Funkcja Carmichaela i funkcja Möbiusa

Funkcja Carmichaela – definicja

Z twierdzenia Eulera, że dla $a \perp m$ będzie – wcześniej czy później – spełniona kongruencja

$$a^k \equiv 1 \pmod{m}; \qquad k > 0.$$

Takie najmniejsze z możliwych k nazywamy rzędem liczby (elementu) a modulo m – $\mathrm{ord}_m(a) = k$. Maksymalną wartością k jest $\phi(m)$ ale jak widzieliśmy z tabeli (dla $m = 13$) dla niektórych liczb a rząd jest wyraźnie mniejszy.

Naturalne pytanie ...

Czy możemy „obniżyć” to oszacowanie od góry rzędu?
Odpowiedź jest twierdząca: takim „lepszym” ograniczeniem „od góry” rzędu jest właśnie ...

. . . funkcja Carmichaela $\lambda(m)$

Dla modułów będących liczbą pierwszą $m = p$ jest ona *równa funkcji Eulera* $\phi(p) = p - 1$; natomiast dla modułów złożonych mamy

$$\lambda(2^\alpha) = \left\{ \begin{array}{ccc} 1 & \text{dla} & \alpha = 1 \\ 2 & \text{dla} & \alpha = 2 \\ 2^{\alpha-2} & \text{dla} & \alpha \geqslant 3 \end{array} \right\} = \phi(2^\alpha) \\ = \tfrac{1}{2}\phi(2^\alpha)$$

$$\lambda(p^\alpha) = \phi(p^\alpha) \quad \text{dla} \quad p \geqslant 3$$

$$\lambda(m) = [\lambda(2^{\alpha_0}), \lambda({p_1}^{\alpha_1}), \ldots, \lambda({p_r}^{\alpha_r})] \quad \text{dla} \quad m = 2^{\alpha_0} {p_1}^{\alpha_1} \ldots {p_r}^{\alpha_r}.$$

Na przykład: $m = 65520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$.
Funkcja Eulera $\phi(65520) = 8 \cdot 6 \cdot 4 \cdot 6 \cdot 12 = 13824$.
Funkcja Carmichaela $\lambda(65520) = [8/2, 6, 4, 6, 12] = 12$.

Uwaga: dla $m > 2$ $\lambda(m)$ jest zawsze liczbą parzystą.

Przykład zastosowania – (http://pl.wikipedia.org/wiki/Funkcja_Carmichaela)

Oblicz $3^{2000} \pmod{248}$.

Rozwiązanie: ponieważ 248 i 3 są względnie pierwsze (248 nie dzieli się przez 3, bo $2+4+8=14$), to możemy skorzystać z właściwości funkcji Carmichaela.
$\lambda(248) = \mathrm{NWW}[\lambda(8), \lambda(31)] = 2 \cdot 30 = 60$.
Mamy więc $3^{60} \equiv 1 \pmod{248}$. Co więcej – ponieważ 60 „mieści się” w 2000 dokładnie 33 razy to zachodzi ((mod 248)):

$$3^{2000} = \left[(3^{60})^{33}\right](3^{20}) \equiv (1^{33})(3^{20}) \equiv 3^{20} \pmod{248},$$

co jest już do policzenia znacznie prostsze, szczególnie jeżeli mamy pod ręką kalkulator. Ale proste jest i bez użycia kalkulatora – 248 jest bardzo bliskie $3^5 = 243$, a więc ((mod 248))

$$3^{20} = \left[(3^5)^4\right] \equiv (-5)^4 = 25^2 = 625 \pmod{248} \equiv 129 \pmod{248}.$$

Definicja

Dla $n \in \mathbb{N}$ określamy *funkcję Möbiusa* $\mu(n)$ jako

$$\mu(n) \begin{cases} 1, & \text{dla} \quad n = 1, \\ 0, & \text{dla} \quad n \quad \text{podzielnego przez kwadrat liczby pierwszej}, \\ (-1)^k, & \text{dla} \quad n = \prod_{i=1}^{k} p_i. \end{cases}$$

Kilka wartości:

n	1	2	3	4	5	6	7	8	9	10	100	101	102	103
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	0	-1	-1	-1

Twierdzenie 1

Funkcja $\mu(n)$ jest multyplikatywna: $\mu(n \cdot m) = \mu(n) \cdot \mu(m)$ dla $m \perp n$.

Dowód: jeżeli $p^2 \mid n$ lub $p^2 \mid m$ to $p^2 \mid mn$;
stąd $\mu(n \cdot m) = \mu(n) \cdot \mu(m) = 0$.
Dla $m = p_1 p_2 \dots p_s$ i $n = q_1 q_2 \dots q_t$ zachodzi

$\mu(mn) = \mu(p_1 p_2 \dots p_s q_1 q_2 \dots q_t) = (-1)^{s+t} = (-1)^s (-1)^t =$
$\mu(m) \cdot \mu(n)$. Mamy także $\mu(n) = \mu(1)\mu(n) = \mu(n)$. □

Twierdzenie 2

Zachodzi także

$$\mathcal{M}(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{dla } n = 1, \\ 0 & \text{dla } n > 1. \end{cases}$$

Dowód: Dla $n = 1$ $\mathcal{M}(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$.
Dla $n > 1$, $n = p^\alpha$ mamy $\mathcal{M}(p^\alpha) = \sum_{d|p^\alpha} \mu(d) =$
$\mu(1) + \mu(p) + \mu(p^2) + \dots = 1 + (-1) + 0 + 0 + \dots = 0$. □

Dowód, c.d.: W zasadzie to wystarczy – funkcja $\mathcal{M}$ jest też multyplikatywna.

Ale – ładny wzór – dla $n = \prod_{i=1}^{r} {p_i}^{\alpha_i}$ dzielnikami dla których $\mu(d) \neq 0$ są liczby
$1, p_1, \ldots, p_r, p_i p_j (i < j), \ldots, p_i p_j p_k (i < j < k), \ldots, p_1 p_2 \ldots p_r$.
Dlatego

$$\sum_{d|n} = \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum_{i<j} \mu(p_i p_j) + \sum_{i<j<k} \mu(p_i p_j p_k) + \ldots + \mu(p_1 p_2 \ldots p_r)$$

$$= 1 - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \ldots - \binom{r}{r}(-1)^r = (1-1)^r = 0 \qquad \square$$

Twierdzenie 3

Jeżeli $f(n)$ i $g(n)$ są funkcjami arytmetycznymi i zachodzi

$$g(n) = \sum_{d|n} f(d), \qquad \text{to mamy}$$

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Dowód: po pierwsze symetria w powyższym wzorze jest jasna – sumowanie po dzielnikach $d \mid n$ jest równoważne sumowaniu po dzielnikach $\frac{n}{d}$. Sam wzór

$$\begin{aligned}\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d'|n/d} f(d') = \sum_{dd'|n} \mu(d) f(d') \\ &= \sum_{d'|n} f(d') \sum_{d|n/d'} \mu(d) = \sum_{d'|n} f(d') \cdot \delta_{d'n} = f(n) \qquad \square.\end{aligned}$$

Twierdzenie 4

Jeżeli $f(n)$ i $g(n)$ są funkcjami arytmetycznymi i zachodzi

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d), \qquad \text{to mamy}$$

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

Dowód analogiczny:

$$\begin{aligned}
\sum_{d|n} g(d) &= \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{d'|n/d} f(d')\mu(d') f\left(\frac{n}{dd'}\right) \\
&= \sum_{d|n} \sum_{d'|n/d} \mu\left(\frac{n}{dd'}\right) f(d') \\
&= \sum_{dd'|n} \mu\left(\frac{n}{dd'}\right) f(d') \\
&= \sum_{d'|n} f(d') \sum_{d|n/d'} \mu\left(\frac{n}{dd'}\right) = f(n). \qquad \square.
\end{aligned}$$

Liczba i suma dzielników n

Mieliśmy

$$\tau(n) = \sum_{d|n} 1, \qquad \text{a także} \qquad \sigma(n) = \sum_{d|n} d.$$

Wzory Möbiusa pozwalają przekształcić te równości w

$$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d), \qquad \text{a także} \qquad n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d).$$

Z wzorów „o odwracaniu” (twierdzenia 3 i 4) wynika

Twierdzenie 5

Dla każdego $n \in \mathbb{N}$ zachodzi $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.
Dowód – stosujemy twierdzenie 3 do $g(n) = n = \sum_{d|n} \phi(d)$.

$$\phi(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}. \qquad \square$$