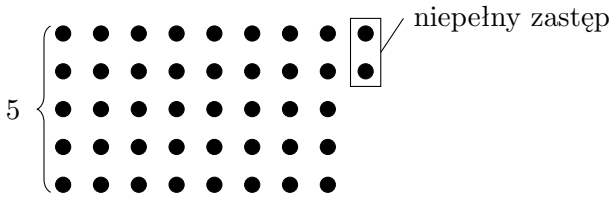
Chińskie twierdzenie o resztach

Bartosz Chomiński

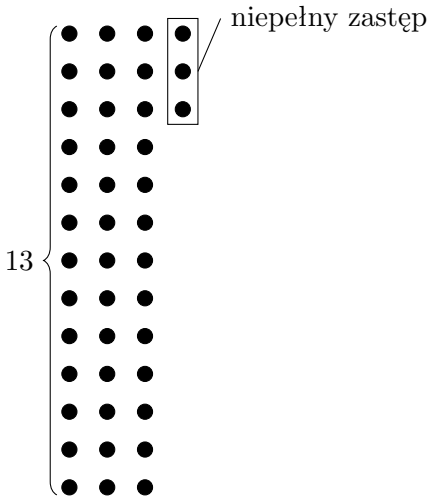
1 Wstęp

Rozważmy pewien chiński pułk żołnierzy, którego liczność chciałby poznać jego dowódca. Żołnierzy w tym pułku jest tak wielu, że ręczne ich policzenie byłoby bardzo czasochłonne.

Żołnierze przeszli solidne szkolenie (jak to żołnierze) i potrafią bardzo szybko ustawić się w zastępy k-osobowe dla dowolnego naturalnego k wybranego przez dowódcę. Gdy dowódca wyda rozkaz z pewnym k, żołnierze ustawiają się w bardzo dużo zastępów k-osobowych i ewentualnie jeden niepełny zastęp, którego liczność widać gołym okiem, co obrazują poniższe ilustracje.



Schemat ustawienia żołnierzy dla rozkazu $k = 5$.



Schemat ustawienia żołnierzy dla rozkazu $k = 13$.

Okazuje się, że liczności niepełnych zastępów wystarczają do stwierdzenia ilu żołnierzy liczy pułk!

Oznaczmy szukaną liczbę żołnierzy przez x. W powyższym przykładzie możemy „na oko" założyć, że liczba żołnierzy nie przekracza 60, a ponadto z informacji o niepełnych zastępach możemy wywnioskować, że

$$x \equiv 2 \pmod 5 \quad \text{oraz} \quad x \equiv 3 \pmod{13}.$$

Wypiszmy wszystkie liczby nieprzekraczające 60, które spełniają po jednym z powyższych warunków:

$$\{2, 7, 12, 17, 22, 27, 32, 37, \mathbf{42}, 47, 52, 57\},$$

$$\{16, 29, \mathbf{42}, 55\}.$$

Tylko jedna liczba jest w obu tych zbiorach – jest to 42 i jest to wobec tego odpowiedź.

2 Uogólnienie

W ogólności zachodzi następujące twierdzenie.

Twierdzenie. (chińskie o resztach) Niech $p_1, p_2, \ldots, p_n$ będą parami względnie pierwszymi liczbami naturalnymi i niech $a_1, a_2, \ldots, a_n$ będą dowolnymi liczbami naturalnymi. Wówczas w zbiorze $\{0, 1, \ldots, p_1 p_2 \cdots p_n - 1\}$ istnieje dokładnie jedna liczba x, spełniająca kongruencje

$$\begin{cases} x \equiv a_1 \pmod{p_1}, \\ x \equiv a_2 \pmod{p_2}, \\ \vdots \\ x \equiv a_n \pmod{p_n}. \end{cases}$$

3 Dowód

3.1 Preliminaria

Przyjmijmy, jak zwykle dla wygody, następującą konwencję notacyjną:

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Ustalmy konkretne liczby $a_1, a_2, \ldots, a_n, p_1, p_2, \ldots, p_n$ z tezy twierdzenia. Niech, ponownie dla wygody, $M = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Rozważmy funkcję f, która liczbie ze zbioru $\mathbb{Z}_M$ przyporządkowuje jej reszty z dzielenia przez $p_1, p_2, \ldots, p_n$. Formalnie potrzebujemy funkcji $f : \mathbb{Z}_M \to \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n}$ danej wzorem

$$f(x) = (x \bmod p_1, x \bmod p_2, \ldots, x \bmod p_n).$$

Przykładowo, jeśli przyjmiemy $p_1 = 2$ i $p_2 = 5$, to wartością funkcji f dla $x = 8$ jest

$$f(8) = (8 \bmod 2, 8 \bmod 5) = (0, 3),$$

natomiast wartością dla $x = 7$ jest

$$f(7) = (7 \bmod 2, 7 \bmod 5) = (1, 2).$$

Mając już zdefiniowaną funkcję f, możemy zauważyć, że teza twierdzenia jest jednoznaczna pokazaniu, że dla każdej krotki ze zbioru $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n}$ (a więc dla każdego układu reszt z dzielenia przez $p_1, p_2, \ldots, p_n$) istnieje dokładnie jedna liczba $x \in \mathbb{Z}_M$, która przekształcona funkcją f daje tę krotkę[1].

3.2 Różnowartościowość f

Na początek pokażemy, że funkcja f jest różnowartościowa (a więc różne argumenty dają różne wyniki). Niech x i y będą dwiema różnymi liczbami ze zbioru $\mathbb{Z}_m$ i nie wprost załóżmy, że $f(x) = f(y)$.

Skoro $f(x) = f(y)$, to znaczy, że x i y dają takie same reszty z dzielenia odpowiednio przez $p_1, p_2, \ldots, p_n$, czyli liczba $x - y$ jest podzielna przez $p_1, p_2, \ldots, p_n$. Wiemy z założeń, że liczby p_i są względnie pierwsze, a więc skoro $x - y$ jest podzielna przez $p_1, p_2, \ldots, p_n$, to jest podzielna też przez ich iloczyn M.

Jest to sprzeczność, ponieważ skoro $0 \leqslant x, y < M$, to ich różnica jest większa od $-M$ i mniejsza od M, zatem, żeby była podzielna przez M, musi być równa zeru, a to stoi w sprzeczności z założeniem o tym, że x i y są równe.

3.3 Konkluzja

Skoro funkcja f jest różnowartościowa, a jej dziedzina i zbiór wartości są równoliczne i skończone, to f jest również „na” (czyli przyjmuje każdą wartość z przeciwdziedziny), a ponadto skoro f jest różnowartościowa, to f jest bijekcją, czyli każda liczba z $\mathbb{Z}_m$ ma odpowiadającą jej krotkę reszt w $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n}$ i, odwrotnie, każda krotka reszt ma odpowiadającą jej dokładnie jedną liczbę z $\mathbb{Z}_m$.

[1] Mówiąc inaczej, pokażemy, że f jest bijekcją.

4 Konstrukcja

Po abstrakcyjnym dowodzie przejdźmy do wyznaczania konkretnych rozwiązań.

4.1 Prostszy przypadek

Najpierw rozwiążemy zadanie dla dwóch kongruencji. Przypomnijmy sobie pewną rodzinę równań diofantycznych, która wystąpiła już przy okazji omawiania odwrotności modularnej:

$$ax + by = \gcd(a, b).$$

Przydatną cechą tej rodziny równań jest to, że gdy mamy już rozwiązanie (x, y) takiego równania, to modyfikując pierwszy element pary (i odpowiednio liczbę po prawej stronie równości), nie zmieniamy reszty z dzielenia przez a, ponieważ zmiana x dodaje do obu stron równiania wielokrotność a.

Niech $\gcd(a, b) = 1$ i niech (x, y) będzie rozwiązaniem równania $ax + by = 1$. Wtedy, w całkiem oczywisty sposób, liczba $1 = ax + by$ jest rozwiązaniem układu kongruencji

$$\begin{cases} z \equiv 1 \pmod{a}, \\ z \equiv 1 \pmod{b}. \end{cases}$$

Rozważmy teraz nieco inny układ kongruencji, na przykład

$$\begin{cases} z \equiv 5 \pmod{a}, \\ z \equiv 1 \pmod{b}. \end{cases}$$

Tym razem $ax+by$ nie jest już rozwiązaniem, ale możemy łatwo zmodyfikować resztę z dzielenia $ax + by$ przez a bez szkody dla reszty z dzielenia przez b. Wystarczy użyć liczby $ax+5by$, której reszty z dzielenia przez a i przez b wynoszą odpowiednio

$$ax+5by \equiv 5ax+5by \equiv 5(ax+by) \equiv 5 \cdot 1 \equiv 5 \pmod{a}$$

oraz

$$ax + 5by \equiv ax + by \equiv 1 \pmod{b},$$

a zatem liczba $ax + 5by$ spełnia drugi z żądanych przez nas układów kongruencji.

Analogicznie możemy pokazać, że, przykładowo, liczba $7ax + 9by$ spełnia układ kongruencji

$$\begin{cases} z \equiv 9 \pmod{a}, \\ z \equiv 7 \pmod{b}. \end{cases}$$

4.2 Uogólnienie

Skoro potrafimy już rozwiązywać układy kongruencji wielkości 2, to dość łatwo przejdziemy do przypadku ogólnego.

Niech

$$\begin{cases} x \equiv a_1 \pmod{p_1}, \\ x \equiv a_2 \pmod{p_2}, \\ \vdots \\ x \equiv a_n \pmod{p_n} \end{cases}$$

będzie układem kongruencji do rozwiązania.

Rozwiążmy mniejszy układ stworzony z dwóch pierwszych kongruencji powyższego. Wówczas uzyskamy rozwiązanie (powiedzmy r_2), które ma własność

$$\begin{cases} r_2 \equiv a_1 \pmod{p_1}, \\ r_2 \equiv a_2 \pmod{p_2}. \end{cases}$$

Mając już r_2, możemy zmniejszyć liczbę kongruencji w początkowym układzie o jeden, zastępując dwa początkowe równania jednym:

$$\begin{cases} x \equiv a_1 \pmod{p_1}, \\ x \equiv a_2 \pmod{p_2}, \\ \vdots \\ x \equiv a_n \pmod{p_n} \end{cases} \rightarrow \begin{cases} x \equiv r_2 \pmod{p_1 p_2}, \\ x \equiv a_3 \pmod{p_3}, \\ \vdots \\ x \equiv a_n \pmod{p_n}. \end{cases}$$

Kontynuujemy ten proces aż uzyskamy układ jednej kongruencji:

$$\begin{cases} x \equiv r_n \pmod{p_1 p_2 p_3 \cdots p_n}. \end{cases}$$

Liczba r_n będzie rozwiązaniem całego układu kongruencji.

5 Kolejne uogólnienie

Dotychczas zakładaliśmy, że wszystkie dzielniki $p_1, p_2, \ldots, p_n$, przez które reszty z dzielenia rozpatrujemy, są względnie pierwsze. Okazuje się, że czasami ten warunek nie jest konieczny.

Spróbujmy rozwiązać przykładowy układ kongruencji, w którym p_i nie są względnie pierwsze, niech będzie to układ

$$\begin{cases} x \equiv 3 \pmod{12}, \\ x \equiv 5 \pmod{10}, \\ x \equiv 10 \pmod{14}. \end{cases}$$

Możemy zapisać każdą kongruencję z powyższego układu jako koniunkcję kilku kongruencji, w których dzielniki będą potęgami liczb pierwszych – przykładowo reszta z dzielenia przez 12 wynika bezpośrednio z reszt z dzielenia przez 3 i przez 4, bo $12 = 3 \cdot 4$ oraz $\gcd(3, 4) = 1$.

Mamy więc układ

$$\begin{cases} x \equiv 0 \pmod{3}, \\ x \equiv 3 \pmod{4}, \\ x \equiv 1 \pmod{2}, \\ x \equiv 0 \pmod{5}, \\ x \equiv 0 \pmod{2}, \\ x \equiv 3 \pmod{7}. \end{cases}$$

Teraz skonfrontujmy ze sobą kongruencje, których dzielniki to potęgi tej samej liczby pierwszej:

$$\begin{cases} \begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 1 \pmod{2}, \\ x \equiv 0 \pmod{2}, \end{cases} \\ \begin{cases} x \equiv 0 \pmod{3}, \end{cases} \\ \begin{cases} x \equiv 0 \pmod{5}, \end{cases} \\ \begin{cases} x \equiv 3 \pmod{7}. \end{cases} \end{cases}$$

Jeśli uda nam się rozwiązać „małe” układy kongruencji, to wylądujemy w standardowej sytuacji, w której dzielniki są względnie pierwsze, ponieważ potęgi różnych liczb pierwszych są względnie pierwsze.

O ile w oryginalnym twierdzeniu mamy pewność, że zawsze istnieje rozwiązanie, tak w przypadku gdy dzielniki nie są względnie pierwsze tej pewności nie mamy. W powyższym przypadku tak właśnie jest: mamy kongruencję $x \equiv 1 \pmod{2}$ i obok kongruencję $x \equiv 0 \pmod{2}$, a te kongruencje są w oczywisty sposób sprzeczne.

Wobec tego, gdy otrzymujemy do rozwiązania układ kongruencji, co do którego nie mamy pewności czy jego dzielniki są względnie pierwsze, nie możemy mieć też pewności co do tego, że rozwiązanie w ogóle istnieje, ale jeśli istnieje, to da się je uzyskać w sposób opisany wyżej (rozbijając dzielniki na potęgi liczb pierwszych i operując najpierw na kongruencjach w obrębie potęg jednej liczby pierwszej).

6 Zobacz też

- https://en.wikipedia.org/wiki/Chinese_remainder_theorem
- https://brilliant.org/wiki/chinese-remainder-
- https://ctext.org/sunzi-suan-jing