Odwrotność modularna

Bartosz Chomiński

1 Definicja

Odwrotność modularna liczby a modulo p to taka liczba b, że liczba $a \cdot b$ daje resztę 1 z dzielenia przez p.

Okazuje się (a nawet za chwilę to **udowodnimy**), że każda liczba niepodzielna przez p ma swoją odwrotność modularną.

2 Wyznaczenie – sposób z twierdzeniem Fermata

W notatce *Małe twierdzenie Fermata* pokazaliśmy, że jeżeli p jest liczbą pierwszą oraz a jest liczbą niepodzielną przez p, to liczba a^{p-1} daje resztę 1 z dzielenia przez p.

Zauważmy, że ten fakt pokazuje nam konkretny wzór na odwrotność modularną. Wystarczy, że zapiszemy

$$a^{p-1} \equiv 1 \pmod{p}$$

jako

$$a \cdot a^{p-2} \equiv 1 \pmod{p}$$

i powinno być już jasne, że a^{p-2} jest odwrotnością a modulo p, ponieważ w oczywisty sposób wypełnia definicję odwrotności modularnej podaną na początku.

W zastosowaniach praktycznych można obliczyć $a^{p-2} \bmod p$ używając algorytmu na szybkie potęgowanie typu *dziel i zwyciężaj*.

3 Wyznaczenie – sposób z algorytmem Euklidesa

3.1 Pewne równanie diofantyczne

Rozważmy równanie

$$ax + by = d,$$

gdzie a i b są danymi liczbami naturalnymi, d ich największym wspólnym dzielnikiem, a x i y szukanymi liczbami całkowitymi.

Jeśli będziemy w stanie szybko rozwiązywać tego typu równania, to będziemy umieli podobnie szybko wyznaczać odwrotności modularne. Wystarczy rozwiązać równanie

$$ax + py = 1,$$

by x było wprost z definicji odwrotnością modularną a modulo p.

Przejdźmy zatem do rozwiązania tego równania w ogólności.

3.2 Krok ku rozwiązaniu

Spróbujmy rozwiązać nieco prostsze równanie od

$$ax + by = d$$

. Przez *nieco prostsze* równanie będziemy uważać takie, w którym liczby a i b będą mniejsze[1].

Załóżmy dla wygody, że $a \geqslant b$ i $b \neq 0$ – jeśli $b = 0$, to równanie jest całkiem proste i ma rozwiązanie $(x, y) = (1, 0)$. Możemy rozważyć analogiczne równanie dla „mniejszej" pary $(b, a-b)$ – okazuje się, że z rozwiązania równania dla pary $(b, a-b)$ można łatwo odzyskać rozwiązanie dla pary (a, b). Załóżmy, że mamy rozwiązanie (x, y) równania dla „mniejszej pary", czyli (x, y) takie, że

$$bx + (a - b)y = d.$$

Wtedy, po drobnych przekształceniach algebraicznych mamy

$$ay + b(x - y) = d,$$

a więc para $(x, y-x)$ jest rozwiązaniem oryginalnego równania.

Tę metodę możemy uogólnić i wiedząc, że

$$a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b$$

zauważyć, że jeśli

$$bx + (a \bmod b)y = d,$$

[1] Nie jest to precyzyjna definicja, a raczej *życzenie* podyktowane intuicją, zgodnie z którą jeśli zadanie ma mniejsze liczby, to jest prostsze.

to

$$ay + b\left(x - \left\lfloor \frac{a}{b} \right\rfloor y\right) = d.$$

W ten sposób, na podstawie dowodu poprawności algorytmu Euklidesa, możemy równanie z dowolnymi parametrami a i b sprowadzić do równania z parametrem b równym 0. Dla przykładu:

$$\begin{array}{ll}
11x + 7y = 1 & 11 \cdot \mathbf{2} + 7 \cdot (-\mathbf{3}) = 1 \\
\quad | & \quad | \\
7x_1 + 4y_1 = 1 & 7 \cdot (-\mathbf{1}) + 4 \cdot \mathbf{2} = 1 \\
\quad | & \quad | \\
4x_2 + 3y_2 = 1 & 4 \cdot \mathbf{1} + 3 \cdot (-\mathbf{1}) = 1 \\
\quad | & \quad | \\
3x_3 + 1y_3 = 1 & 3 \cdot \mathbf{0} + 1 \cdot \mathbf{1} = 1 \\
\quad | & \quad | \\
1x_4 + 0y_4 = 1 & \text{——————} \; 1 \cdot \mathbf{1} + 0 \cdot \mathbf{0} = 1
\end{array}$$

(Zauważ przejścia typu $(x, y) \mapsto (y, x - ky)$ idąc w górę w drugiej kolumnie.)

4 Czytaj też

- `https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity`
- `https://en.wikipedia.org/wiki/Euclidean_algorithm`