I Liceum Ogólnokształcące
im. Cypriana Kamila Norwida
w Bydgoszczy

Wojciech Kretowicz

PODZIELNOŚĆ SILNI A SUMA CYFR

Opiekun Mariusz Adamczak

wojtekkretowicz@gmail.com

Bydgoszcz 2017

Spis treści

Wstęp

Rozwiązując 12 zadanie z części korespondencyjnej z tegorocznej olimpiady stanąłem przed problemem udowodnienia fałszywości pewnego równania. Pomyślałem wtedy o podzielności przez 2 i zacząłem rozmyślać nad podzielnością współczynników dwumianowych, a przez to również o podzielności silni. Zadanie udało się rozwiązać, a mi pozostało w głowie pytanie: „Czy da się udowodnione na potrzeby zadania zależności ze względu na podzielność przez 2, uogólnić na pozostałe liczby naturalne?”.

Tak krok po kroku powstała ta praca. Na samym początku przedstawiłem najbardziej podstawowe własności sumy cyfr liczb w różnych systemach i podzielności przez daną liczbę pierwszą. Na podstawie nich udowodniłem pewną zależność pomiędzy podzielnością silni a sumą cyfr jej argumentu. Pokazałem też łatwy sposób na przybliżanie tej wartości z góry przy użyciu granicy pewnego ciągu.

Udowodniłem również kilka własności sum cyfr. Przedstawiłem między innymi jej wartość w postaci sumy nie wykorzystującej cyfr, a także udowodniłem nierówność zachodzącą pomiędzy sumami cyfr a sumą cyfr sumy ich argumentów.

Na końcu zaprezentowałem jeszcze jedną funkcję i wzór na nią oraz dwa rozwiązania zadań olimpijskich w oparciu o przedstawione w pracy twierdzenia, w tym też to zadanie wspomniane na początku.

Choć do wszystkich przestawionych tu zależności doszedłem samemu, to przeglądając potem literaturę bliską tych tematów przedstawionych w mojej pracy („Cyfry liczb naturalnych” serii „Podróże po imperium liczb” Andrzeja Nowickiego) zauważyłem, że część wyników się powtarza. W wymienionej wyżej książce można spotkać wersję twierdzenia 2 dla systemu dziesiętnego oraz szczególny przypadek twierdzenia 6.

1. Podstawowe własności sumy cyfr i podzielności przez daną liczbę pierwszą

Wprowadźmy dwa oznaczenia.

Niech $d(n;k)$ dla $n,k \in \mathbb{N}$, $k \geq 2$ oznacza ile razy można maksymalnie podzielić liczbę n przez k bez reszty.

Niech $s(n;P)$ dla $n,P \in \mathbb{N}$, $P \geq 2$ oznacza sumę cyfr liczby n w systemie pozycyjnym P.

Okazuje się, że w rozpatrywanej przeze mnie podzielności (i nie tylko) suma cyfr w różnych systemach będzie wielokrotnie występowała.

W pracy będziemy wiele razy korzystali z kilku oczywistych lematów.

1. $s(k^l n;k) = s(n;k)$, dla $l \in \mathbb{N}$.
   Dowód.
   Łatwo zauważyć, że mnożąc daną liczbę przez podstawę systemu pozycyjnego w jakiej jest zapisana dopisujemy do jej końca odpowiednią ilość zer, więc suma cyfr się nie zmienia.
2. $s(kn+r;k) = s(n;k) + r$, dla $r \in \mathbb{N} \cup \{0\}$ i $0 \leq r < k$.
   Dowód.
   Po pomnożeniu liczby przez podstawę systemu pozycyjnego w jakiej jest zapisana do jej końca dopiszemy jedno zero. Jeśli następnie dodamy nieujemną liczbę naturalną mniejszą od tej podstawy (czyli cyfrę), to to zero zostanie zastąpione tą cyfrą. Zatem suma cyfr zwiększy się o dodaną wartość.
3. $s(kn+r_1;k) - s(kn+r_2;k) = r_1 - r_2$, dla $r_1, r_2 \in \mathbb{N} \cup \{0\}$ i $0 \leq r_1, r_2 < k$.
   Dowód.
   $L = s(kn+r_1;k) - s(kn+r_2;k) = s(n;k) + r_1 - s(n;k) - r_2 = r_1 - r_2 = P$
4. $d(n;k) \geq 0$.
   Dowód.
   Dowód jest oczywisty. Nie można ujemną ilość razy podzielić danej liczby bez reszty.
5. $d(kn+r;k) = 0$, dla $r \in \mathbb{N}$ i $0 < r < k$.
   Dowód:
   Łatwo zauważyć, że $kn+r$ dla $r \in \mathbb{N}, 0 < r < k$ nie jest podzielne przez k. Zatem funkcja ta zwraca zero.
6. $d(nm;p) = d(n;p) + d(m;p)$, dla dowolnej liczby pierwszej p.
   Dowód.
   Niech $n = p^a n'$ oraz $m = p^b m'$, gdzie $a,b \in \mathbb{N} \cup \{0\}$ oraz $NWD(n';p) = 1$ i $NWD(m';p) = 1$.
   $$L = d(nm;p) = d(p^{a+b}n'm';p) = a + b = d(p^a n';p) + d(p^b m') \\ = d(n;p) + d(m;p) = P$$
7. $d\left(\frac{n}{m};p\right) = d(n;p) - d(m;p)$, dla $m|n$ oraz dla dowolnej liczby pierwszej p.

Dowód.
Niech $n = p^a n'$ oraz $m = p^b m'$, gdzie $m|n$, $a, b \in \mathbb{N} \cup \{0\}$ oraz $NWD(n'; p) = 1$ i $NWD(m'; p) = 1$.

$$L = d\left(\frac{n}{m}; k\right) = d\left(k^{a-b}\frac{n'}{m'}; k\right) = a - b = d(k^a n'; k) - d(k^b m'; k)$$
$$= d(n; k) - d(m; k) = P$$

8. $d(n; k^l) = \left[\frac{d(n;k)}{l}\right]$
Dowód.
Niech $n = k^x n'$ oraz $x = ay + r$, gdzie n' nie dzieli się przez k, $0 \leq r < y$, $x, y, a, r \in \mathbb{N}$.
Oczywiście $d(n; k) = x$, $n = k^x n' = (k^y)^{\frac{x}{y}} n' = (k^y)^{a + \frac{r}{y}} n'$. Widzimy jasno, że będziemy w stanie podzielić liczbę n przez k^y y razy mniej niż dzieląc po prostu przez k. Część całkowita wynika z obecności ułamka $\frac{r}{y}$.
9. $d(n^k; p) = kd(n; p)$, dla dowolnej liczby pierwszej p.
Dowód.
Niech $n = p^x n'$, gdzie $NWD(n'; p) = 1$ i $x \in \mathbb{N} \cup \{0\}$. Wtedy: $n^k = p^{xk} n'^k$.
10. $s(n; k) \leq (k - 1)(\log_k n + 1)$
Dowód.
Liczba n w systemie pozycyjnym k ma co najwyżej $\log_k n + 1$ cyfr, z czego równość zajdzie tylko dla potęgi k równej 1. Zatem największa suma jest dla samych cyfr $k - 1$.

2. Podzielność silni a suma cyfr

Teraz możemy przejść do ogólniejszych wniosków wynikających z powyższych lematów.

Twierdzenie 1. Dla każdej liczby całkowitej nieujemnej n i dowolnej liczby pierwszej p zachodzi równość

$$d(n!;p) = \frac{n - s(n;p)}{p-1}$$

Dowód.

Do udowodnienia tego twierdzenia będziemy potrzebować dodatkowego lematu.

Lemat.

$$(k-1)d(n+1;k) = s(n;k) - s(n+1;k) + 1$$

Dowód lematu.

Rozpatrzmy dwa przypadki.

1. Niech $n = kn' + r$, gdzie $0 \leq r < k-1$.

Wtedy korzystając z lematu 2 oraz lematu 5 otrzymujemy

$$\begin{aligned} &s(n;k) - (k-1)d(n+1;k) - s(n+1;k) + 1 \\ &\qquad = s(kn'+r;k) - (k-1)d(kn'+r+1;k) - s(kn'+r+1;k) + 1 \\ &\qquad = s(n';k) + r - (k-1)0 - s(n';k) - r - 1 + 1 = 0 \end{aligned}$$

2. Niech $n = kn' + k - 1$.

Wtedy korzystając z lematu 2 mamy

$$\begin{aligned} &s(n;k) - (k-1)d(n+1;k) - s(n+1;k) + 1 \\ &\qquad = s(kn'+k-1;k) - (k-1)d(kn'+k;k) - s(kn'+k;k) + 1 \end{aligned}$$

Z definicji funkcji d oraz lematu 1 uzyskujemy dalej, że

$$\begin{aligned} &s(n;k) - (k-1)d(n+1;k) - s(n+1;k) + 1 \\ &\qquad = s(n';k) + k - 1 - (k-1)d(k(n'+1);k) - s(k(n'+1);k) + 1 \\ &\qquad = s(n';k) + k - 1 - (k-1)\big(1 + d(n'+1;k)\big) - s(n'+1;k) + 1 \\ &\qquad = s(n';k) + k - 1 - (k-1) - (k-1)d(n'+1;k) - s(n'+1;k) + 1 \\ &\qquad = s(n';k) - (k-1)d(n'+1;k) - s(n'+1;k) + 1 \end{aligned}$$

Otrzymaliśmy więc

$$\begin{aligned} &s(n;k) - (k-1)d(n+1;k) - s(n+1;k) + 1 \\ &\qquad = s(n';k) - (k-1)d(n'+1;k) - s(n'+1;k) + 1, \end{aligned}$$

gdzie $n' < n$. Powtarzając tak tę czynność uzyskamy w końcu liczbę n postaci rozpatrzonej w przypadku 1 lub w skrajnym przypadku zejdziemy do zera, które również zawiera się w pierwszym przypadku. W przeciwnym wypadku dzieląc nieskończenie długo n przez k uzyskiwalibyśmy ciągle resztę $k-1$, co nie jest możliwe – n musiałoby być nieskończenie duże (trochę inaczej patrząc: n zapisane w systemie pozycyjnym k zawierałoby nieskończenie wiele cyfr $k-1$), co kończy dowód lematu.

Twierdzenie 1 udowodnimy indukcyjnie.

Niech $n = 0$.

$$L = d(n!; p) = d(0!; p) = 0$$

$$P = \frac{n - s(n; p)}{p - 1} = \frac{0 - 0}{p - 1} = 0$$

Załóżmy, że dla pewnego $n \in \mathbb{N} \cup \{0\}$ zachodzi:

$$d(n!; p) = \frac{n - s(n; p)}{p - 1}$$

Wtedy na podstawie lematu 6. i założenia indukcyjnego

$$d\big((n+1)!; p\big) = d(n!; p) + d(n+1; p) = \frac{n - s(n; p)}{p - 1} + d(n+1; p)$$
$$= \frac{n - s(n; p) + (p-1)d(n+1; p)}{p - 1}$$

Stosując teraz wyżej udowodniony lemat uzyskujemy ostatecznie, że

$$d\big((n+1)!; p\big) = \frac{n - s(n; p) + (p-1)d(n+1; p)}{p - 1}$$
$$= \frac{n - s(n; p) + s(n; p) - s(n+1; p) + 1}{p - 1} = \frac{n + 1 - s(n+1; p)}{p - 1}$$

Zatem na mocy zasady indukcji matematycznej wnioskujemy, że twierdzenie jest prawdziwe dla każdej liczby naturalnej wraz z zerem. *c. n. d.*

Warto zauważyć, że to lemat 6. sprawia, że twierdzenie to działa tylko dla liczb pierwszych w drugim argumencie. Wszystkie inne operacje wraz z lematem z początku dowodu są prawdziwe dla wszystkich liczb naturalnych.

Twierdzenie to pozwala nam na szybkie policzenie, ile razy można podzielić $n!$ przez dowolną liczbę pierwszą.

Przykład 1.

Ile razy można podzielić przez 7 *liczbę* $1234567890!$?

Liczba ta jest bardzo duża, lecz sprawdzenie jest proste. A mianowicie

$$1234567890_{10} = 42410440203_7$$

Stąd wiemy, że $s(1234567890; 7) = 24$.

Zatem $d(1234567890!; 7) = \frac{1234567890-24}{6} = 205761311$.

Czyli $7^{205761311}$ dzieli $1234567890!$, a $7^{205761312}$ już nie.

□

Nie jest trudno zauważyć teraz, że na podstawie lematu 8. mamy $d(n!; p^r) = \left[\frac{d(n!;p)}{r}\right]$. Co jednak, jeżeli chcemy policzyć podzielność nie dla liczby pierwszej, a złożonej? Każda liczba złożona składa się z czynników pierwszych podniesionych do odpowiedniej potęgi. Należy znaleźć najmniejszą wartość funkcji $d(n!; p^r)$, gdzie p to właśnie taki czynnik pierwszy. Innymi słowy znaleźć tę wartość, która najbardziej ograniczy ilość podzieleń.

Zatem dla $k = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ mamy

$$d(n!; k) = \min\left(d\left(n!; p_1^{a_1}\right); d\left(n!; p_2^{a_2}\right); \dots; d\left(n!; p_r^{a_r}\right)\right)$$

Przykład 2.

Ile razy można maksymalnie podzielić bez reszty $77!$ *przez* 12?

Zauważmy, że $12 = 2^2 \cdot 3$.

Musimy zatem policzyć $d(77!; 2^2)$ i $d(77!; 3)$ oraz poznać sumę cyfr liczby 77 w systemie dwójkowym oraz trójkowym. Mamy więc

$$77_{10} = 1001101_2$$

$$77_{10} = 2212_3$$

$$d(77!; 2^2) = \left[\frac{d(77!; 2)}{2}\right] = \left[\frac{\frac{77 - s(77; 2)}{2-1}}{2}\right] = \left[\frac{77-4}{2}\right] = 36$$

$$d(77!; 3) = \frac{77 - s(77; 3)}{3-1} = \frac{77-7}{2} = 35$$

Wnioskujemy stąd, że $77!$ podzieli nam się dokładnie 35 razy bez reszty. □

Zauważmy, że z twierdzenia 1. wynika szczególny przypadek znanej cechy podzielności $k-1|n-s(n;k)$. Oczywistym jest, że $d(n;k) \in \mathbb{N}$. Zatem jeżeli zachodzi równość $d(n!;p) = \frac{n-s(n;p)}{p-1}$, to $p-1|n-s(n;p)$.

Ponadto zestawiając twierdzenie 1 z twierdzeniem Legendre'a możemy wyprowadzić wzór na sumę cyfr danej liczby w danym systemie o podstawie będącym liczbą pierwszą. Mamy więc

$$\frac{n-s(n;p)}{p-1} = \sum_{i\geq 1}\left[\frac{n}{p^i}\right]$$

Stąd

$$s(n;p) = n-(p-1)\sum_{i\geq 1}\left[\frac{n}{p^i}\right]$$

Okazuje się, że wzór ten jest prawdziwy dla każdej podstawy, nie tylko dla liczb pierwszych.

Twierdzenie 2. Dla dowolnej liczby całkowitej nieujemnej n i dowolnej liczby naturalnej $k \geq 2$ zachodzi

$$s(n;k) = n-(k-1)\sum_{i\geq 1}\left[\frac{n}{k^i}\right]$$

Dowód.
Niech $n = k^r a_r + k^{r-1}a_{r-1} + \cdots + k^1 a_1 + k^0 a_0$, gdzie a_i to cyfry liczby n w systemie k. Oczywistym jest, że $s(n;k) = a_r + a_{r-1} + \cdots + a_1 + a_0$. Zauważmy, że

$$\begin{aligned}\left[\frac{n}{k^i}\right] &= \left[\frac{k^r a_r + k^{r-1}a_{r-1} + \cdots + k^1 a_1 + k^0 a_0}{k^i}\right] \\ &= \left[k^{r-i}a_r + k^{r-i-1}a_{r-1} + \cdots + k^0 a_i \right.\\ &\quad \left. + \frac{k^{i-1}a_{i-1} + k^{i-2}a_{i-2} + \cdots + k^1 a_1 + k^0 a_0}{k^i}\right] \\ &= k^{r-i}a_r + k^{r-i-1}a_{r-1} + \cdots + k^0 a_i\end{aligned}$$

bo $\sum_{i=0}^{s} k^i a_i < k^{s+1}$, jeżeli tylko $a_i < k$.

Stąd

$$\begin{aligned}&n-(k-1)\sum_{i\geq 1}\left[\frac{n}{k^i}\right] = \\ &\quad = (k^r a_r + k^{r-1}a_{r-1} + \cdots + k^1 a_1 + k^0 a_0) \\ &\quad - (k-1)\big((k^{r-1}a_r + k^{r-2}a_{r-1} + \cdots + k^0 a_1) \\ &\quad + (k^{r-2}a_r + k^{r-3}a_{r-2} + \cdots + k^0 a_2) + \cdots + (k^1 a_r + k^0 a_{r-1}) + k^0 a_r\big).\end{aligned}$$

Zauważmy, że pomnożeniu $(k^{r-1}a_r + k^{r-2}a_{r-1} + \cdots + k^0 a_1)$ przez k i odjęciu od pierwszego nawiasu zostanie samo a_0. Otrzymujemy więc dalej

$$-1\left(k^{r-i}a_r + k^{r-i-1}a_{r-1} + \cdots + k^0 a_i\right) + k\left(k^{r-i-1}a_r + k^{r-i-1}a_{r-1} + \cdots + k^0 a_{i+1}\right) = -k^0 a_i = -a_i$$

Po uwzględnieniu minusa przed nawiasem $k-1$ i zsumowaniu z początkowym a_0 uzyskujemy sumę cyfr liczby n w systemie pozycyjnym $p.\ c.\ n.\ d.$

W ten oto sposób otrzymaliśmy wzór jawny na ilość cyfr danej liczby w danym systemie. Zauważmy, że z twierdzenia 2. natychmiast uzyskujemy pełną cechę podzielności, jaką wcześniej dostaliśmy dla liczb pierwszych, a mianowicie

$$k-1 | n - s(n;k)$$

<u>Przykład 3.</u>

Ile wynosi suma cyfr liczby 2017 *w systemie szóstkowym?*

Z twierdzenia 2. mamy

$$s(2017;6) = 2017 - 5\left(\left[\frac{2017}{6}\right] + \left[\frac{2017}{36}\right] + \left[\frac{2017}{216}\right] + \left[\frac{2017}{1296}\right]\right) = 2017 - 5(336 + 56 + 9 + 1) = 2017 - 2010 = 7$$

□

Twierdzenie 1. prowadzi także do następnego wniosku.

Twierdzenie 3. Dla dowolnej liczby pierwszej p zachodzi

$$\lim_{n\to\infty} \frac{d(n!;p)}{n} = \frac{1}{p-1}$$

Dowód. Z twierdzenia 1. mamy

$$\lim_{n\to\infty} \frac{d(n!;p)}{n} = \lim_{n\to\infty} \frac{n - s(n;p)}{n(p-1)} = \lim_{n\to\infty} \left(\frac{1}{p-1} - \frac{s(n;p)}{n(p-1)}\right) = \frac{1}{p-1} - \lim_{n\to\infty} \frac{s(n;p)}{n(p-1)}$$

Wykażemy, że

$$\lim_{n\to\infty} \frac{s(n;p)}{n(p-1)} = 0$$

Z lematu 10. otrzymujemy

$$1 \leq s(n;p) < (\mathrm{p}-1)(\log_p n + 1)$$

Stąd

$$\frac{1}{n(p-1)} \leq \frac{s(n;p)}{n(p-1)} < \frac{\log_p n}{n} + \frac{1}{n}$$

Widzimy, że

$$\lim_{n\to\infty} \frac{1}{n(p-1)} = 0$$

oraz że

$$\lim_{n\to\infty} \frac{1}{n} = 0$$

Wystarczy więc wykazać, że

$$\lim_{n\to\infty} \frac{\log_p n}{n} = 0$$

i wtedy na podstawie twierdzenia o trzech ciągach dostaniemy tezę.

Ponieważ $\frac{\log_p n}{n} = \log_p n^{\frac{1}{n}}$ oraz $\lim_{n\to\infty} n^{\frac{1}{n}} = 1$, to z uwagi na ciągłość logarytmu otrzymujemy, że

$$\lim_{n\to\infty} \log_p n^{\frac{1}{n}} = 0$$

c.n.d.

Twierdzenie 3. umożliwia bardzo łatwe przybliżanie wartości $d(n!;p)$. Wynosi ono bowiem

$$d(n!;p) \approx \frac{n}{p-1}$$

<u>Przykład 4</u>

Przybliżmy wartość $d(1234567890!;7)$, którą dokładnie wyliczyliśmy w poprzednim przykładzie. Z twierdzenia 2. powinna ona być bliska $\frac{1234567890}{6} = 205761315$. Wynik dokładny to 205761311. Pomyliliśmy się o $1 - \frac{205761311}{205761315} = 0{,}00000001944$.

□

Zauważmy tutaj ponadto, że w zestawieniu z twierdzeniem 1. dostajemy, że jest to również ograniczenie z góry.

3. Podzielność współczynników dwumianowych

Twierdzenie 1. prowadzi nas do jeszcze jednej własności.

Twierdzenie 4. Dla dowolnej liczby całkowitej nieujemnej n oraz dowolnej liczby całkowitej nieujemnej k nie większej od n oraz dowolnej liczby pierwszej p zachodzi

$$d\left(\binom{n}{k};p\right)=\frac{s(k;p)+s(n-k;p)-s(n;p)}{p-1}$$

Dowód.

$$L=d\left(\binom{n}{k};p\right)=d\left(\frac{n!}{k!\,(n-k)!};p\right)=d(n!;p)-d(k!;p)-d\big((n-k)!;p\big)$$

Wykorzystując lemat 6. i 7. oraz twierdzenie 1. uzyskujemy, że

$$L=\frac{n-s(n;p)-k+s(k;p)-n+k+s(n-k;p)}{p-1}=\frac{s(k;p)+s(n-k;p)-s(n;p)}{p-1}=P$$

c .n. d.

Umożliwia to na szybkie sprawdzanie podzielności współczynnika dwumianowego Newtona. Podobnie jak wyżej uczyniliśmy to dla silni, tak teraz można łatwo policzyć

$$d\left(\binom{n}{k};p^k\right)=\left[\frac{s(k;p)+s(n-k;p)-s(n;k)}{k(p-1)}\right]$$

Zauważmy też, że to, ile razy można dany współczynnik dwumianowy Newtona podzielić przez daną liczbę pierwszą, zależy jedynie od sumy cyfr liczb n, k, $n-k$, a nie zależy zupełnie od ich wielkości.

Przykład 5.

Ile razy maksymalnie można podzielić $\binom{2017}{1000}$ *przez* 11*?*

Musimy poznać sumy cyfr liczby 2017, 1000, 1017 w systemie 11. Możemy tutaj skorzystać z twierdzenia 2.

$$s(2017;11)=2017-10\left(\left[\frac{2017}{11}\right]+\left[\frac{2017}{121}\right]+\left[\frac{2017}{1331}\right]\right)=2017-10(183+16+1)$$
$$=2017-2000=17$$

$$s(1000; 11) = 1000 - 10\left(\left[\frac{1000}{11}\right] + \left[\frac{1000}{121}\right]\right) = 1000 - 10(90 + 8) = 1000 - 980 = 20$$

$$s(1017; 11) = 1017 - 10\left(\left[\frac{1017}{11}\right] + \left[\frac{1017}{121}\right]\right) = 1017 - 10(92 + 8) = 1017 - 1000 = 17$$

Zatem z twierdzenia 4.

$$d\left(\binom{2017}{1000}; 11\right) = \frac{20 + 17 - 17}{10} = 2$$

□

Możemy też uzyskać dzięki twierdzeniu 4. oraz twierdzeniu 2. ograniczenie z góry podzielności danego współczynnika Newtona.

Twierdzenie 5. Dla dowolnej liczby całkowitej nieujemnej n, k oraz dowolnej liczby pierwszej p prawdziwa jest nierówność

$$d\left(\binom{n}{k}; p\right) \leq [\log_p n]$$

Dowód.

$$\begin{aligned} d\left(\binom{n}{k}; p\right) &= \frac{s(k; p) + s(n-k; p) - s(n; p)}{p-1} \\ &= \frac{k - (p-1)\sum_{i\geq 1}\left[\frac{k}{p^i}\right] + n - k - (p-1)\sum_{i\geq 1}\left[\frac{n-k}{p^i}\right] - n + (p-1)\sum_{i\geq 1}\left[\frac{n}{p^i}\right]}{p-1} \\ &= \frac{(p-1)\sum_{i\geq 1}(\left[\frac{n}{p^i}\right] - \left[\frac{k}{p^i}\right] - \left[\frac{n-k}{p^i}\right])}{p-1} = \frac{(p-1)\sum_{i\geq 1}^{[\log_p n]}(\left[\frac{n}{p^i}\right] - \left[\frac{k}{p^i}\right] - \left[\frac{n-k}{p^i}\right])}{p-1} \\ &\leq \frac{(p-1)[\log_p n]}{p-1} = [\log_p n] \end{aligned}$$

c .n. d.

Można tu zauważyć, że wraz ze wzrostem n to górne ograniczenie podzielności współczynnika dwumianowego Newtona będzie rosło logarytmicznie, a więc bardzo wolno.

<u>Przykład 6.</u>

$$d\left(\binom{2017}{789}; 7\right) \leq [\log_7 2017] = [3{,}91 \dots] = 3$$

Zatem ta liczba nie podzieli się więcej razy przez 7 jak 3 razy. □

4. Własności sumy cyfr

Z twierdzenia 4. wynika, że $s(k;p) + s(n-k;p) - s(n;p) \geq 0$. Jedyne założenia jakie występują dla tej nierówności, to te wynikające z założeń dla symbolu Newtona. Tzn. $n \geq 0$, $k \geq 0$, $n-k \geq 0$. Podstawmy teraz za $k = a$, $n - k = b$. Wtedy oczywiście $n = a + b$. Z założeń dla n i k mamy, że $a \geq 0$ i $b \geq 0$. Otrzymujemy więc

$$s(a;p) + s(b;p) \geq s(a+b;p)$$

dla dowolnej liczby pierwszej p. Udowodnimy teraz ogólniejszą nierówność.

Twierdzenie 6. Dla dowolnych liczb całkowitych nieujemnych a_i oraz dowolnego naturalnego $k \geq 2$ i dowolnego naturalnego n zachodzi nierówność

$$\sum_{i=1}^{n} s(a_i;k) \geq s(\sum_{i=1}^{n} a_i;k)$$

Dowód.

Dowód przeprowadzimy poprzez indukcję ze względu na n.

Dla $n = 1$ nierówność staje się równością w oczywisty sposób prawdziwą.

Załóżmy teraz, że dla pewnego n zachodzi nierówność

$$\sum_{i=1}^{n} s(a_i;k) \geq s(\sum_{i=1}^{n} a_i;k)$$

Korzystając z twierdzenia 2. mamy

$$\begin{aligned} s(a;k) + s(b;k) &= a - (k-1)\sum_{i\geq 1}\left[\frac{a}{k^i}\right] + b - (k-1)\sum_{i\geq 1}\left[\frac{b}{k^i}\right] \\ &= (a+b) - (k-1)\sum_{i\geq 1}\left(\left[\frac{a}{k^i}\right] + \left[\frac{b}{k^i}\right]\right) \geq (a+b) - (k-1)\sum_{i\geq 1}\left[\frac{a+b}{k^i}\right] \\ &= s(a+b;k) \end{aligned}$$

Wykorzystując teraz założenie indukcyjne oraz wyżej udowodnioną nierówność otrzymujemy

$$\sum_{i=1}^{n+1} s(a_i;k) = \sum_{i=1}^{n} s(a_i;k) + s(a_{n+1};k) \geq s(\sum_{i=1}^{n} a_i;k) + s(a_{n+1};k) \geq s(\sum_{i=1}^{n+1} a_i;k)$$

Zatem na mocy zasady indukcji matematycznej wnioskujemy, że twierdzenie jest prawdziwe dla każdej liczby naturalnej. *c. n. d.*

Przykład 7.

Udowodnij, że stosunek sumy cyfr kwadratu dowolnej liczby całkowitej do sumy jej cyfr jest niewiększy od niej samej w dowolnym systemie.

Niech n będzie dowolną liczbą naturalną, a k dowolną liczbą naturalną większą od 1. Wykorzystując twierdzenie 6. dla n liczb n mamy

$$n \cdot s(n;k) = \sum_{i=1}^{n} s(n;k) \geq s(\sum_{i=1}^{n} n;k) = s(n^2;k)$$

Stąd otrzymujemy tezę

$$n \geq \frac{s(n^2;k)}{s(n;k)}$$

□

Przykład 8.

Udowodnij, że nie więcej jedynek będzie w zapisie 64-bitowym sumy 8 liczb 8-bitowych całkowitych dodatnich niż gdyby zapisać je obok siebie na tych 64 bitach w zapisie U1.

Ilość jedynek w tym przypadku to suma cyfr danej liczby. Zatem zadanie sprowadza się do prostego użycia nierówności z twierdzenia 6.

$$s\left(\sum_{i=1}^{8} a_i\,;2\right) \leq \sum_{i=1}^{8} s(\,a_i;2)$$

□

Nierówność tę można też łatwo dalej rozszerzyć.

Mamy liczbę $n = k^r a_r + k^{r-1}a_{r-1} + \cdots + k^1 a_1 + k^0 a_0$, a liczby $a_r, a_{r-1} \ldots a_0$ to jej cyfry w systemie pozycyjnym o podstawie $k \in \mathbb{N}$, $k \geq 2$. Chcemy znaleźć pewną relację między $s(n;k)$ a $s(n;k^l)$. Zauważmy, że

$$\begin{aligned} n = k^r a_r + k^{r-1}a_{r-1} + \cdots + k^1 a_1 + k^0 a_0 \\ &= (k^l)^0(k^0 a_0 + k^1 a_1 + \cdots + k^{l-1}a_{l-1}) \\ &+ (k^l)^1(k^0 a_l + k^1 a_{l+1} + \cdots + k^{l-1}a_{2l-1}) \\ &+ (k^l)^2(k^0 a_{2l} + k^1 a_{2l+1} + \cdots + k^{l-1}a_{3l-1}) + \cdots \\ &+ (k^l)^m(k^0 a_{ml} + p^1 a_{ml+1} + \cdots) \end{aligned}$$

Teraz cyframi liczby n w systemie k^l są: $(k^0 a_0 + k^1 a_1 + \cdots + k^{l-1}a_{l-1})$, $(k^0 a_l + k^1 a_{l+1} + \cdots + k^{l-1}a_{2l-1})$,…,$(k^0 a_{ml} + k^1 a_{ml+1} + \cdots)$. Łatwo zauważyć, że

$$\begin{aligned} (k^0 a_0 + k^1 a_1 + \cdots + k^{l-1}a_{l-1}) + (k^0 a_l + k^1 a_{l+1} + \cdots + k^{l-1}a_{2l-1}) + \cdots \\ + (k^0 a_{ml} + k^1 a_{ml+1} + \cdots) \geq a_0 + a_1 + \cdots + a_r \end{aligned}$$

Mamy więc, że

$$s(n;k^l) \geq s(n;k)$$

Odnosząc to do twierdzenia 6 dostajemy

$$s(\sum_{i=1}^{n} a_i;k) \leq \sum_{i=1}^{n} s(a_i;k) \leq \sum_{i=1}^{n} s(a_i;k^{l_i})$$

gdzie l_i to dowolne potęgi naturalne.

Wnioskiem z ostatnich dwóch nierówności jest na przykład to, że zamieniając liczbę zapisaną w systemie dwójkowym na dowolny inny system o podstawie będącym potęgą dwójki otrzymamy większą sumę jej cyfr.

Przykład 9.

Mamy daną liczbę

$$110000100111000000010010110110101111000000010100000000110_2$$

Z góry wiemy, że jeżeli zapiszemy ją w systemie szesnastkowym to uzyskamy większą sumę cyfr. Przeliczmy to jednak.

Suma cyfr tej liczby w systemie dwójkowym to 21. Ta sama liczba w systemie szesnastkowym jest postaci

$$613812DAF02806_{16}$$

Stąd suma jej cyfr wynosi 75.

□

W twierdzeniach 4 i 5 wykazaliśmy, że

$$d\left(\binom{n}{k};p\right) = \frac{s(k;p)+s(n-k;p)-s(n;p)}{p-1} \leq \left[\log_p n\right]$$

Teraz możemy to odnieść jeszcze do twierdzenia 6. Mamy więc

$$s(k;p)+s(n-k;p)-s(n;p) \geq 0$$

Uzyskujemy tak, że

$$0 \leq s(k;p)+s(n-k;p)-s(n;p) \leq (p-1)\left[\log_p n\right]$$

Podstawmy teraz za $k=a$, $n-k=b$. Wtedy $n=a+b$. Dostajemy tak, że dla dowolnych nieujemnych liczb całkowitych a i b oraz dowolnej liczby pierwszej p zachodzi

$$0 \leq s(a;p)+s(b;p)-s(a+b;p) \leq (p-1)\left[\log_p(a+b)\right]$$

Okazuje się, że twierdzenie to jest prawdziwe dla wszystkich podstaw, nie tylko dla liczb pierwszych. Skorzystamy tu, podobnie jak wyżej dowodziliśmy ograniczenie podzielności dla współczynnika dwumianowego Newtona, z twierdzenia 2.

$$
\begin{aligned}
s(a;k) + s(b;k) - s(a+b;k) \\
&= a - (k-1)\sum_{i\geq 1}\left[\frac{a}{k^i}\right] + b - (k-1)\sum_{i\geq 1}\left[\frac{b}{k^i}\right] - a - b + (k-1)\sum_{i\geq 1}\left[\frac{a+b}{k^i}\right] \\
&= (k-1)\sum_{i\geq 1}(\left[\frac{a+b}{k^i}\right] - \left[\frac{a}{k^i}\right] - \left[\frac{b}{k^i}\right]) \\
&= (k-1)\sum_{i=1}^{[\log_k(a+b)]}\left(\left[\frac{a+b}{k^i}\right] - \left[\frac{a}{k^i}\right] - \left[\frac{b}{k^i}\right]\right) \leq (k-1)[\log_k(a+b)]
\end{aligned}
$$

Udowodniliśmy więc kolejne twierdzenie.

Twierdzenie 7. Dla dowolnych liczb nieujemnych całkowitych a, b oraz dowolnej liczby naturalnej $k \geq 2$ zachodzi

$$0 \leq s(a;k) + s(b;k) - s(a+b;k) \leq (k-1)[\log_k(\, a+b)]$$

Twierdzenie to, prawdziwe dla dwóch liczb, nie jest jednak prawdziwe dla dowolnej ilości liczb, co pokazuje ten kontrprzykład.

Weźmy liczby 39, 478, 1399, 1, 783 oraz system siódemkowy. Dzięki twierdzeniu 6. wiemy, że ta wartość jest z całą pewnością nieujemna.

$$
\begin{aligned}
0 \leq s(39;7) + s(478;7) + s(1399;7) + s(1;7) + s(783;7) \\
&- s(39+478+1399+1+783;7) = 9 + 10 + 13 + 1 + 15 - s(2700;7) \\
&= 48 - 12 = 36
\end{aligned}
$$

Ale

$$(7-1)[\log_7 2700] = 24$$

co przeczy tezie.

□

5. O pewnych dwóch funkcjach

Rozpatrzmy jeszcze funkcję $\theta_p(n)$ zdefiniowaną następująco

$$\theta_p(n) = d(\prod_{k=0}^{n} \binom{n}{k}; p)$$

Mówi ona o tym, ile razy można podzielić iloczyn wszystkich współczynników dwumianowych o górnym argumencie równym n przez daną liczbę pierwszą p. Udało mi się wyprowadzić wzór na tę funkcję dla $p = 2$. Wzór ten wygląda następująco

$$\theta_2(n) = \sum_{k \geq 0} \sigma(n; k)$$

gdzie

$$\sigma(n; k) = \begin{cases} 0, \text{ gdy } k \geq [\log_2 n] + 2 \text{ lub gdy na } k - tej \text{ pozycji liczby n znajduje się 0} \\ s(n; 2), \qquad \text{gdy } k = [\log_2 n] + 1 \\ ([\log_2 n] - s(n; 2) + 2(x_k - 1) - k) \cdot 2^{[\log_2 n] - k} \text{ w przeciwnym wypadku.} \end{cases}$$

Cyfry liczby n numerujemy od lewej strony, a numerację zaczynamy od 0, a x_k oznacza ilość jedynek jakie wystąpiły do pozycji $k - tej$ włącznie.

Przykład 10.

Wyliczymy teraz dla przykładu $\theta_2(234)$. Zatem wyliczmy odpowiednie wartości funkcji σ.

$$234_{10} = 11101010_2$$

$$[\log_2 234] = 7$$

$$s(234; 2) = 5$$

Na początku trafiamy na trzy jedynki.

$$\sigma(11101010_2; 0) = (7 - 5 + 2(1 - 1) - 0) \cdot 2^{7-0} = 256$$

$$\sigma(11101010_2; 1) = (7 - 5 + 2(2 - 1) - 1) \cdot 2^{7-1} = 192$$

$$\sigma(11101010_2; 2) = (7 - 5 + 2(3 - 1) - 2) \cdot 2^{7-2} = 128$$

Teraz natrafiamy na jedno zero.

$$\sigma(11101010_2; 3) = 0$$

Teraz znów 1.

$$\sigma(11101010_2;4) = (7-5+2(4-1)-4)\cdot 2^{7-4} = 32$$

Na piątym tak numerowanym miejscu jest znów 0.

$$\sigma(11101010_2;5) = 0$$

$$\sigma(11101010_2;6) = (7-5+2(5-1)-6)\cdot 2^{7-6} = 8$$

$$\sigma(11101010_2;7) = 0$$

Teraz $k = 7+1$, czyli $k = [\log_2 234] + 1$, więc

$$\sigma(11101010_2;8) = s(234;2) = 5$$

Wszystkie pozostałe wartości funkcji σ, z uwagi na to, że ich drugi argument jest nie mniejszy od $[\log_2 234] + 2$ są równe 0.

Zatem

$$\theta_2 = 256 + 192 + 128 + 32 + 8 + 5 = 621$$

Stąd iloczyn całego takiego „rzędu" współczynników dwumianowych jest podzielny przez 2^{621}.

□

Przy użyciu tego wzoru, znając zapis dwójkowy liczby n, dowodzenie pewnych własności funkcji θ_2 staje się mechaniczne. Można nawet powiedzieć, że da się tak tworzyć dowolnie dużo różnych równości. Dla przykładu udowodnimy jej dwie własności. Pierwszą nawet na dwa sposoby w oparciu o wcześniejsze rozważania.

Twierdzenie 8. Dla dowolnej liczby naturalnej *n* prawdziwe są równości

$$\theta_2(2^n - 1) = 0$$

$$\theta_2(2^n + 2^{n-1} - 1) = 2^{n-1}$$

Dowód 1.1. W pierwszym dowodzie zrobimy to dla każdej liczby pierwszej p.

Ponieważ $P^n - 1$ jest złożone tylko z największej cyfry występującej w systemie o podstawie P, to odejmując dowolną liczbę niewiększą od niej, tak naprawdę odejmujemy tylko ich cyfry. Łatwo wtedy zauważyć, że

$$s(k;P) + s(P^n - 1 - k;P) = s(P^n - 1;P)$$

Stąd jednak wynika, że

$$d\left(\binom{p^n-1}{k};p\right) = \frac{s(k;p) + s(p^n-1-k;p) - s(p^n-1;p)}{p-1} = 0$$

Stąd już w oczywisty sposób dostajemy, że

$$\theta_p(p^n - 1) = 0$$

Dowód 1.2. Teraz udowodnimy to samo w oparciu o podany wyżej wzór. Zauważmy na początku, że $2^n - 1$ w zapisie dwójkowym składa się z samych jedynek. Zatem $x_k = k + 1$, $s(2^n - 1; 2) = n$ oraz $[\log_2 2^n - 1] = n - 1$. Wobec tego

$$\begin{aligned}
\theta_2(2^n - 1) &= \sum_{k \geq 0} \sigma(2^n - 1; k) = \sum_{k=0}^{[\log_2 2^n - 1]+1} \sigma(2^n - 1; k) \\
&= \sum_{k=0}^{[\log_2 2^n - 1]} \sigma(2^n - 1; k) + \sigma(2^n - 1; [\log_2 2^n - 1] + 1) \\
&= \sum_{k=0}^{n-1} \sigma(2^n - 1; k) + s(2^n - 1; 2) \\
&= \sum_{k=0}^{n-1} ([\log_2 2^n - 1] - s(2^n - 1; 2) + 2(k + 1 - 1) - k) \cdot 2^{[\log_2 2^n - 1] - k} + n \\
&= \sum_{k=0}^{n-1} (n - 1 - n + 2k - k) \cdot 2^{n-1-k} + n = \sum_{k=0}^{n-1} (k - 1) \cdot 2^{n-1-k} + n \\
&= 2^{n-1} \sum_{k=0}^{n-1} \frac{k-1}{2^k} + n = 2^{n-1} \left(\sum_{k=0}^{n-1} \frac{k}{2^k} - \sum_{k=0}^{n-1} \frac{1}{2^k} \right) + n \\
&= 2^{n-1} \left(\left(2 - \frac{n - 1 + 2}{2^{n-1}} \right) - 2 - \frac{1}{2^{n-1}} \right) + n = -2^{n-1} \cdot \frac{n}{2^{n-1}} + n = 0
\end{aligned}$$

Skorzystaliśmy tutaj z powszechnie znanego wzoru

$$\sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$$

□

Dowód 2.

Oczywiście

$$2^n + 2^{n-1} - 1 = 10111 \ldots 1_2$$

Zauważmy tutaj, że $[\log_2 2^n + 2^{n-1} - 1] = n$, $s(2^n + 2^{n-1} - 1; 2) = n$ oraz że $x_k = k$ dla $k \geq 2$. Tutaj również skorzystamy z tego samego wzoru na sumę ułamków $\frac{k}{2^k}$. Mamy więc

$$
\begin{aligned}
\theta_2(2^n+2^{n-1}-1) &= \sum_{k\geq 0}\sigma(2^n+2^{n-1}-1;k)\\
&= \sigma(2^n+2^{n-1}-1;0) + \sum_{k=2}^{[\log_2 2^n+2^{n-1}-1]}\sigma(2^n+2^{n-1}-1;k)\\
&\quad + \sigma(2^n+2^{n-1}-1;[\log_2 2^n+2^{n-1}-1]+1) =
\end{aligned}
$$

$$
\begin{aligned}
&= ([\log_2 2^n+2^{n-1}-1] - s(2^n+2^{n-1}-1;2) + 2(1-1)+0)\cdot 2^{[\log_2 2^n+2^{n-1}-1]-0}\\
&\quad + \sum_{k=2}^{n}([\log_2 2^n+2^{n-1}-1] - s(2^n+2^{n-1}-1;2) + 2(x_k-1)+k)\\
&\quad \cdot 2^{[\log_2 2^n+2^{n-1}-1]-k} + s(2^n+2^{n-1}-1;2) = 0 + \sum_{k=2}^{n}(k-2)\cdot 2^{n-k} + n\\
&= 2^n\left(\sum_{k=2}^{n}\frac{k}{2^k} - 2\sum_{k=2}^{n}\frac{1}{2^k}\right) + n = 2^n\left(\left(2-\frac{n+2}{2^n}-\frac{1}{2}\right)-1+\frac{1}{2^{n-1}}\right)+n\\
&= 2^n\left(\frac{1}{2}-\frac{n}{2^n}\right)+n = 2^{n-1}
\end{aligned}
$$

□

Zauważmy, że z twierdzenia 4. oraz lematu 6. wynika także, że

$$
\begin{aligned}
\theta_p(n) &= \sum_{k=0}^{n}\big(s(k;p)+s(n-k;p)-s(n;p)\big)\\
&= \sum_{k=0}^{n}s(k;p) + \sum_{k=0}^{n}s(n-k;p) - (n+1)s(n;p)\\
&= 2\sum_{k=0}^{n}s(k;p) - (n+1)s(n;p)
\end{aligned}
$$

Zatem

$$
\sum_{k=0}^{n}s(k;p) = \frac{1}{2}\big(\theta_p(n)+(n+1)s(n;p)\big)
$$

Stąd przy użyciu przedstawionego wzoru dla θ_2 można wyliczać odpowiednie wartości tej funkcji, a następnie wstawiać do tej równości i uzyskać sumę cyfr wszystkich liczb naturalnych niewiększych od n. Na przykład na podstawie tych dwóch udowodnionych własności funkcji θ_2 (twierdzenie 8.) dostajemy, że dla $n = 2^m - 1$

$$
\sum_{k=0}^{n}s(k;2) = \sum_{k=0}^{2^m-1}s(k;2) = \frac{1}{2}\big(\theta_2(n)+(n+1)s(n;2)\big) = \frac{1}{2}(0+2^m\cdot m) = m2^{m-1}
$$

Tutaj możemy jeszcze zauważyć, że

$$\sum_{k=0}^{2^m-1} s(k;2) = m2^{m-1} = \sum_{k=1}^{m} k\binom{m}{k}$$

Można też tak uzyskać wzór na sumę cyfr wszystkich liczb naturalnych n-cyfrowych w systemie dwójkowym. Jest to bowiem

$$\sum_{k=0}^{2^m-1} s(k;2) - \sum_{k=0}^{2^{m-1}-1} s(k;2) = m2^{m-1} - (m-1)2^{m-2} = 2^{m-2}(2m-m+1)$$
$$= (m+1)2^{m-2}$$

Z drugiego równania w twierdzeniu 8. dostajemy, że dla $n = 2^m + 2^{m-1} - 1$

$$\sum_{k=0}^{n} s(k;2) = \sum_{k=0}^{2^m+2^{m-1}-1} s(k;2) = \frac{1}{2}(2^{m-1} + (2^m + 2^{m-1})m) = 2^{m-2}(2m+m+1)$$
$$= (3m+1)2^{m-2}$$

Oczywiście przy użyciu tego wzoru można „generować” dowolnie dużo podobnych równości. Wystarczy chociażby obrać pewne dowolne zestawienie potęg dwójki i po prostu zobaczyć co w rezultacie otrzymamy. Ja zaprezentowałem dwie przeze mnie wybrane.

6. Zastosowania w zadaniach olimpijskich

Przy użyciu przedstawionych wyżej twierdzeń i własności zadanie 6. z finałów XLIII olimpiady matematycznej staje się dość proste.

<u>*Zadanie.*</u>

Udowodnić, że dla każdej liczby naturalnej k liczba $(k!)^{k^2+k+1}$ jest dzielnikiem liczby $(k^3)!$.

Rozwiązanie.

Chodzi tu o wykazanie nierówności

$$d\big((k^3)!; p\big) - d\big((k!)^{k^2+k+1}; p\big) \geq 0$$

dla każdej liczby pierwszej $p < \sqrt{k}$ (w $(k!)^{k^2+k+1}$ nie pojawią się liczby pierwsze większe). Wystarczy teraz tę nierówność zapisać (twierdzenie 1. oraz lemat 9.):

$$\frac{k^3 - s(k^3; p)}{p-1} - (k^2+k+1)\frac{k - s(k; p)}{p-1} \geq 0$$

Co jest równoważne:

(1) $$(k^2+k+1)s(k; p) - k^2 - k - s(k^3; p) \geq 0$$

Załóżmy, że $s(k; p) \geq 2$. Wtedy

(2) $$(k^2+k+1)s(k; p) - k^2 - k - s(k^3; p) \geq k^2 + k + 2 - s(k^3; p)$$

Oczywistym jest (lemat 10.), że

(3) $$s(k^3; p) < (p-1)(\log_p k^3 + 1) = p - 1 + \frac{3(p-1)}{\log_k p}$$

Łatwo zauważyć, że $p - 1$ wraz ze wzrostem p rośnie.

Udowodnimy, że i funkcja $f(p) = \frac{3(p-1)}{\log_k p}$ jest rosnąca.

$$f'(p) = \frac{3\log_k p - \frac{3(p-1)}{p \ln k}}{\log^2{}_k p} \geq 0 \Leftrightarrow \log_k p - \frac{p-1}{p \ln k} \geq 0$$

Ponieważ $k \geq 1$, to ta nierówność jest równoważna kolejno nierównościom

$$p \ln k \log_k p - p + 1 \geq 0$$

$$p \ln k^{\log_k p} - p + 1 \geq 0$$

$$p(\ln p - 1) + 1 \geq 0$$

Teraz widać jasno, że dla $p \geq e$ nierówność ta na pewno zajdzie. Zatem dla $p \geq 3$ funkcja $f(p)$ rośnie. Ręcznie pokażemy też, że $f(2) < f(3)$.

$$f(3) - f(2) = \frac{6}{\log_k 3} - \frac{3}{\log_k 2} = \frac{3(2\log_k 2 - \log_k 3)}{\log_k 2 \log_k 3} = \frac{3(\log_k 4 - \log_k 3)}{\log_k 2 \log_k 3} > 0$$

bo oczywiście $\log_k 4 - \log_k 3 > 0$. Zatem funkcja $f(p)$ rośnie w całej dziedzinie, czyli zbiorze liczb pierwszych. Tak więc na mocy (3) oraz z tym, że $p - 1$ rośnie wraz z p uzyskujemy, że

$$s(k^3; p) < (p-1)\,(\log_p k^3 + 1) = p - 1 + \frac{3(p-1)}{\log_k p}$$
$$< \sqrt{k} - 1 + \left(\sqrt{k} - 1\right)\log_{\sqrt{k}} k^3 = 7(\sqrt{k} - 1)$$

Wracając do (2) otrzymujemy

$$k^2 + k + 2 - s(k^3; p) > k^2 + k + 2 - 7\left(\sqrt{k} - 1\right) = k^2 + k - 7\sqrt{k} + 9 \geq k^2 - 6k + 9$$
$$= (k-3)^2 \geq 0$$

Przejście $\sqrt{k} \leq k$ jest prawdziwe dla wszystkich liczb naturalnych.

Zatem nierówność ta jest zawsze prawdziwa dla $s(k; p) \geq 2$. Pozostał tylko przypadek, gdy $s(k; p) = 1$. Oznacza to, że k jest potęgą p, więc i k^3 jest potęgą p. Stąd $s(k^3; p) = 1$. Po podstawieniu do (1) tych dwóch wartości funkcji s uzyskujemy równość z zerem.

Tak oto rozwiązaliśmy finałowe zadanie olimpiady matematycznej.

Na koniec już rozwiążemy ostatnie zadanie z części korespondencyjnej LXVIII olimpiady matematycznej, które zostało przeze mnie wspomniane na wstępie.

Zadanie 12.

Niech α będzie taką liczbą rzeczywistą, że $tg(\alpha\pi) = \sqrt{2}$. Rozstrzygnąć, czy α musi być liczbą wymierną.

Rozwiązanie.

Załóżmy, że $\alpha \in \mathbb{Q}$ i $\alpha = \frac{n}{m}$. Niech $z = \cos\frac{\pi}{m} + i\sin\frac{\pi}{m}$. Korzystając ze wzoru de Moivre'a otrzymujemy $z^m = -1$. Łatwo zauważyć, że $\frac{1}{z} = \frac{1}{\cos\frac{\pi}{m} + i\sin\frac{\pi}{m}} = \frac{\cos\frac{\pi}{m} - i\sin\frac{\pi}{m}}{\cos^2\frac{\pi}{m} + \sin^2\frac{\pi}{m}} = \cos\frac{\pi}{m} - i\sin\frac{\pi}{m}$. Stąd dostajemy, że $\sin\frac{\pi}{m} = \frac{1}{2i}\left(z - \frac{1}{z}\right)$, a ze względu na wzór de Moivre'a:

$\sin n\frac{\pi}{m} = \frac{1}{2i}\left(z^n - \frac{1}{z^n}\right)$.

Analogicznie $\cos\frac{\pi}{m} = \frac{1}{2}\left(z + \frac{1}{z}\right)$, a $\cos n\frac{\pi}{m} = \frac{1}{2}\left(z^n + \frac{1}{z^n}\right)$. Dzięki temu możemy wyliczyć z^{2n}:

$$\sqrt{2} = tg(\alpha\pi) = \frac{\sin(\alpha\pi)}{\cos(\alpha\pi)} = \frac{\sin(n\frac{\pi}{m})}{\cos(n\frac{\pi}{m})} = \frac{\frac{1}{2i}\left(z^n - \frac{1}{z^n}\right)}{\frac{1}{2}\left(z^n + \frac{1}{z^n}\right)} = \frac{z^{2n} - 1}{(z^{2n} + 1)i}$$

Stąd

$$z^{2n}\sqrt{2}i + i\sqrt{2} = z^{2n} - 1$$

$$z^{2n} = -\frac{1}{3} + \frac{2\sqrt{2}}{3}i$$

Łatwo zauważyć, że

$$z^{2nm} = z^{2nm}$$

$$(z^{2n})^m = (z^m)^{2n}$$

$$(-\frac{1}{3} + \frac{2\sqrt{2}}{3}i)^m = (-1)^{2n} = 1$$

Uzyskujemy tak, implikację

$$\alpha \in \mathbb{Q} \Rightarrow \bigvee_{m\in\mathbb{N}} (-\frac{1}{3} + \frac{2\sqrt{2}}{3}i)^m = 1$$

Załóżmy zatem, że $\bigvee_{m\in\mathbb{N}} (-\frac{1}{3} + \frac{2\sqrt{2}}{3}i)^m = 1$. Równoważnym zdaniem do niego jest $\bigvee_{m\in\mathbb{N}} (-1 + 2\sqrt{2}i)^m = 3^m$. Część nierzeczywista tej liczby jest równa zero. Korzystając ze wzoru dwumianowego Newtona rozpisujemy część nierzeczywistą

$$\pm\binom{m}{1}(2\sqrt{2}i)^1 \pm \binom{m}{3}(2\sqrt{2}i)^3 \pm \binom{m}{5}(2\sqrt{2}i)^5 \pm \cdots \pm \binom{m}{2k+1}(2\sqrt{2}i)^{2k+1} \pm \cdots = 0$$

Znaki jakie się tam pojawiają oraz to, na której dokładnie wartości kończy się ta suma zależy od reszty z dzielenia przez 4 liczby m. Nas jednak to nie interesuje, my zajmiemy się jedynie podzielnością przez 2.

$$(2\sqrt{2}i)^{2k+1} = (2^{\frac{3}{2}}i)^{2k+1} = \pm 2^{3k+\frac{3}{2}}i = \pm 2^{3k} \cdot 2\sqrt{2}i$$

Podzielmy stronami przez $2\sqrt{2}i$, otrzymujemy wtedy:

$$\pm\binom{m}{1}2^0 \pm \binom{m}{3}2^3 \pm \binom{m}{5}2^6 \pm \cdots \pm \binom{m}{2k+1}2^{3k} \pm \cdots = 0$$

Wykorzystując twierdzenie 4. mamy

$$
\begin{aligned}
d\left(\binom{n}{2k+1};2\right) - d\left(\binom{n}{1};2\right) \\
&= s(2k+1;2) + s(n-2k-1;2) - s(n;2) - s(1;2) - s(n-1;2) \\
&+ s(n;2) = s(k;2) + 1 + s(n-2k-1;2) - 1 - s(n-1;2) \\
&= s(k;2) + s(n-2k-1;2) - s(n-1;2) \\
&= s(2k;2) + s(n-2k-1;2) - s(n-1;2) \geq 0
\end{aligned}
$$

Nierówność wynika z twierdzenia 7. Pokazaliśmy, że każdy współczynnik dwumianowy Newtona o nieparzystym indeksie można podzielić co najmniej tyle razy przez 2, co współczynnik z indeksem 1. W naszej równości każdy współczynnik o nieparzystym indeksie większym od 1 jest dodatkowo mnożony razy odpowiednią potęgę dwójki większą od 1. Zatem w tej równości każdy nieparzysty współczynnik dwumianowy Newtona można podzielić więcej razy przez 2 niż współczynnik z indeksem 1. Dzieląc teraz równość stronami przez największą potęgę dwójki przez jaką dzieli się $\binom{m}{1}$ uzyskamy po lewej stronie dokładnie jeden wyraz nieparzysty i same wyrazy parzyste, podczas gdy po prawej stronie jest liczba parzysta. Uzyskujemy równość liczby nieparzystej z parzystą – sprzeczność. Zatem założenie, że $\alpha \in \mathbb{Q}$ prowadzi nas do sprzeczności. Stąd α jest niewymierna.

Bibliografia

[1] M. Aigner, G. Ziegler, *Dowody z Księgi*, Wydawnictwo Naukowe PWN, Warszawa 2002,

[2] R. L. Graham, D. E. Knuth, O. Patashnik, *Matematyka konkretna*, Wydawnictwo Naukowe PWN, Warszawa 1998.

[3] A. Nowicki, *Cyfry liczb naturalnych*,

http://www-users.mat.umk.pl/~anow/imperium/cyf03.pdf