}\right)b\right|^2 = \left|\left(a - \tfrac{1}{2}b\right) + i\tfrac{\sqrt{3}}{2}b\right|^2 = \left(a - \tfrac{1}{2}b\right)^2 + \left(\tfrac{\sqrt{3}}{2}b\right)^2 = a^2 - ab + \tfrac{b^2}{4} + \tfrac{3b^2}{4}$$

$$N(z) = a^2 - ab + b^2 \in \mathbb{Z}.$$

De plus $N(z)$ est positif car égal à $|z|^2$, donc $\underline{N(z) \in \mathbb{N}}$

(13) Si $z = a + cb$ et $z' = a' + cb'$, alors

$$zz' = (a+cb)(a'+cb') = aa' + c^2bb' + c(a'b + b'a)$$
$$= aa' + (-1-c)bb' + c(a'b + b'a)$$
$$= aa' - bb' + c(a'b + b'a - bb') \in \mathbb{Z}[c]$$

car zz' est bien de la forme $A + cB$ avec A et $B \in \mathbb{Z}$.

$c^2 = e^{i\frac{4\pi}{3}} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$
$= -1 + \frac{1}{2} - i\frac{\sqrt{3}}{2}$
$= -1 - \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = \underline{-1-c}$

(13) $N(z)N(z') = |z|^2|z'|^2 = |zz'|^2 = N(zz')$

(15) Si $z = a + cb \in \mathbb{Z}[c]$, alors $N(z) = a^2 - ab + b^2$

• Si a et b ont le même signe, alors $N(z) = (a-b)^2 + ab$
$(a-b)^2$ et ab sont > 0. $N(z) = 2 \iff$ ① $a - b = \pm 1$ ou ② $ab = 2$ ou ③ $ab = 0$

① $ab = 1 \Rightarrow a = \pm 1$ et $b = \pm 1$, alors $a - b \neq \pm 1$ impossible

② $a - b = 0 \Rightarrow a = b \Rightarrow a^2 = 2 \Rightarrow a = \pm\sqrt{2}$. Ce n'est pas un entier ! impossible

③ $ab = 0 \Rightarrow a = 0$ ou $b = 0 \Rightarrow a^2 = 2$ ou $b^2 = 2$ impossible

Donc $\boxed{N(z) \neq 2}$

• Si a et b ont un signe opposé, alors a^2, $-ab$ et b^2 sont positifs.

Si $a^2 + (-ab) + b^2 = 2$, alors l'un des trois au moins a^2, $-ab$, ou b^2 est nul

avec $a = 0$, on obtient $N(z) = b^2 = 2$ impossible car $b \in \mathbb{Z}$

avec $b = 0$ $a^2 = 2$ " car $a \in \mathbb{Z}$

Donc $\boxed{N(z) \neq 2}$

(16) Si $z \in \mathbb{Z}(c)$ est inversible, alors il existe z' tel que $zz' = 1$

$N(zz') = 1 = N(z)N(z')$ et $N(z)$ et $N(z')$ sont des entiers naturels, donc $\underline{N(z) = 1}$

$N(3) = 3^2 = 9 \neq 1$, donc 3 n'est pas inversible

(17) $c \cdot c^2 = e^{i\frac{2\pi}{3}} \cdot e^{i\frac{4\pi}{3}} = e^{i\frac{6\pi}{3}} = 1$. De plus, $c^2 = -1 - c \in \mathbb{Z}[c]$, donc $\underline{c \text{ est inversible}}$

et l'inverse de c est c^2.

(18) $N(\beta) = 3 \neq 1$, donc **β n'est pas inversible**

(19) $N(\beta) = 1 \Leftrightarrow a^2 - ab + b^2 = 1$

Si a et b ont le même signe, alors $(a-b)^2 + ab = 1$

Comme $(a-b)^2$ et ab sont des entiers positifs : l'un est nul et l'autre vaut 1

1er cas : $a-b=0$ et $ab=1$ | $a=b$, $ab=1$, a et $b \in \mathbb{Z}$ $\Rightarrow a=b=1$ ou $a=b=-1$ alors **$\beta = \pm(1+c)$**

2e cas : $a-b=1$ et $ab=0$ $\quad a=0$ ou $b=0$ **$\beta = 1$**

Si $a=0$ $b=-1$

Si $b=0$ $a=1$ ou **$\beta = -c$**

Si a et b ont un signe opposé, alors $a^2 + (-ab) + b^2 = 1$

donc l'un des trois au moins est nul :

Si $a^2=0$, alors $b^2=1$ $\quad b=\pm 1$ **$\beta = \pm c$**

Si $b^2=0$, alors $a^2=1$ $\quad a=\pm 1$ **$\beta = \pm 1$**

Si $ab=0$, alors a ou $b=0$, on est revenu aux deux cas précédents

L'inverse de c est $c^2 = -(1+c)$

——— $-c$ est $-c^2 = 1+c$ ces six complexes ont tous un module 1

L'inverse de 1 est 1

L'inverse de -1 est -1

Donc, si on sait que $\beta \in \mathbb{Z}[c]$, alors

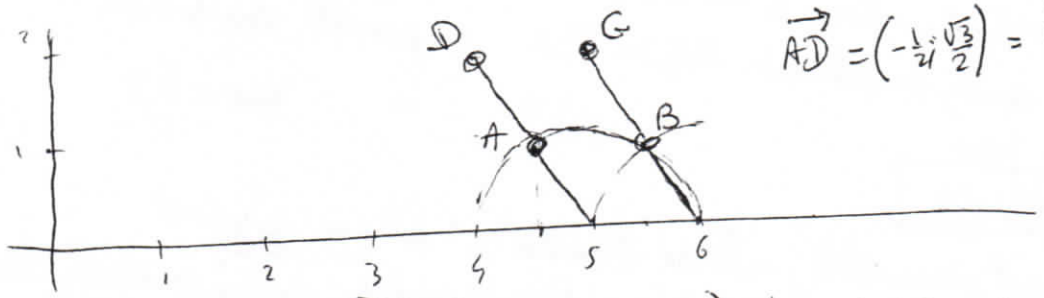
β est inversible $\Leftrightarrow N(\beta) = 1$

---

(21) $\beta_{\overrightarrow{AB}} = \beta_B - \beta_A = a+1+cb-(a+cb) = 1$

$\beta_{\overrightarrow{DG}} = \beta_G - \beta_D = (a+1)+c(b+1)-(a+c(b+1)) = 1$

$\overrightarrow{AB} = \overrightarrow{DG}$, donc ABGD est un parallélogramme



$\overrightarrow{AD} = \left(-\frac{1}{2}; \frac{\sqrt{3}}{2}\right) = \overrightarrow{BG}$

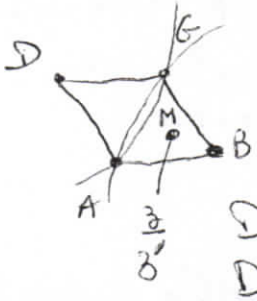
(22) $\beta_{\overrightarrow{BA}} = -1 \Rightarrow \|\overrightarrow{BA}\| = 1$

$\beta_{\overrightarrow{BG}} = c = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ $\quad |c| = 1$ $\quad \|\overrightarrow{BG}\| = 1$

donc A et G sont sur le cercle de centre B de rayon 1

De même, $\|\overrightarrow{DA}\| = \|\overrightarrow{DG}\| = 1$

(23) $\begin{cases} a \le \alpha < a+1 \\ b \le \beta < b+1 \end{cases}$, donc l'image de $\frac{z}{z'} = \alpha + c\beta$ est à l'intérieur du parallélogramme ABGD



Appelons M le point d'affixe $\frac{z}{z'}$.
Un point à l'intérieur du parallélogramme est soit compris dans le cercle de centre B de rayon 1 soit dans le cercle de centre D de rayon 1

Dans le 1er cas, B fait l'affaire car $d(M,B) = \left|\frac{z}{z'} - (a+1+cb)\right| < 1$
Dans le 2ème cas, D fait l'affaire : $q = a + c(b+1)$
Si $M = A$, on choisit A pour $q = a + cb$
Si $M = G$, ——— G.

(24) $r = z - z'q$.
z' et $q \in \mathbb{Z}[c]$, donc $z'q$ aussi (Q 14). Donc $r \in \mathbb{Z}[c]$

$\left|\frac{z}{z'} - q\right| < 1 \Rightarrow |z'| \cdot \left|\frac{z}{z'} - q\right| < |z'| \Rightarrow |z - qz'| < |z'|$ càd $|r| < |z'|$

$N(r) < N(z')$

Ainsi $\forall z, z' \in \mathbb{Z}[c], \exists q, r \in \mathbb{Z}[c] / \begin{cases} z = z'q + r \\ N(r) < N(z') \end{cases}$

(31)

15120	2
7560	2
3780	2
1890	2
945	3
315	3
105	3
35	5
7	7

$15120 = 2^4 \cdot 3^3 \cdot 5 \cdot 7$

(32) $N(f) = 3$. Si $f = z_1 z_2$, alors $N(z_1) N(z_2) = 3$
Il y a deux possibilités : $N(z_1) = 1$ et $N(z_2) = 3$ z_1 est inversible
$N(z_1) = 3$ et $N(z_2) = 1$ z_2 est inversible
Donc f est irréductible dans $\mathbb{Z}[c]$

(33) $2 - 2c = 2(1-c) = 2 \cdot f$ On a vu que 2 et f sont irréductibles

(34) $N(f) = |f|^2 = f \cdot \bar{f} = 3$ $f = 1 - c$
Et $\bar{f} = 1 - \bar{c} = 1 - c^2 = 1 - (-1-c) = 2 + c$
En effet : $(1-c)(2+c) = 2 - 2c - c^2 = 2 - 2c + 1 + c = 3$

$3 = f \cdot \bar{f} = (1-c)(2+c)$

(41)

ε	1	-1	c	$-c$	$1+c$	$-(1+c)$
ε^2	1	1	$-1-c$	$-1+c$	c	c
ε^3	1	-1	1	-1	-1	1
$\frac{1}{\varepsilon}$	1	-1	$-1-c$	$1+c$	$-c$	c

$c^2 = -1-c$ $\quad c^3 = 1$

$(1+c)^2 = (e^{i\pi/3})^2 \quad c^8 \cdot c = 1$

$= c$

$(1+c)^3 = (e^{i\pi/3})^3 = e^{i\pi} = -1$

$\frac{1}{c} = c^2$ car $c^3 = 1$

$= -1-c$

(42)

	$\varepsilon^2 = 1$	$\varepsilon^2 = c$	$\varepsilon^2 = -1-c$
$(\varepsilon')^2 = 1$	$2+c$ (1)	0 (2)	$1-c$ (3)
$(\varepsilon')^2 = c$	$1+2c$ (4)	$-1+c$ (5)	0 (6)
$(\varepsilon')^2 = -1-c$	0 (7)	$-2-c$ (8)	$-1-2c$ (9)

$\varepsilon'^2 - c^2\varepsilon^2 = \varepsilon'^2 + (1+c)\varepsilon^2 = 1+1+c = 2+c$ (1)

$= 1+(1+c)c = 1+c+(-1-c) = 0$ (2)

$= 1+(1+c)(-1-c) = 1-(1+c)^2 = 1-c$ (3)

$= c+(1+c) = 1+2c$ (4)

$= c+(1+c)c = -1+c$ (5)

$= c-(1+c)^2 = c-c = 0$ (6)

$= -1-c+1+c = 0$ (7)

$= -1-c+(1+c)c = -2-c$ (8)

$= -1-c-(1+c)^2 = -1-c-c = -1-2c$

(43)

	$\varepsilon^2 = 1$	$\varepsilon^2 = c$	$\varepsilon^2 = -1-c$
$\varepsilon'^2 = 1$	$f(1+c)$	$f\cdot 0$	$f\cdot 1$
$\varepsilon'^2 = c$	$f\cdot c$	$f\cdot(-1)$	$f\cdot 0$
$\varepsilon'^2 = -1-c$	$f\cdot 0$	$f(-1-c)$	$f\cdot(-c)$

$f\cdot(1+c) = (1-c)(1+c) = 1-c^2 = 1+1+c = 2+c$

$f(-1-c) = -f\cdot(1+c) = -2-c$

$f\cdot c = (1-c)c = c-c^2 = c+1+c = 1+2c$

Ainsi, **Tous les $(\varepsilon')^2 - c^2\varepsilon^2$ sont divisibles par f**

(44) Si $p \in \mathbb{Z}[\varepsilon]$, n'est pas divisible par f, alors il existe q et r tels que

$p = fq + r$ et $N(r) < N(f) = 3$

Comme $N(r)$ ne peut pas être égal à 2 (Q15) : $N(r) = 1$

Donc r est inversible

(45) $p^3 = (fq+\varepsilon)^3 = f^3q^3 + 3f^2q^2\varepsilon + 3fq\varepsilon^2 + \varepsilon^3$

$-f^2c^2 = -(1-c)^2c^2 = -(1-2c+c^2)c^2 = -c^2+2c^3-c^4 = -(-1-c)+2-c = 3$

(46) $p^3 - \varepsilon^3 = f^3q^3 - f^2c^2fq^2\varepsilon - f^2c^2fq\varepsilon^2 = f^3q(q^2 - fc^2q\varepsilon - c^2\varepsilon^2)$

(47) $q^2 = (fq'+\varepsilon')^2 = f^2q'^2 + 2fq'\varepsilon' + \varepsilon'^2 \qquad q^2 - \varepsilon^2 = f(fq'^2 + 2q'\varepsilon')$

$q^2 - c^2\varepsilon^2 = \underbrace{q^2 - \varepsilon'^2}_{\text{div par } f} + \underbrace{\varepsilon'^2 - c^2\varepsilon^2}_{\text{div par } f \text{ (Q43)}}$ donc $q^2 - c^2\varepsilon^2$ est divisible par f.

(48) $q^2 - c^2\varepsilon^2 = f\cdot q'$ Donc $p^3 - \varepsilon^3 = fq(fq' - fc^2q\varepsilon) = f^4q(q' - c^2q\varepsilon)$

Donc $p^3 - \varepsilon^3$ est divisible par f^4 (qd q n'est pas divisible par f).

Si q est div par f c'est tout de suite clair

(49) $\varepsilon^3 = \pm 1$ (Q41), donc **$p^3 + 1$ ou $p^3 - 1$ est divisible par f^4**

(51) Si p est irréductible dans $\mathbb{Z}[\varepsilon]$ et si p divise x et y, alors il divise x^3+y^3 et donc εz^3.
Comme ε est inversible, p divise z^3 et donc p divise z.
On procède de façon identique dans les autres cas.
Conclusion : En simplifiant dans l'équation $x^3+y^3=-\varepsilon z^3$ par tous les p irréductibles divisant x, y et z, on récupère trois éléments x', y' et z' de $\mathbb{Z}[\varepsilon]$ tels que $\begin{cases} x'^3+y'^3+\varepsilon z'^3=0 \\ x', y', z' \text{ sont premiers entre eux deux à deux.} \end{cases}$

(52) $N(\pm 1 \pm 1 \pm \varepsilon) \leq N(\pm 1)+N(\pm 1)+N(\varepsilon) = 1+1+1 = 3$ Donc $\boxed{N(\pm 1 \pm 1 \pm \varepsilon) \leq 9}$
c'est l'inégalité triangulaire.

$N(kf^4) = N(k)\,N(f^4) \geq 1 \cdot N(f^4) = (N(f))^4 = 3^4 = 81$

On peut examiner les huit valeurs possibles de $\pm 1 \pm 1 \pm \varepsilon$. On ne trouve jamais 0.
Si x, y et z ne sont pas divisibles par f, alors il existe k_1, k_2 et k_3 tels que $x^3 = \pm 1 + k_1 f^4$; $y^3 = \pm 1 + k_2 f^4$ et $z^3 = \pm 1 + k_3 f^4$.
Donc $\pm 1 \pm (\pm \varepsilon + (k_1+k_2+\varepsilon k_3) f^4 = 0$
$\pm 1 \pm 1 \pm \varepsilon = k f^4$
$N(\pm 1 \pm 1 \pm \varepsilon) \leq 3$ et $N(kf^4) \geq 81$ si $k \neq 0$ donc $k = 0$
Donc $\pm 1 \pm 1 \pm \varepsilon = 0$ impossible.
Donc $\boxed{f \text{ divise l'un des trois}}$

(53) $\varepsilon' x^3 = -\varepsilon' y^3 - z^3$ $x = fx'$ et $y^3 = \pm 1 + k_1 f^4$
$z^3 = \pm 1 + k_2 f^4$
Donc $f^3 x'^3 = \pm 1 \pm \varepsilon' + k f^4$
$k f^3 = \pm 1 \pm \varepsilon'$. Si $k \neq 0$, alors $N(kf^3) \geq 27$ et $N(\pm 1 \pm \varepsilon) \leq 4$
Donc $k = 0$ et $\boxed{\varepsilon' = \pm 1}$
Les équations $x^3+y^3+z^3=0$ et $x^3+y^3-z^3=0$ sont bien de la forme voulue.

(54) $x^3 = \pm 1 + k_1 f^4$ et $y^3 = \pm 1 + k_2 f^4$.

Donc $\varepsilon z^3 = \pm 1 \pm 1 + (k_1 + k_2) f^4$ et $z = k_3 f$

donc $\pm 1 \pm 1 = (-k_1 + k_2) f + k_3 \varepsilon) f^3 = k f^3$

Et, comme précédemment: $k = 0$ et $\pm 1 \pm 1 = 0$

Donc $\varepsilon k_3^3 f^3 = (k_1 + k_2) f^4 \Rightarrow \varepsilon k_3^3 = (k_1 + k_2) f$

f divise k_3^3, donc il divise k_3. $z = k_3 f$, donc f^4 divise z

(55) • $(x+y)(x+cy)(x+c^2y) = (x^2 + xy + cxy + cy^2)(x + c^2 y)$

$= x^3 + x^2 y + cx^2 y + cxy^2 + c^2 x^2 y + c^2 xy^2 + c^3 xy^2 + c^3 y^3$

$= x^3 + (1 + c + c^2) x^2 y + (c + c^2 + c^3) xy^2 + c^3 y^3$

Or: $c^3 = 1$ et $1 + c + c^2 = c + c^2 + c^3 = 0$

Donc $(x+y)(x+cy)(x+c^2y) = x^3 + y^3 = -\varepsilon z^3$

• $\beta = x + cy = x + (1-f)y = \alpha - fy$ et $\alpha = k.f$

Donc $\beta = (k_4 - y) f$

• f divise aussi $\beta - cfy = \gamma$

(56) On suppose que f^2 divise α et β.

$\alpha - \beta = y - cy = (1-c)y = fy = f^2 k$, donc f divise y impossible.

Donc f^2 divise au seul des trois

(57) ρ divise $\alpha + \beta + \gamma = 3x + (1 + c + c^2) y = 3x$ car $1 + c + c^2 = 0$

De plus $3\alpha - 3x = 3y$, donc ρ divise aussi $3y$

Comme x et y sont premiers entre eux : ρ divise $3 = ff\bar{f}$

Donc $\rho = \varepsilon' f$ ou $\varepsilon' \bar{f}$. Comme $f = f(1+c) = \varepsilon^4 f$: $\rho = \varepsilon' f$

(58) $\mathfrak{p}$ divise α et β · $\mathfrak{p}^2$ ne divise pas α et β · $\mathfrak{p}^2$ divise γ.

Donc $\alpha = \varepsilon_1 \mathfrak{p} x'^3$ $\quad \beta = \varepsilon_2 \mathfrak{p} y'^3$ $\quad \gamma = \varepsilon_3 \mathfrak{p}^k z'^3$ où $\mathfrak{p}$ ne divise pas z'.

$\alpha\beta\gamma = -\varepsilon z^3 = -\varepsilon \mathfrak{p}^{3n} z''^3$ où $\mathfrak{p}$ ne divise pas z^{3n}.

Donc $k+2 = 3n$ $\quad$ $\boxed{\gamma = \varepsilon_3 \mathfrak{p}^{3n-2} z'^3}$

(59) $\alpha + c\beta + c^2\gamma = x + y + cx + c^2 y + c^2 x + cy = (1+c+c^2)(x+y) = 0$ car $1+c+c^2 = 0$

$\alpha + c\beta + c^2\gamma = \left(\varepsilon_1 x'^3 + c\varepsilon_2 y'^3 + c^2 \varepsilon_2 \mathfrak{p}^{3n-3} z'^3\right)\mathfrak{p} = 0$

Donc $\varepsilon_1 x'^3 + c\varepsilon_2 y'^3 + c^2 \varepsilon_2 \mathfrak{p}^{3n-3} z'^3 = 0$ ou encore $x'^3 + \varepsilon_1' y'^3 + \varepsilon_2' \mathfrak{p}^{3n-3} z'^3 = 0$

(Avec $\varepsilon_1' = c\dfrac{\varepsilon_2}{\varepsilon_1}$ et $\varepsilon_3' = c^2 \dfrac{\varepsilon_3}{\varepsilon_1}$)

$x'^3 = \pm 1 + k_1 \mathfrak{p}^4$ et $y'^3 = \pm 1 + k_2 \mathfrak{p}^4$ d'après la question 49

Donc $\pm 1 \pm \varepsilon_1' = k\mathfrak{p}^3$ car $n \geq 2$.

Donc comme à la question 53 : $k = 0$ et $\pm 1 \pm \varepsilon_1' = 0$

$\boxed{\varepsilon_1' = \pm 1}$.

Quitte à remplacer y' par $-y'$, on vient de trouver trois éléments de $\mathbb{Z}[\zeta]$ tels que $x'^3 + y'^3 + \varepsilon' z''^3 = 0$ et $z'' = \mathfrak{p}^{n-1} k$, $\mathfrak{p}^n$ ne divisant pas z''.

En reproduisant n fois ce procédé, on construit x, y, z tels que

$x^3 + y^3 + \varepsilon z^3 = 0$ et tels que $\mathfrak{p}$ ne divise aucun des trois.

Ceci contredit le résultat de la question 52.