Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Examen terminal, le 10 mai 2023, 8h30-11h30

CORRIGE

Exercice 1. Comme $\mathbb{F}_{101}$ est un corps fini, le groupe multiplicatif $\mathbb{F}_{101}^\times$ de $\mathbb{F}_{101}$ est cyclique d'ordre $101-1=100$. On cherche donc un élément du groupe $\mathbb{F}_{101}^\times$ d'ordre 100. Comme $100 = 10^2 = (2\times 5)^2 = 2^2\times 5^2$, les diviseurs maximaux [1] propres [2] de 100 sont $100/2 = 50$ et $100/5 = 20$. Comme on a vu en cours, un élément x de $\mathbb{F}_{101}^\times$ est donc d'ordre 100 si et seulement si $x^{50}\neq 1$ et $x^{20}\neq 1$ dans $\mathbb{F}_{101}$. Remarquons que 101 est un nombre premier, on a donc $\mathbb{F}_{101} = \mathbb{Z}/101\mathbb{Z}$.

Regardons si $2\in\mathbb{F}_{101}$ satisfait la condition ci-dessus pour être d'ordre 100. On a

$$2^{10} = 1024 = 10\times 101 + 14 = 14 \pmod{101}.$$

Donc

$$2^{20} = (2^{10})^2 = 14^2 = 196 = 95 \neq 1 \pmod{101}.$$

Et aussi

$$2^{50} = (2^{20})^2\times 2^{10} = (-6)^2\times 14 = 36\times 14 = 504 = 5\times 101 - 1 = -1 \neq 1 \pmod{101}.$$

Il s'ensuit que 2 est un générateur de $\mathbb{F}_{101}^\times$.

Exercice 2. a. Comme $K = \mathbb{F}_2[X]/(X^4+X+1)$, il suffit de vérifier que le polynôme X^4+X+1 est irréductible dans $\mathbb{F}_2[X]$. Or, ce polynôme n'a pas de racine dans $\mathbb{F}_2$, donc s'il était réductible, il serait produit de deux polynômes irréductibles de degré 2. Le seul polynôme irréductible de degré 2 dans $\mathbb{F}_2[X]$ étant X^2+X+1, on aurait $X^4+X+1 = (X^2+X+1)^2 = X^4+X^2+1$ par Frobenius, ce qui est absurde. Par conséquent X^4+X+1 est bien irréductible dans $\mathbb{F}_2[X]$.

b. Comme $1, X, X^2, X^3$ est une $\mathbb{F}_2$-base du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2[X]/(X^4+X+1)$, ce dernier est de dimension 4 sur $\mathbb{F}_2$. Il est donc isomorphe à $\mathbb{F}_2^4$ en tant qu'espace vectoriel. Il s'ensuit que

$$|K| = |\mathbb{F}_2^4| = 2^4 = 16.$$

c. Comme K est un corps à 16 éléments, le groupe $K^\times$ est un groupe cyclique d'ordre $15 = 3\times 5$. Il suffit donc de vérifier que $g^3\neq 1$ et $g^5\neq 1$ dans K. On a

$$\begin{aligned}
g^3 &= (X+1)^3 \\
&= X^3+3X^2+3X+1 && \text{d'après le binôme de Newton}\\
&= X^3+X^2+X+1 && \text{car } 3=1 \text{ dans } \mathbb{F}_2\\
&\neq 1 \pmod{X^4+X+1}
\end{aligned}$$

car deux polynômes de degré ≤ 3 sont congrus modulo un polynôme de degré 4 si et seulement s'ils sont égaux, et

$$\begin{aligned}
g^5 &= g^3\times g^2 \\
&= (X^3+X^2+X+1)\times(X+1)^2 && \text{d'après le calcul précédent}\\
&= (X^3+X^2+X+1)\times(X-1)\times(X+1) && \text{car } -1=1 \text{ dans } \mathbb{F}_2\\
&= (X^4-1)\times(X+1)\\
&= (X^4+1)\times(X+1)\\
&= (-X)\times(X+1) && \text{car } X^4+1 = -X \pmod{X^4+X+1}\\
&= X^2+X && \text{car } -1=1 \text{ dans } \mathbb{F}_2\\
&\neq 1 \pmod{X^4+X+1}
\end{aligned}$$

1. par rapport à l'ordre partiel de divisibilité !
2. c-à-d différents de 100 dans le cas présent

pour la même raison que ci-dessus. Il s'ensuit que g est bien un générateur du groupe $K^\times$.

d. On calcule g^i, pour $i = 0, \dots, 14$, jusqu'à ce que $g^i = h = X^3 + X^2 + 1$ ou $g^i = k = X^3 + 1$. On a

$$\begin{aligned}
g^0 &= 1 \neq h, k \\
g^1 &= X + 1 \neq h, k \\
g^2 &= (X+1)^2 = X^2 + 1 \neq h, k && \text{par Frobenius} \\
g^3 &= X^3 + X^2 + X + 1 \neq h, k && \text{d'après le c} \\
g^4 &= (g^2)^2 \\
&= (X^2+1)^2 && \text{d'après le calcul de } g^2 \text{ ci-dessus} \\
&= X^4 + 1 && \text{par Frobenius} \\
&= X \neq h, k && \text{car } X^4 + 1 = X \pmod{X^4 + X + 1} \\
g^5 &= X^2 + X \neq h, k && \text{d'après le c} \\
g^6 &= g^5 \times g \\
&= (X^2 + X) \times (X+1) && \text{d'après le calcul de } g^5 \text{ ci-dessus} \\
&= X^3 + X \neq h, k \\
g^7 &= g^6 \times g \\
&= (X^3 + X) \times (X+1) && \text{d'après le calcul de } g^6 \text{ ci-dessus} \\
&= X^4 + X^3 + X^2 + X \\
&= X^3 + X^2 + 1 = h! && \text{car } X^4 + X = 1 \pmod{X^4 + X + 1}
\end{aligned}$$

Du coup, l'entier a choisi par Alice est congru à 7 modulo 15. La clé secrète qu'Alice et Bob partagent est donc

$$k^7 = (X^3 + 1)^7$$

qu'on calcule par exponentiation rapide :

$$(X^3+1)^7 = (X^3+1)^{1+2+4} = (X^3+1)(X^3+1)^2((X^3+1)^2)^2.$$

Or, $(X^3+1)^2 = X^6 + 1$ par Frobenius, et la division longue de $X^6 + 1$ par $X^4 + X + 1$ donne

$$X^6 + 1 = X^2 \times (X^4 + X + 1) + X^3 + X^2 + 1.$$

Du coup, $(X^3+1)^2 = X^3 + X^2 + 1 \pmod{X^4 + X + 1}$. On a donc $((X^3+1)^2)^2 = (X^3 + X^2 + 1)^2 = X^6 + X^4 + 1 \pmod{X^4 + X + 1}$, par Frobenius encore. La division longue de $X^6 + X^4 + 1$ par $X^4 + X + 1$ donne

$$X^6 + X^4 + 1 = (X^2 + 1)(X^4 + X + 1) + X^3 + X^2 + X.$$

Du coup, $((X^3+1)^2)^2 = X^3 + X^2 + X \pmod{X^4 + X + 1}$. Par conséquent,

$$\begin{aligned}
(X^3+1)^7 &= (X^3+1)(X^3 + X^2 + 1)(X^3 + X^2 + X) \\
&= (X^6 + X^5 + X^2 + 1)(X^3 + X^2 + X) \\
&= (X^3 + X^2 + X + 1)(X^3 + X^2 + X) && \text{car } X^6 + X^5 = (X^2 + X)(X^4 + X + 1) + X^3 + X \\
&= X^6 + X^4 + X^3 + X \\
&= X^2 + 1
\end{aligned}$$

car $X^6 + X^4 = (X^2+1)(X^4 + X + 1) + X^3 + X^2 + X + 1$. La clé secrète est donc $X^2 + 1$.

Exercice 3. On a $n = 360 = 6^2 \times 10 = (2 \times 3)^2 \times 2 \times 5 = 2^3 \times 3^2 \times 5$. L'anneau $\mathbb{Z}/360\mathbb{Z}$ est donc isomorphe à l'anneau $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ à travers l'isomorphisme du Théorème Chinois

$$f \colon \mathbb{Z}/360\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

défini par $f(\bar{x}) = (\bar{x}, \bar{x}, \bar{x})$. Comme on sait déterminer des générateurs du groupe multiplicatif de l'anneau de droite, on cherche une expression pour $f^{-1}(\bar{a}, \bar{b}, \bar{c})$ afin d'obtenir une famille génératrice du groupe multiplicatif de l'anneau de gauche, i.e. $(\mathbb{Z}/360\mathbb{Z})^\times$.

On cherche des entiers u, v, w tels que

$$u \times 3^2 \times 5 + v \times 2^3 \times 5 + w \times 2^3 \times 3^2 = 1.$$

On commence par remarquer que

$$1 \times 3^2 + (-1) \times 2^3 = 1.$$

D'où

$$1 \times 3^2 \times 5 + (-1) \times 2^3 \times 5 = 5.$$

Comme

$$29 \times 5 + (-2) \times 2^3 \times 3^2 = 1,$$

on a

$$29 \times 3^2 \times 5 + (-29) \times 2^3 \times 5 + (-2) \times 2^3 \times 3^2 = 1.$$

On peut donc prendre $u = 29$, $v = -29$ et $w = -2$. On en déduit que

$$f^{-1}(\bar{a}, \bar{b}, \bar{c}) = 29 \times 3^2 \times 5 \times a + (-29) \times 2^3 \times 5 \times b + (-2) \times 2^3 \times 3^2 \times c.$$

Cette fonction nous permettra donc de transférer une famille génératrice du groupe multiplicatif de l'anneau $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ vers une famille génératrice de $\mathbb{Z}/360\mathbb{Z}$.

Afin de déterminer une famille génératrice minimale du groupe multiplicatif de $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, on commence par déterminer des familles génératrices des groupes multiplicatifs de ses facteurs.

D'après le cours, $\{-\bar{1}, -\bar{3}\}$ est une famille génératrice du groupe multiplicatif $(\mathbb{Z}/8\mathbb{Z})^\times$.

Quant à $\mathbb{Z}/9\mathbb{Z}$, on sait que son groupe mutliplicatif est cyclique. De plus, comme $-\bar{1}$ engendre le groupe multiplicatif de $\mathbb{Z}/3\mathbb{Z}$, soit $-\bar{1}$ soit $-\bar{1} + \bar{3} = \bar{2}$ engendre le groupe multiplicatif de $\mathbb{Z}/3^2\mathbb{Z} = \mathbb{Z}/9\mathbb{Z}$. Comme $-\bar{1}$ n'en est évidemment pas un, $\bar{2}$ est un générateur de $(\mathbb{Z}/9\mathbb{Z})^\times$.

Quant à $\mathbb{Z}/5\mathbb{Z}$, son groupe multiplicatif est cyclique d'ordre 4. Comme $\bar{2} \neq \bar{1}$ et $\bar{2}^2 \neq \bar{1}$ dans $\mathbb{Z}/5\mathbb{Z}$, l'élément $\bar{2}$ est un générateur de $(\mathbb{Z}/5\mathbb{Z})^\times$.

Par conséquent, une famille génératrice minimale de $(\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})^\times$ est

$$(-\bar{1}, \bar{1}, \bar{1}), (-\bar{3}, \bar{1}, \bar{1}), (\bar{1}, \bar{2}, \bar{1}), (\bar{1}, \bar{1}, \bar{2}).$$

La famille

$$f^{-1}((-\bar{1}, \bar{1}, \bar{1})), f^{-1}((-\bar{3}, \bar{1}, \bar{1})), f^{-1}((\bar{1}, \bar{2}, \bar{1})), f^{-1}((\bar{1}, \bar{1}, \bar{2}))$$

est donc une famille génératrice de $(\mathbb{Z}/360\mathbb{Z})^\times$. On calcule :

$$f^{-1}((-\bar{1}, \bar{1}, \bar{1})) = 29 \times 3^2 \times 5 \times (-1) + (-29) \times 2^3 \times 5 \times 1 + (-2) \times 2^3 \times 3^2 \times 1 = 271 \pmod{360}$$
$$f^{-1}((-\bar{3}, \bar{1}, \bar{1})) = 29 \times 3^2 \times 5 \times (-3) + (-29) \times 2^3 \times 5 \times 1 + (-2) \times 2^3 \times 3^2 \times 1 = 181 \pmod{360}$$
$$f^{-1}((\bar{1}, \bar{2}, \bar{1})) = 29 \times 3^2 \times 5 \times 1 + (-29) \times 2^3 \times 5 \times 2 + (-2) \times 2^3 \times 3^2 \times 1 = 281 \pmod{360}$$
$$f^{-1}((\bar{1}, \bar{1}, \bar{2})) = 29 \times 3^2 \times 5 \times 1 + (-29) \times 2^3 \times 5 \times 1 + (-2) \times 2^3 \times 3^2 \times 2 = 217 \pmod{360}.$$

La famille

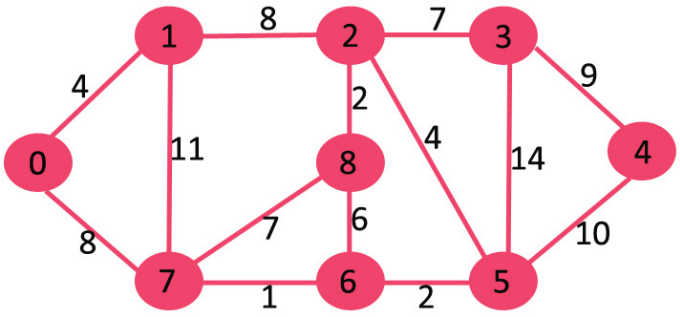
$$\overline{271}, \overline{181}, \overline{281}, \overline{217}$$

est donc une famille génératrice minimale de $(\mathbb{Z}/360\mathbb{Z})^\times$.

Exercice 4. On applique les règles de calcul pour le symbole de Jacobi :

$$\begin{aligned}
\left(\frac{1789}{2023}\right) &= \left(\frac{2023}{1789}\right) && \text{car } 1789 \equiv 1 \pmod 4\\
&= \left(\frac{234}{1789}\right) && \text{car } 2023 \equiv 234 \pmod{1789}\\
&= \left(\frac{2}{1789}\right)\left(\frac{117}{1789}\right) && \text{car } 234 = 2 \times 117\\
&= -\left(\frac{117}{1789}\right) && \text{car } 1789 \equiv -3 \pmod 8\\
&= -\left(\frac{1789}{117}\right) && \text{car } 1789 \equiv 1 \pmod 4\\
&= -\left(\frac{34}{117}\right) && \text{car } 1789 \equiv 34 \pmod{117}\\
&= -\left(\frac{2}{117}\right)\left(\frac{17}{117}\right) && \text{car } 34 = 2 \times 17\\
&= \left(\frac{17}{117}\right) && \text{car } 117 \equiv -3 \pmod 8\\
&= \left(\frac{117}{17}\right) && \text{car } 17 \equiv 1 \pmod 4\\
&= \left(\frac{15}{17}\right) && \text{car } 117 \equiv 15 \pmod{17}\\
&= \left(\frac{17}{15}\right) && \text{car } 17 \equiv 1 \pmod 4\\
&= \left(\frac{2}{15}\right) && \text{car } 17 \equiv 2 \pmod{15}\\
&= 1 && \text{car } 15 \equiv -1 \pmod 8
\end{aligned}$$

Exercice 5. On doit dérouler l'algorithme de Dijkstra sur le graphe suivant



avec point de départ le sommet 0. On commence par initialiser : $W = \emptyset$, et $\ell(v) = +\infty$ pour $v \neq 0$ et $\ell(0) = 0$.

Le complementaire W^c de W dans V, l'ensemble des sommets du graphe, est

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}\,.$$

Les valeurs de ℓ sont respectivement

$$\{0, +\infty, +\infty, +\infty, +\infty, +\infty, +\infty, +\infty, +\infty\}\,.$$

Le minimum de ℓ sur W^c est 0. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{0\}$. On prend le sommet $u = 0$. On rajoute le sommet 0 a W. Les voisins du sommet 0 dans W^c est/sont le(s) sommet(s) $\{1, 7\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 1$ est 4. Comme c'est inferieur

strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(1) = 0$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 7$ est 8. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(7) = 0$. On réitère.

Le complementaire W^c de W est

$$\{1, 2, 3, 4, 5, 6, 7, 8\}.$$

Les valeurs de ℓ sont respectivement

$$\{0, 4, +\infty, +\infty, +\infty, +\infty, +\infty, 8, +\infty\}.$$

Le minimum de ℓ sur W^c est 4. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{1\}$. On prend le sommet $u = 1$. On rajoute le sommet 1 a W. Les voisins du sommet 1 dans W^c est/sont le(s) sommet(s) $\{2, 7\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 2$ est 12. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(2) = 1$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 7$ est 15. Ce n'est pas inferieur strict a la valeur $l(v) = 8$. On réitère.

Le complementaire W^c de W est

$$\{2, 3, 4, 5, 6, 7, 8\}.$$

Les valeurs de ℓ sont respectivement

$$\{0, 4, 12, +\infty, +\infty, +\infty, +\infty, 8, +\infty\}.$$

Le minimum de ℓ sur W^c est 8. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{7\}$. On prend le sommet $u = 7$. On rajoute le sommet 7 a W. Les voisins du sommet 7 dans W^c est/sont le(s) sommet(s) $\{6, 8\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 6$ est 9. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(6) = 7$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 8$ est 15. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(8) = 7$. On réitère.

Le complementaire W^c de W est

$$\{2, 3, 4, 5, 6, 8\}.$$

Les valeurs de ℓ sont respectivement

$$\{0, 4, 12, +\infty, +\infty, +\infty, 9, 8, 15\}.$$

Le minimum de ℓ sur W^c est 9. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{6\}$. On prend le sommet $u = 6$. On rajoute le sommet 6 a W. Les voisins du sommet 6 dans W^c est/sont le(s) sommet(s) $\{5, 8\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 5$ est 11. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(5) = 6$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 8$ est 15. Ce n'est pas inferieur strict a la valeur $l(v) = 15$. On réitère.

Le complementaire W^c de W est

$$\{2, 3, 4, 5, 8\}.$$

Les valeurs de ℓ sont respectivement

$$\{0, 4, 12, +\infty, +\infty, 11, 9, 8, 15\}.$$

Le minimum de ℓ sur W^c est 11. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{5\}$. On prend le sommet $u = 5$. On rajoute le sommet 5 a W. Les voisins du sommet 5 dans W^c est/sont le(s) sommet(s) $\{2, 3, 4\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 2$ est 15. Ce n'est pas inferieur strict a la valeur $l(v) = 12$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 3$ est 25. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(3) = 5$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 4$ est 21. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(4) = 5$. On réitère.

Le complementaire W^c de W est

$$\{2, 3, 4, 8\}.$$

Les valeurs de ℓ sont respectivement

$$\{0, 4, 12, 25, 21, 11, 9, 8, 15\}\,.$$

Le minimum de ℓ sur W^c est 12. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{2\}$. On prend le sommet $u = 2$. On rajoute le sommet 2 a W. Les voisins du sommet 2 dans W^c est/sont le(s) sommet(s) $\{3, 8\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 3$ est 19. Comme c'est inferieur strict a la valeur $l(v) = 25$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(3) = 2$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 8$ est 14. Comme c'est inferieur strict a la valeur $l(v) = 15$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(8) = 2$. On réitère.

Le complementaire W^c de W est

$$\{3, 4, 8\}\,.$$

Les valeurs de ℓ sont respectivement

$$\{0, 4, 12, 19, 21, 11, 9, 8, 14\}\,.$$

Le minimum de ℓ sur W^c est 14. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{8\}$. On prend le sommet $u = 8$. On rajoute le sommet 8 a W. Les voisins du sommet 8 dans W^c est/sont le(s) sommet(s) $\{\}$. On réitère.

Le complementaire W^c de W est

$$\{3, 4\}\,.$$

Les valeurs de ℓ sont respectivement

$$\{0, 4, 12, 19, 21, 11, 9, 8, 14\}\,.$$

Le minimum de ℓ sur W^c est 19. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{3\}$. On prend le sommet $u = 3$. On rajoute le sommet 3 a W. Les voisins du sommet 3 dans W^c est/sont le(s) sommet(s) $\{4\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 4$ est 28. Ce n'est pas inferieur strict a la valeur $l(v) = 21$. On réitère.

Le complementaire W^c de W est

$$\{4\}\,.$$

Les valeurs de ℓ sont respectivement

$$\{0, 4, 12, 19, 21, 11, 9, 8, 14\}\,.$$

Le minimum de ℓ sur W^c est 21. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{4\}$. On prend le sommet $u = 4$. On rajoute le sommet 4 a W. Les voisins du sommet 4 dans W^c est/sont le(s) sommet(s) $\{\}$. Et on a terminé !

Voici le tableau correspondant

v	$\ell(v), p(v)$
0	|
1	4, 0 |
2	12, 1 |
3	25, 5 19, 2 |
4	21, 5 |
5	11, 6 |
6	9, 7 |
7	8, 0 |
8	15, 7 14, 2 |