Rozwiązanie zadania F 775.
Przez układ (r, R_2) nie przechodzi strumień zmiennego pola magnetycznego, zatem nie indukuje się w tym układzie siła elektromotoryczna. Opory R_2 i r można więc traktować jako połączone równolegle, stąd

$$I = \frac{\mathcal{E}/N}{R_1 + rR_2/(r+R_2)} \frac{rR_2}{r+R_2} \frac{1}{r} = \\ = \frac{\mathcal{E}R_2}{N[r(R_1+R_2)+R_1R_2]}.$$

Współczynniki dwumianowe modulo m

Tomasz IDZIASZEK

W informatycznym kąciku olimpijskim w poprzednim numerze *Delty* opisane zostało zadanie, którego rozwiązanie sprowadzono do obliczenia pewnej liczby współczynników dwumianowych modulo ustalony moduł m. Przedstawiono tam też prosty algorytm obliczania wartości $\binom{n}{k}$ mod m, działający w czasie $O(k^2 \log n)$, zatem niezbyt praktyczny, gdy zarówno n, jak i k są duże.
W niniejszym artykule przedstawimy inny algorytm, który po fazie obliczeń wstępnych zajmujących czas $O(m)$ pozwoli na obliczanie $\binom{n}{k}$ mod m w czasie $O\big(\frac{\log m}{\log\log m}\log n + \log m\big)$.

Na początku pokażemy, jak obliczać współczynniki dwumianowe modulo potęga liczby pierwszej. W dalszej części artykułu p zawsze będzie oznaczać liczbę pierwszą, a p^α jej potęgę o wykładniku całkowitym dodatnim.

Aby obliczyć $\binom{n}{k}$ mod p^α, skorzystamy ze wzoru

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

i spróbujemy sprowadzić zadanie do obliczenia $n!$ mod p^α. Musimy jednak uważać, gdyż np. dla $k = p^\alpha$ w mianowniku pojawia nam się zero. Aby poradzić sobie z tym kłopotem, wyciągniemy z silni wszystkie czynniki p. Niech mianowicie $\alpha_p(n)$ będzie największą potęgą liczby p dzielącą $n!$. Jeśli będziemy umieli znaleźć liczbę

$$\beta_p(n) \equiv \frac{n!}{p^{\alpha_p(n)}} \pmod{p^\alpha},$$

to rozwiązaniem będzie

$$(*) \qquad \binom{n}{k} \equiv p^{\alpha_p(n)-\alpha_p(k)-\alpha_p(n-k)} \frac{\beta_p(n)}{\beta_p(k)\beta_p(n-k)} \pmod{p^\alpha}.$$

Dzielenie w powyższym wzorze jest wykonywane w grupie $\mathbb{Z}^*_{p^\alpha}$.

Dzielenie przez x w grupie $\mathbb{Z}^*_{p^\alpha}$ jest mnożeniem przez odwrotność x^{-1} elementu x w tej grupie. Odwrotność można obliczyć w czasie $O(\log p^\alpha)$, korzystając z rozszerzonego algorytmu Euklidesa.

Czytelnicy znający rozwiązanie zadania „obliczyć, iloma zerami kończy się zapis dziesiętny liczby n!" wiedzą, a pozostali łatwo się przekonają, że

$$\alpha_p(n) = \sum_{i \geqslant 1} \lfloor n/p^i \rfloor = \lfloor n/p \rfloor + \alpha_p(\lfloor n/p \rfloor),$$

zatem $\alpha_p(n)$ możemy łatwo obliczyć w czasie $O(\log n)$. Pozostaje już tylko znaleźć wartość $\beta_p(n)$.

Zdefiniujmy silniopodobną funkcję $n!_p$ oznaczającą iloczyn liczb od 1 do n niepodzielnych przez p. Wprowadźmy też oznaczenie

$$\varepsilon_p = \begin{cases} -1 & \text{dla } p \neq 2 \text{ lub } p^\alpha = 4, \\ 1 & \text{dla } p = 2 \text{ i } p^\alpha \neq 4. \end{cases}$$

Przypomnijmy, że twierdzenie Wilsona orzeka, że dla liczby pierwszej p spełnione jest $p!_p \equiv -1 \pmod p$. Uogólnienie tego twierdzenia na potęgi liczb pierwszych p^α wygląda następująco:

$$p^\alpha!_p \equiv \varepsilon_p \pmod{p^\alpha}.$$

Rozwiązanie zadania F 776.
Z prawa zachowania energii dostajemy

$$C\frac{U_0^2}{2} = L_1\frac{I_1^2}{2} + L_2\frac{I_2^2}{2}.$$

Porównując strumienie magnetyczne przechodzące przez cewki, mamy $L_1I_1 = L_2I_2$. Rozwiązując układ równań, otrzymujemy

$$I_1 = U_0\sqrt{\frac{L_2}{L_1}\frac{C}{L_1+L_2}},$$

$$I_2 = U_0\sqrt{\frac{L_1}{L_2}\frac{C}{L_1+L_2}}.$$

Dla dowodu zauważmy, że po lewej stronie kongruencji mamy iloczyn wszystkich elementów grupy $\mathbb{Z}^*_{p^\alpha}$. Każdy element tej grupy ma zdefiniowany jednoznacznie element odwrotny. Iloczyn elementów, które nie są swoimi własnymi odwrotnościami, wynosi 1. Pozostaje zatem obliczyć iloczyn elementów spełniających równanie

$$(**) \qquad x^2 \equiv 1 \pmod{p^\alpha}.$$

Równanie to jest równoważne kongruencji $(x-1)(x+1) \equiv 0 \pmod{p^\alpha}$, co dla $p \neq 2$ jest równoważne $x \equiv 1 \pmod{p^\alpha}$ lub $x \equiv p^\alpha - 1 \pmod{p^\alpha}$. Zatem $p^\alpha!_p \equiv -1 \pmod{p^\alpha}$.

W przypadku $p = 2$ mamy $2!_p = 1$, $4!_p = 3$, a dla $\alpha \geqslant 3$ równanie $(**)$ ma cztery rozwiązania: 1, $2^{\alpha-1}-1$, $2^{\alpha-1}+1$ i $2^\alpha - 1$, których iloczyn modulo p^α wynosi 1.

Rozwiązanie zadania M 1294.
Szukamy liczb całkowitych dodatnich a, b oraz liczby pierwszej p, dla których

$$(a+b)(a^2-ab+b^2)=p^4.$$

Dla $a=b=1$ powyższe równanie sprowadza się do $p^4=2$, co spełnione być nie może. Przyjmijmy więc bez straty ogólności, że $a \geqslant b$ oraz $a \geqslant 2$. Wtedy $a+b>1$ oraz $a^2-ab+b^2>1$, skąd wniosek, że $p \mid a+b$ oraz $p \mid a^2-ab+b^2=(a+b)^2-3ab$. A zatem $p \mid 3ab$. Wobec tego $p=3$ lub $p \mid ab$.

W przypadku, gdy $p=3$, otrzymujemy równanie $a^3+b^3=81$. Bezpośrednio sprawdzamy, że równanie to nie ma rozwiązań w liczbach całkowitych dodatnich a, b.

Z kolei z podzielności $p \mid ab$ wynika, że p jest dzielnikiem jednej z liczb a lub b, co po wykorzystaniu podzielności $p \mid a+b$ pozwala wywnioskować, że liczba p jest dzielnikiem obu liczb a, b. Wobec tego $a=pa_1$, $b=pb_1$, gdzie liczby a_1, b_1 są całkowite i dodatnie. Dane równanie przybiera wtedy postać

$$(a_1+b_1)(a_1^2-a_1b_1+b_1^2)=p.$$

A ponieważ $a_1+b_1>1$, więc $a_1+b_1=p$ oraz $a_1^2-a_1b_1+b_1^2=1$. Z ostatniej równości dostajemy: $a_1=b_1=1$. Stąd $p=a_1+b_1=2$, $a=p=2$ oraz $b=p=2$.

Bezpośrednie sprawdzenie dowodzi, że para $(a,b)=(2,2)$ spełnia warunki zadania.

Teraz już możemy pokazać, jak obliczać $\beta_p(n)$. Mianowicie, jeśli wprowadzimy oznaczenie $N_i=\lfloor n/p^i \rfloor \bmod p^\alpha$, to

$$\beta_p(n) \equiv \varepsilon_p^{\alpha_p(\lfloor n/p^{\alpha-1} \rfloor)} \prod_{i \geqslant 0} N_i!_p \pmod{p^\alpha}.$$

Dowód przeprowadzimy przez indukcję względem n. Jeśli $n=0$, to wzór na $\beta_p(n)$ jest spełniony. Dla $n \geqslant 1$ załóżmy więc, że spełniony jest w przypadku $\lfloor n/p \rfloor < n$ i wywnioskujmy z tego prawdziwość dla n.

Kluczową sprawą jest wyznaczenie $n!_p \bmod p^\alpha$. Każdą liczbę w tym iloczynie przedstawiamy w postaci $k=ip^\alpha+j$, a następnie korzystamy z uogólnionego twierdzenia Wilsona:

$$\begin{aligned} n!_p &= \prod_{\substack{1 \leqslant k \leqslant n \\ p \nmid k}} k = \prod_{\substack{0 \leqslant i < \lfloor n/p^\alpha \rfloor \\ 1 \leqslant j < p^\alpha \\ p \nmid j}} (ip^\alpha+j) \cdot \prod_{\substack{1 \leqslant j < N_0 \\ p \nmid j}} \left(\lfloor n/p^\alpha \rfloor p^\alpha + j\right) \equiv \\ &\equiv \prod_{0 \leqslant i < \lfloor n/p^\alpha \rfloor} \prod_{\substack{1 \leqslant j < p^\alpha \\ p \nmid j}} j \cdot \prod_{\substack{1 \leqslant j < N_0 \\ p \nmid j}} j \equiv (p^\alpha!_p)^{\lfloor n/p^\alpha \rfloor} \cdot N_0!_p \equiv \\ &\equiv \varepsilon_p^{\lfloor n/p^\alpha \rfloor} \cdot N_0!_p \pmod{p^\alpha}. \end{aligned}$$

W celu obliczenia $\beta_p(n)$, liczby od 1 do n rozbijamy na dwie grupy: niepodzielne przez p (ich iloczyn to oczywiście $n!_p$) oraz resztę, do której zastosujemy założenie indukcyjne:

$$\begin{aligned} \frac{n!}{p^{\alpha_p(n)}} &= n!_p \cdot \frac{\lfloor n/p \rfloor !}{p^{\alpha_p(\lfloor n/p \rfloor)}} \equiv n!_p \cdot \beta_p(\lfloor n/p \rfloor) \equiv \\ &\equiv \varepsilon_p^{\lfloor n/p^\alpha \rfloor} N_0!_p \cdot \varepsilon_p^{\alpha_p(\lfloor n/p^{\alpha-2} \rfloor)} \prod_{i \geqslant 0} N_{i+1}!_p = \\ &= \varepsilon_p^{\alpha_p(\lfloor n/p^{\alpha-1} \rfloor)} \cdot \prod_{i \geqslant 0} N_i!_p \pmod{p^\alpha}. \end{aligned}$$

Dla ustalonego p^α wartości $s[x]=x!_p \bmod p^\alpha$ dla $0 \leqslant x < p^\alpha$ możemy wyznaczyć w fazie obliczeń wstępnych. Faktycznie, $s[0]=1$ oraz dla $x \geqslant 1$

$$s[x] = \begin{cases} (s[x-1] \cdot x) \bmod p^\alpha & \text{dla } p \nmid x, \\ s[x-1] & \text{dla } p \mid x, \end{cases}$$

zatem możemy to zrobić w czasie $O(p^\alpha)$. Mając tablicę s, obliczamy $\beta_p(n)$ w czasie $O(\log n)$. Ostatecznie, wzór $(*)$ obliczamy w czasie $O(\log n + \log p^\alpha)$.

Współczynniki w dwudziestu krokach

$b_1 := a_1 + a_2$,
$b_2 := a_1 \cdot a_2$,
$b_3 := a_3 + a_4$,
$b_4 := a_3 \cdot a_4$,
$b_5 := b_1 + b_3$,
$b_6 := b_5 + a_5 = p$,
$b_7 := b_5 \cdot a_5$,
$b_8 := b_2 + b_4$,
$b_9 := b_1 \cdot b_3$,
$b_{10} := b_8 + b_9$,
$b_{11} := b_{10} + b_7 = q$,
$b_{12} := b_{10} \cdot a_5$,
$b_{13} := b_1 \cdot b_4$,
$b_{14} := b_2 \cdot b_3$,
$b_{15} := b_{13} + b_{14}$,
$b_{16} := b_{12} + b_{15} = r$,
$b_{17} := b_{15} \cdot a_5$,
$b_{18} := b_2 \cdot b_4$,
$b_{19} := b_{17} + b_{18} = s$,
$b_{20} := b_{18} \cdot a_5 = t$.

Przejdźmy teraz do przypadku ogólnego. Chcąc obliczyć $\binom{n}{k} \bmod m$, musimy najpierw rozłożyć moduł na iloczyn potęg liczb pierwszych

$$m = \prod_{1 \leqslant i \leqslant \ell} p_i^{\alpha_i}.$$

Możemy sobie pozwolić na zastosowanie naiwnego algorytmu $O(m)$, gdyż i tak obliczanie tablic s zajmie czas $O(\sum p_i^{\alpha_i}) = O(m)$.

Jeśli teraz oznaczymy $c_i = \binom{n}{k} \bmod p_i^{\alpha_i}$, to z chińskiego twierdzenia o resztach dostajemy, że

$$(***) \qquad \binom{n}{k} \equiv \sum_{1 \leqslant i \leqslant \ell} c_i \frac{m}{p_i^{\alpha_i}} \left(\frac{m}{p_i^{\alpha_i}} \right)^{-1} \pmod{m},$$

gdzie $\left(\frac{m}{p_i^{\alpha_i}} \right)^{-1}$ oznacza odwrotność tego elementu w grupie $\mathbb{Z}^*_{p_i^{\alpha_i}}$. Ponieważ

$$\sum \log p_i^{\alpha_i} = \log \prod p_i^{\alpha_i},$$

zatem obliczenie wszystkich odwrotności (również tych używanych przy obliczaniu c_i) zabierze łączny czas $O(\log m)$. Ostatecznie obliczenie wartości c_i i wzoru $(***)$ zajmie czas $O(\ell \log n + \log m + \ell)$.

Ponieważ $\ell = O\left(\frac{\log m}{\log \log m}\right)$, zatem ostatecznie dostajemy, że po wstępnych obliczeniach zajmujących czas $O(m)$ możemy obliczyć dowolny współczynnik dwumianowy $\binom{n}{k}$ modulo m w czasie $O\left(\frac{\log m}{\log \log m} \log n + \log m\right)$.