Le 257-gone régulier

Le groupe multiplicatif $G := (\mathbb{Z}/257\mathbb{Z})^\times$ est cyclique, d'ordre 256. Pour chaque $N \in \{2^i | 0 \le i \le 8\}$, il existe donc un unique sous-groupe $G_N < G$ d'ordre N. Chaque G_N est cyclique, i.e. est une suite géométrique de $\mathbb{Z}/257\mathbb{Z}$.

Pour $k \in G$, soit C_k^N la classe de k modulo G_N. On peut représenter toutes ces classes dans le tableau suivant.

$$\begin{array}{cccc|cccc|cccc|cccc}
1 & 16 & 2 & 32 & 11 & 81 & 22 & 95 & 3 & 48 & 6 & 96 & 33 & 14 & 66 & 28 \\
4 & 64 & 8 & 128 & 44 & 67 & 88 & 123 & 12 & 65 & 24 & 127 & 125 & 56 & 7 & 112 \\
\hline
15 & 17 & 30 & 34 & 92 & 70 & 73 & 117 & 45 & 51 & 90 & 102 & 19 & 47 & 38 & 94 \\
60 & 68 & 120 & 121 & 111 & 23 & 35 & 46 & 77 & 53 & 103 & 106 & 76 & 69 & 105 & 119 \\
\hline\hline
9 & 113 & 18 & 31 & 99 & 42 & 59 & 84 & 27 & 82 & 54 & 93 & 40 & 126 & 80 & 5 \\
36 & 62 & 72 & 124 & 118 & 89 & 21 & 79 & 108 & 71 & 41 & 115 & 97 & 10 & 63 & 20 \\
\hline
122 & 104 & 13 & 49 & 57 & 116 & 114 & 25 & 109 & 55 & 39 & 110 & 86 & 91 & 85 & 75 \\
26 & 98 & 52 & 61 & 29 & 50 & 58 & 100 & 78 & 37 & 101 & 74 & 87 & 107 & 83 & 43
\end{array} \tag{1}$$

Dans (1), chaque bloc dyadique de forme carrée ou 2×1 représente une classe. Par exemple le bloc $\left(\begin{smallmatrix} 33 & 14 \\ 125 & 56 \end{smallmatrix}\middle|\begin{smallmatrix} 66 & 28 \\ 7 & 112 \end{smallmatrix}\right)$, en haut à droite, signifie que $C_{33}^{16} = \{\pm 33, \pm 66, \pm 125, \pm 7, \pm 14, \pm 28, \pm 56, \pm 112\} = \{7.2^i\}_{i=0}^{15}$. Comme $-1 \in G_N$ pour $N \neq 1$, on peut se contenter de travailler ainsi au signe près : $C_k^N = C_{-k}^N = -C_k^N$ pour $N \ge 2$, et $C_k^2 = \{k, -k\}$ et $C_k^1 = \{k\}$. Toute classe C_k^N pour $N \ge 2$ est l'union de deux sous-classes $C_k^{N/2}$ et $C_{k'}^{N/2}$, uniques à l'échange près et apparentes dans (1) : dans notre exemple, $C_{33}^{16} = C_{33}^8 \sqcup C_{66}^8$.

Soit ω une racine 257e de l'unité. Pour $N \ge 2$, notons

$$\sigma_k^N := \sum_{i \in C_k^N} \omega^i \quad \text{et} \quad \pi_k^N := \sigma_k^{N/2} \sigma_{k'}^{N/2} \quad \text{où} \quad C_k^N = C_k^{N/2} \sqcup C_{k'}^{N/2}.$$

Pour $m \in G_N$, la multiplication par m préserve chaque classe kG_N. Cela signifie que pour tout $k \in G$, l'automorphisme $\varphi_m : \omega \mapsto \omega^m$ permute transitivement les éléments de $\{\omega^i | i \in C_k^N\}$. Donc $\varphi_m(\sigma_k^N) = \sigma_k^N$. De plus, φ_m préserve aussi π_k^N. En effet, φ_m préserve ou échange les facteurs $\sigma_k^{N/2}$ et $\sigma_{k'}^{N/2}$, selon que $m \in G_{N/2}$ ou $m \in G_N \smallsetminus G_{N/2}$. Cette propriété $\varphi_m(\pi_k^N) = \pi_k^N$ signifie que π_k^N est toujours une combinaison linéaire des σ_ℓ^N, et d'un entier. Les relations

$$\sigma_k^{N/2} \sigma_{k'}^{N/2} = \pi_k^N \in \mathbb{Z} + \sum_{\ell \in G/G_N} \sigma_\ell^N \mathbb{Z} \quad \text{et} \quad \sigma_k^{N/2} + \sigma_{k'}^{N/2} = \sigma_k^N$$

permettent donc de calculer les $\sigma_k^{N/2}$ à partir des σ_ℓ^N, par la formule du binôme.

On connaît déjà $\sigma_1^{256} = -1$ car c'est la somme de toutes les racines 257es de l'unité, autres que 1. Cela donne des formules pour tous les σ_k^N, avec des racines carrées emboîtées. Tous les σ_k^N pour $N \neq 1$ sont réels puisque $C_k^N = -C_k^N$. Comme $\sigma_1^2 = \omega + \omega^{-1} = 2\cos\frac{2n\pi}{257}$ pour quelque entier n, ces formules fournissent une construction du 257-gone régulier à la règle et au compas.

Déterminer les coefficients des équations quadratiques à résoudre revient donc à exprimer chaque π_k^N comme une combinaison linéaire

$$\pi_k^N = \beta + \sum_{\ell \in G/G_N} \alpha_\ell \sigma_\ell^N \quad \text{où} \quad \beta, \alpha_\ell \in \mathbb{Z}. \tag{2}$$

Théorème. *Les coefficients β, α_ℓ dans* (2) *sont donnés pour tout $k \in G$ par*

$$\begin{array}{rcl|rcl} \pi_k^{256} &=& -64 & \pi_k^{16} &=& \sigma_k^{16}+\sigma_{3k}^{16}+\sigma_{7k}^{16}+\sigma_{9k}^{16} \\ \pi_k^{128} &=& -16 & \pi_k^{8} &=& \sigma_{3k}^{8}+\sigma_{5k}^{8} \\ \pi_k^{64} &=& 2\sigma_k^{64}+5\sigma_{3k}^{64}+5\sigma_{5k}^{64}+4\sigma_{9k}^{64} & \pi_k^{4} &=& \sigma_{15k}^{4} \\ \pi_k^{32} &=& 2(\sigma_k^{32}+\sigma_{7k}^{32}+\sigma_{9k}^{32})+\sigma_{11k}^{32}+\sigma_{21k}^{32} & \pi_k^{2} &=& 1\ . \end{array}$$

Preuve. Soit $2 \le N \le 256$ une puissance de 2, et soit γ un générateur de $G_{N/2}$. Comme $\pi_k^N = \sigma_k^{N/2}\sigma_{k'}^{N/2}$, le coefficient α_ℓ de σ_ℓ^N dans (2) vaut $\frac{1}{N}\#\{(i,j) \in \{0,\dots,\frac{N}{2}-1\}^2 \mid k\gamma^i + k'\gamma^j \in C_\ell^N\}$. Comme C_ℓ^N est une union disjointe de (deux) suites géométriques de raison γ, l'entier $\#(\{k\gamma^i + k'\gamma^j\}_{i=0}^{N/2-1} \cap C_\ell^N)$ est indépendant de j, si bien que

$$\alpha_\ell = \frac{1}{2}\#(\{k\gamma^i + k'\}_{i=0}^{N/2-1} \cap C_\ell^N). \tag{3}$$

Si $N \ge 4$ on peut encore diviser le travail par deux en ne gardant que les indices i pairs : en effet, si η est un générateur de G_N tel que $\eta^2 = \gamma$, alors $k' = k\eta^{2s+1}$ pour un certain entier s, si bien que modulo $G_N = \{\eta^i\}_{i=0}^{N-1}$ on ait

$$k\gamma^{2i+1} + k' = k\eta^{4i+2} + k' = k'\eta^{4i+1-2s} + k\eta^{2s+1} \equiv k' + k\eta^{4s-4i} = k' + k\gamma^{2(s-i)}.$$

Ainsi (3) devient

$$\alpha_\ell = \#(\{k\gamma^{2i} + k'\}_{i=0}^{N/4-1} \cap C_\ell^N) = \#\big((C_k^{N/4} + \{k'\}) \cap C_\ell^N\big). \tag{4}$$

Montrons maintenant le théorème. Comme appliquer φ_m à (2) donne $\pi_{mk}^N = \beta + \sum_\ell \alpha_\ell \sigma_{m\ell}^N$, on peut se contenter de traiter $k = 1$.
• $N = 256$: on a $\pi_1^{256} = 64\sigma_1^{256} = -64$ car $C_\ell^N = G$ dans (4).
• $N = 128$: il n'y a que deux classes, C_1^{128} (résidus carrés) et C_3^{128}. Développons $\pi_1^{128} = \sigma_1^{64}\sigma_9^{64}$ en somme de 2^{12} termes de la forme ω^i. Les termes avec $i \in C_1^{128}$ (resp. $i \in C_3^{128}$) paraissent tous le même nombre de fois. Il suffit donc de montrer que ω^1 paraît exactement $2^4 = 16$ fois. Comme les coefficients du tableau (1) représentent des paires $\{k, -k\}$ de classes modulo 257, il s'agit de dénombrer les couples d'entiers consécutifs de $\{1,\dots,128\}$ dont l'un appartient à C_1^{64} (quart NW du tableau) et l'autre à C_9^{64} (quart SW). On compte 16 tels couples $(k, k+1)$, pour $k \in \{8, 17, 21, 29, 30, 31, 35, 59, 60, 72, 88, 116, 117, 121, 122, 123\}$.
• $N = 64$: comme $C_1^{64} = C_1^{32} \sqcup C_{11}^{32}$, par (4) il suffit de voir que $\{11 + 2^i\}_{i=0}^{15} = \{11 \pm 2^i\}_{i=0}^{7}$ rencontre les quarts C_1^{64}, C_3^{64}, C_5^{64} et C_9^{64} du tableau (1) en des ensembles de 2, 5, 5 et 4 points respectivement : à savoir $\{15, -117\}$, $\{3, 7, 12, 19, -53\}$, $\{10, 27, 43, 75, -5\}$ et $\{9, 13, -21, -118\}$.
• $N = 32$: comme $C_1^{32} = C_1^{16} \sqcup C_{15}^{16}$, par (4) il suffit de voir que $\{15 + 4^i\}_{i=0}^{7} = \{15 \pm 4^i\}_{i=0}^{3}$ rencontre les blocs C_1^{32}, C_7^{32}, C_9^{32}, C_{11}^{32} et C_{21}^{32} de (1) en 2, 2, 2, 1, 1 points respectivement (et ne rencontre pas les blocs restants C_3^{32}, C_5^{32},C_{27}^{32}). Les intersections sont $\{-1, 16\}$, $\{14, 19\}$, $\{-49, 31\}$, $\{11\}$ et $\{79\}$.
• $N = 16$: comme $C_1^{16} = C_1^8 \sqcup C_2^8$, voir que $\{2 + 16^i\}_{i=0}^{3} = \{2\} \pm \{1, 16\} = \{1, 3, -14, 18\}$ rencontre les blocs $C_1^{16} = \left(\begin{smallmatrix} \mathbf{1} & 16 & 2 & 32 \\ 4 & 64 & 8 & 128 \end{smallmatrix}\right)$, $C_3^{16} = \left(\begin{smallmatrix} \mathbf{3} & 48 & 6 & 96 \\ 12 & 65 & 24 & 127 \end{smallmatrix}\right)$, $C_7^{16} = \left(\begin{smallmatrix} 33 & \mathbf{14} & 66 & 28 \\ 125 & 56 & 7 & 112 \end{smallmatrix}\right)$, et $C_9^{16} = \left(\begin{smallmatrix} 9 & 113 & \mathbf{18} & 31 \\ 36 & 62 & 72 & 124 \end{smallmatrix}\right)$.
• $N = 8$: comme $C_1^8 = C_1^4 \sqcup C_4^4$, voir $\{4 \pm 1\} = \{3, 5\} \subset C_3^8 \sqcup C_5^8 = \left(\begin{smallmatrix} \mathbf{3} & 48 \\ 12 & 65 \end{smallmatrix}\right) \sqcup \left(\begin{smallmatrix} 80 & \mathbf{5} \\ 63 & 20 \end{smallmatrix}\right)$.
• $N = 4$: comme $C_1^4 = C_1^2 \sqcup C_{16}^2$, vérifier $\{16 + 1\} = \{17\} \subset C_{15}^4 = \left(\begin{smallmatrix} 15 & 17 \end{smallmatrix}\right)$.
• $N = 2$: enfin, $\pi_1^2 = \omega\omega^{-1} = 1$. □