Ciekawostka: Macierze z $\mathbb{Z}_n$

Piotr Migdał

26 października 2005

Dla każdej grupy $\mathbb{Z}_n$ możemy stworzyć dwie tabele — dodawania i odejmowania. Są one równoważne wykonywaniu obliczaniu w/w funkcji na liczbach całkowitych, modulo n.

Przykład:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Potraktujmy te tabele jako macierze A i B (z elementami a_{ij} i a_{ij}), definiujec je w następujący sposób

$$\begin{array}{ll} A \text{ — macierz dodawania} & a_{ij} := i + j \pmod n \\ B \text{ — macierz mnożenia} & b_{ij} := i * j \pmod n, \end{array}$$

dla $i, j \in \{0, ..., n-1\}$.

Skoro już mamy dwie macierze, czemu by ich nie wymnożyć?

$$\begin{aligned} C &:= AB \pmod n \\ D &:= BA \pmod n \end{aligned}$$

Zwróćmy uwagę, że zaróno A, jak i B są symetryczne. Wobec tego kolejność mnożenia nie robi wielkiej różnicy (bo $D = BA = B^T A^T = (AB)^T = C^T$). Tym samym będziemy się zajmować tylko ich iloczynem C.

W załączniku są policzone macierze C dla przedziału $n \in \{1, ..., 11\}$. Wyglądają dość ciekawie — łatwo zauważyć okresowość ich współczynników. Co jednak jeszcze bardziej interesujące, w tym przedziale zerują się wtedy gdy $n > 3$ jest pierwsze (i tylko wtedy). Czy można znaleźć na to jakieś konkretne reguły? Liczmy (mod n), przy $i, j \in \{0, ..., n-1\}$.

$$
\begin{aligned}
c_{ij} &\equiv \sum_{k=0}^{n-1} a_{ik}\, b_{kj} = \\
&= \sum_{k=0}^{n-1} (i+k)\, k\, j = \sum_{k=0}^{n-1} \left(i\, j\, k + j\, k^2 \right) = \\
&= i\, j \sum_{k=0}^{n-1} k + j \sum_{k=0}^{n-1} k^2 = \\
&= i\, j \frac{(n-1)n}{2} + j \frac{(n-1)n(2n-1)}{6}
\end{aligned} \tag{1}
$$

Z racji tego, że „bawimy się" w liczbach całkowitych, a w jednym mianowniku widnieje liczba 6, naturalnym podejściem do uproszczenia (1) jest rozważenie reszty z dzielenia n przez 6. Rozwiążmy kolejne przypadki, przy $r \in \mathbb{Z}$

- 0° $\quad n = 6r$

$$
\begin{aligned}
c_{ij} &\equiv i\, j \frac{(6r-1)6r}{2} + j \frac{(6r-1)6r(12r-1)}{6} = \\
&= i\, j \left(18r^2 - 3r \right) + j \left(72r^3 - 18r^2 + r \right) \equiv \\
&\equiv i\, j(3r) + j(r) = \\
&= i\, j \frac{n}{2} + j \frac{n}{6}
\end{aligned}
$$

- 1° $\quad n = 6r + 1$

$$
\begin{aligned}
c_{ij} &\equiv i\, j \frac{(6r-1)6r}{2} + j \frac{(6r-1)6r(12r-1)}{6} = \\
&= i\, j \left(18r^2 + 3r \right) + j \left(72r^3 + 18r^2 + r \right) \equiv \\
&\equiv i\, j(0) + j(0) = \\
&= 0
\end{aligned}
$$

- 2° $\quad n = 6r + 2$

$$
\begin{aligned}
c_{ij} &\equiv i\, j \frac{(6r-1)6r}{2} + j \frac{(6r-1)6r(12r-1)}{6} = \\
&= i\, j \left(18r^2 + 9r + 1 \right) + j \left(72r^3 + 54r^2 + 13r + 1 \right) \equiv \\
&\equiv i\, j(3r+1) + j(3r+1) = \\
&= (i+1)\, j \frac{n}{2}
\end{aligned}
$$

- $3^\circ \qquad n = 6r + 3$

$$\begin{aligned} c_{ij} &\equiv i\,j\frac{(6r-1)6r}{2} + j\frac{(6r-1)6r(12r-1)}{6} = \\ &= i\,j\left(18r^2+15r+3\right) + j\left(72r^3+90r^2+31r+5\right) \equiv \\ &\equiv i\,j(0) + j(4r+2) = \\ &= j\frac{2n}{3} \end{aligned}$$

- $4^\circ \qquad n = 6r + 4$

$$\begin{aligned} c_{ij} &\equiv i\,j\frac{(6r-1)6r}{2} + j\frac{(6r-1)6r(12r-1)}{6} = \\ &= i\,j\left(18r^2+21r+6\right) + j\left(72r^3+126r^2+73r+14\right) \equiv \\ &\equiv i\,j(3r+2) + j(3r+2) = \\ &= (i+1)\,j\frac{n}{2} \end{aligned}$$

- $5^\circ \qquad n = 6r + 5$

$$\begin{aligned} c_{ij} &\equiv i\,j\frac{(6r-1)6r}{2} + j\frac{(6r-1)6r(12r-1)}{6} = \\ &= i\,j\left(18r^2+27r+10\right) + j\left(72r^3+162r^2+121r+30\right) \equiv \\ &\equiv i\,j(0) + j(0) = \\ &= 0 \end{aligned}$$

Podsumowując, możemy nasze wyniki spisać następująco:

Przypadki	$6r+1$ $6r+5$	$6r+2$ $6r+4$	$6r$	$6r+3$
Wzory (mod n)	0	$(i+1)j\frac{n}{2}$	$i\,j\frac{n}{2} + j\frac{n}{6}$	$j\frac{2n}{3}$
Powtarzające się cz. mac.	$\begin{pmatrix} 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \frac{n}{2} \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \frac{n}{6} & \frac{n}{3} & \frac{n}{2} & \frac{2n}{3} & \frac{5n}{6} \\ 0 & \frac{2n}{3} & \frac{n}{3} & 0 & \frac{2n}{3} & \frac{n}{3} \end{pmatrix}$	$\begin{pmatrix} 0 & \frac{2n}{3} & \frac{n}{3} \end{pmatrix}$
j. w., czynnik $\frac{n}{6}$ wyciągnięty	$\begin{pmatrix} 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 4 & 2 & 0 & 4 & 2 \end{pmatrix}$	$\begin{pmatrix} 0 & 4 & 2 \end{pmatrix}$

Tym samym macierze C przestają dla nas być czymś dziwnym. W szczególności dziwna właściwość zerowania się ich dla $2 < 3 < n < 5^2$, n nie jest liczbą pierwszą, wtedy i tylko wtedy, gdy ją nie dzieli ani 2 ani 3.

Załącznik

$$
\begin{array}{ll}
1 & \begin{pmatrix} 0 \end{pmatrix} \\
2 & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\
3 & \begin{pmatrix} 0 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 2 & 1 \end{pmatrix} \\
4 & \begin{pmatrix} 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\
5 & \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\
6 & \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 4 & 2 & 0 & 4 & 2 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 4 & 2 & 0 & 4 & 2 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 4 & 2 & 0 & 4 & 2 \end{pmatrix} \\
7 & \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\
8 & \begin{pmatrix} 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}
\end{array}
$$

$$9 \quad \begin{pmatrix} 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \\ 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \\ 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \\ 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \\ 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \\ 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \\ 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \\ 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \\ 0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 3 \end{pmatrix}$$

$$10 \quad \begin{pmatrix} 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$11 \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$