Podzielność

Będziemy się dziś zajmować jednym tylko pojęciem: ord_p.

Definicja 1 ($ord_p(n)$) *Niech $n, p \in \mathbb{N}$, przy czym p – liczba pierwsza. Przez $ord_p(n)$ oznaczamy takie $k \in \mathbb{N} \cup \{0\}$, że $p^k \mid n$, ale $p^{k+1} \nmid n$.*

Po ludzku: maksymalna potęga z jaką p wchodzi do rozkładu n, o ile wchodzi :)

Pojęcie to jest niczym innym jak narzędziem ułatwiającym korzystanie z twierdzenia o jednoznaczności rozkładu na czynniki pierwsze. Zamiast pisać rozkład każdej z nich, oznaczać jakoś nieznane bliżej liczby pierwsze i używać wielu niepotrzebnych indeksów, ord_p działa dla każdej liczby pierwszej. Także tej, która nie wchodzi do rozkładu. Jest to zatem coś na kształt teorioliczbowego logarytmu, tylko bardziej subtelnego.
Aby móc wykorzystać to pojęcie w praktyce, odnotujmy wspólnie kilka jego oczywistych własności.

Uwaga 1 *Niech a, b – liczby naturalne, zaś p – liczba pierwsza. Wówczas:*

$$\begin{aligned} ord_p(ab) &= ord_p(a) + ord_p(b), \\ ord_p(a/b) &= ord_p(a) - ord_p(b), \\ ord_p(NWD(a,b)) &= \min(ord_p(a), ord_p(b)), \\ ord_p(NWW(a,b)) &= \max(ord_p(a), ord_p(b)). \end{aligned}$$

noindent Dla ułatwienia zapisu w dalszym ciągu $NWD(a, b)$ oznaczać będziemy przez (a,b), natomiast $NWW(a, b)$ przez [a,b].

Zadanie 1 *Udowodnij, że $(a, b) \cdot [a, b] = ab$.*

Użyjemy naszego nowego narzędzia. Stosować będziemy też oczywiście powyższe stwierdzenie. Z twierdzenia o jednoznaczności rozkładu dla każdej liczby pierwszej p mamy:

$$\begin{aligned} ord_p((a,b) \cdot [a,b]) &= ord_p(ab) \\ ord_p((a,b)) + ord_p([a,b]) &= ord_p(a) + ord_p(b) \\ \min(ord_p(a), ord_p(b)) + \max(ord_p(a), ord_p(b)) &= ord_p(a) + ord_p(b) \end{aligned}$$

Ostatnia równość jest oczywiście prawdziwa.

Nowa funkcja może mieć oczywiście więcej argumentów i nie ma wątpliwości co oznacza zapis $ord_p(a_1, a_2, \ldots, a_n)$.
No to teraz jakiś ochotnik na pewno zechce szybko uzasadnić następujące równości.

Zadanie 2

$$(a,b,c) = ((a,b),c) = (a,(b,c))$$
$$[a,b,c] = [[a,b],c] = [a,[b,c]]$$

Sprawy można naturalnie komplikować, dokładać jakieś warunki...

Zadanie 3 *Niech $ab = cd$. Wykaż, że:*

$$\frac{(a,c)\cdot(a,d)}{(a,b,c,d)} = a.$$

Rozumowanie będzie podobne jak wcześniej. Teraz jednak dochodzi nowy warunek. Jeśli przyjmiemy, że:

$$ord_p(a) = A, ord_p(b) = B, ord_p(c) = C, ord_p(d) = D,$$

wówczas przy założeniu: $A + B = C + D$ wykazujemy równość:

$$\min(A,C) + \min(A,D) - \min(A,B,C,D) = A.$$

Oczywiście, nie wolno za bardzo przyzwyczajać się do jednej metody i zapominać o co chodzi z rozkładem na czynniki pierwsze. Przyjrzyjmy się następującemu zadaniu.

Zadanie 4

Dane są liczby naturalne a, b, c, d takie, że $ab = cd \neq 0$. Wykaż, że istnieją takie liczby naturalne u, w, v, x, że:

$$a = uv, \quad b = wx, \quad c = uw, \quad d = vx.$$

I tu można startować z ord. Gdy trzeba jednak wykazywać istnienie, rzecz staje się mniej korzystna. Cóż nam po tym, że jeśli oznaczymy $ord_p(a) = A, ord_p(b) = B, ord_p(c) = C, ord_p(d) = D$, to $A+B = C+D$? Widać, że poszukiwane u, v, w, x to jakieś elementy rozkładu, tu trzeba się wgryźć i nie ma siły (a przynajmniej tak mi się wydaje...). Rozwiązanie w 'tradycyjnym' stylu jest zupełnie standardowe, wgryzamy się tak długo, aż dostaniemy to, co chcemy.

Niech $u = (a,c)$. Istnieją $(a_1, c_1) = 1$, że $ua_1 = a$ oraz $uc_1 = c$. Wstawiając to do równości $ab = cd$ otrzymujemy: $ua_1b = uc_1d$. Podobnie jeśli $x = (b,d)$, to istnieją $(b_1, d_1) = 1$, że $xb_1 = b$, $xd_1 = d$. Teraz równość z założenia ma postać:

$$uxa_1b_1 = uxc_1d_1.$$

Wobec tego, że $(a_1, c_1) = 1$, $(b_1, d_1) = 1$ widzimy, że $a_1/d_1 = c_1/b_1 = t$ (przy założeniu, że $a_1 > d_1$, bsog). Teraz równość przybiera postać:

$$uxd_1tb_1 = uxb_1td_1.$$

Wstawiamy nawiasy zgodnie z tym jakie były wyjściowe a, b, c, d:

$$(ud_1t)(xb_1) = (ub_1)(d_1tx).$$

Zatem widać, że:

$$a = (u)(d_1t), \quad b = (b_1)(x), \quad c = (u)(b_1), \quad d = (d_1t)(x).$$

Całe to zadanie może się wydać bardzo mało atrakcyjne. Jest to jednak w istocie jedynie fakcik pomocniczy do innego – zupełnie już nietrywialnego:

Zadanie 5 *Jeśli a, b, c, d są naturalne i $ab = cd$, wtedy dla każdego n naturalnego liczba $a^n + b^n + c^n + d^n$ jest złożona.*

Na pozór zadanie jest całkowicie nie do ruszenia. Jednak korzystając z poprzedniej uwagi każdy będzie umiał je zrobić, prawda? Zróbmy je zatem wspólnie. Załóżmy, że nic tu nie jest zerem, dla oddalenia trywialnych opcji. Wstawmy to, co mówi poprzednie zadanie.

$$a^n + b^n + c^n + d^n = (uv)^n + (wx)^n + (uw)^n + (vx)^n.$$

Łatwo widać, że wyrażenie po prawej można zwinąć do iloczynu:

$$(u^n + x^n)(v^n + w^n).$$

O ile nie mieliśmy żadnych zer, to każdy z czynników równy jest co najmniej 2. I dowód jest zakończony.

Zadań związanych z ord i z podzielnością można produkować więcej. Inspiracją dla ciekawszych zadań jest twierdzenie o tym ile wynosi $ord_p(n!)$ dla dowolnego n naturalnego. Czy bylibyśmy w stanie wyznaczyć tę wielkość? Oczywiście, możemy sobie całość rozbić na sumę postaci:

$$ord_p(1) + ord_p(2) + \ldots + ord_p(n).$$

Jaki z tego pożytek? Niewielki, można się domyślić. Zacznijmy więc kombinować. Szukamy potęg p mieszkających wśród liczb od 1 do n. No to poszukajmy najpierw wielokrotności. Może być tak, że $n < p$, ale wtedy nasz problem nie jest trudny i $ord_p(n!) = 0$. Jeśli $p < n$, to na pewno i $ord_p(n!) \geqslant 1$. Ile wielokrotności p leży w n? Oczywiście $n = kp + r, 0 \leqslant r < p$, a więc powiemy, że leży k wielokrotności. Jeśli podzielimy to równanie przez p widzimy, że $\frac{n}{p} = k + \frac{r}{p}$. Ostatni ułamek jest mniejszy od 1, a więc k to nic innego tylko $\left[\frac{n}{p}\right]$. Część sukcesu jest już więc za nami. Gdyby więc każda liczba od 1 do n miała w rozkładzie na czynniki tylko jedną kopię p, wtedy $ord(p!) = \left[\frac{n}{p}\right]$. Może się jednak złośliwie zdarzyć, że któraś z liczb dzieli się przez p^2. To znaczy, że $p^2 < n$. Ile będzie takich liczb? To już łatwo stwierdzić: $\left[\frac{n}{p^2}\right]$. No dobrze, to ile mamy ich teraz, przecież te, co się dzielą przez p^2 dzielą się też przez p, a więc je już wyłowiliśmy... No tak, ale interesuje nas ord_p, a więc popatrzmy dokładnie: $\left[\frac{n}{p}\right]$ zlicza po jednej potędze p, załatwia więc wszystkie takie liczby k, że $ord_p(k) = 1$. Z liczb, dla których $ord_p(k) = 2$ zlicza po jednym p, a więc drugie zostaje. Ile jest tych 'drugich'? Dokładnie $\left[\frac{n}{p^2}\right]$. Zatem gdyby wśród liczb $1 \leqslant k \leqslant n$ było tak, że $ord_p(k) \leqslant 2$, wtedy $ord_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right]$. Widać teraz co dalej... Widać też, że procedura, którą zaczęliśmy musi się skończyć. Zatem wzór ogólny ma postać:

$$ord_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots.$$

Piszemy wielokropek, ale ta suma w istocie się kończy. W rozważaniach zwykle nie będzie nas interesowała końcówka tej sumy. To, co tu widzieliśmy to było wyprowadzenie, ale wzorek ten można teraz łatwo dowieść indukcyjnie.

Profity natomiast są mnogie, małe i duże. Zacznijmy od zabawowych przykładów.

Zadanie 6 *Iloma zerami kończy się liczba* 2009!*?*

Skoro mają być zera, to chodzi o potęgi 10. Ta nie jest pierwsza, ale chyba widać, że interesuje nas tak naprawdę $ord_5(2009!)$. Przecież, do każdej piątki dobierzemy dwójkę tak, by w iloczynie dały 10. Odwrotnie już raczej nie. Zgodnie natomiast ze wzorkiem:

$$ord_5(2009!) = \left[\frac{2009}{5}\right] + \left[\frac{2009}{25}\right] + \left[\frac{2009}{125}\right] + \left[\frac{2009}{625}\right] = 401 + 80 + 16 + 3 = 500.$$

Zatem na końcu 2009! będzie 500 zer.

Oczywiście takie zadanka są na poziomie Kangura i sprawdzają raczej naszą pamięć niż umiejętności. Standardowym zastosowaniem udowodnionego faktu są zadania związane z podzielnością w symbolach dwumianowych. Przypomnijmy:

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

Z pewnych kombinatorycznych powodów wiemy, że liczba ta jest całkowita. Gdyby jednak powyższy wzorek był definicją, mielibyśmy już więcej problemów. Mając jednak w garści nasze twierdzenie, radzimy sobie bez problemu. W końcu:

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

Oczywiście rzecz w tym, by dla każdej liczby pierwszej różnica ta była liczbą nieujemną. Użyjmy teraz naszego twierdzenia. Jak? Spróbujmy wykazać, że dla każdego wykładnika s mamy:

$$\left[\frac{n}{p^s}\right] \geqslant \left[\frac{k}{p^s}\right] + \left[\frac{n-k}{p^s}\right].$$

To oczywiście wystarczy, bo nierówności takie zsumujemy stronami dla wszystkich koniecznych s i będzie teza. Udowodnijmy zatem powyższą nierówność. Niech $n = mp^s + r$, zaś $k = m_1p^s + r_1$, $n-k = m_2p^s + r_2$, gdzie $0 \leqslant r, r_1, r_2 < p^s$. Oczywiście $n + (n-k) = n$, zatem $m_1 + m_2 \leqslant m$. A przecież m, m_1, m_2, to właśnie części całkowite o jakie chodziło.

W ten sposób można kontynuować zabawę w nieskończoność. W ramach długich listopadowych nocy można pobawić się w dowodzenie, że całkowite są liczby:

- $\frac{(2m)!(2n)!}{m!n!(m+n)!}$,
- $\frac{(3m)!(3n)!(3q)!}{(m!)^2(n!)^2(q!)^2(m+n+q)!}$,
- $\frac{n!}{k_1!k_2!\ldots k_s!}$, $\quad k_1 + k_2 + \ldots + k_s \leqslant n$.

Spróbujmy teraz zrobić zadanie z eliminacji szkolnych. Przypomnijmy, dla każdej liczby pierwszej p:

$$\binom{2p}{p} = 2 \bmod p.$$

Pomińmy przypadek $p = 2$, wtedy wiadomo co, i jak. Udowodnimy powyższą kongruencję dla nieparzystych p wykorzystując poznaną wcześniej metodę. Na omówieniu zadań wspominałem, że dla każdej różnej od p liczby $0 < k < 2p$ zachodzi:

$$\binom{2p}{k} = 0 \bmod p.$$

Zanim to wykażemy zastanówmy się na ile to pomoże. Oczywiście:

$$(1-1)^{2p} = \binom{2p}{0} - \binom{2p}{1} + \ldots - \binom{2p}{p} - \ldots - \binom{2p}{2p-1} + \binom{2p}{2p} = 0.$$

Jeśli nasz fakt pomocniczy jest prawdziwy, to niemal wszystko w tej naprzemiennej sumie stanie się zerem. Pozostanie tylko:

$$\binom{2p}{0} - \binom{2p}{p} + \binom{2p}{2p} = 1 - \binom{2p}{p} + 1 = 0.$$

Dowód będzie zatem zakończony. Weźmy się więc za $\binom{2p}{k}$. Wiemy, że dla każdego s wykazać chcemy nierówność:

$$\left[\frac{2p}{p^s}\right] \geqslant \left[\frac{k}{p^s}\right] + \left[\frac{2p-k}{p^s}\right].$$

Przy czym, aby teza zadania była spełniona, dla pewnego s nierówność musi być ostra. Rzeczywiście, chcemy, by do $(2p)!$ wchodziła przynajmniej jedna potęga p więcej niż do iloczynu $k!(2p-k)!$. Wtedy symbol dwumianowy będzie podzielny przez p. Oczywiście, dla $s > 1$ nierówności te są równościami, bo wszędzie będą zera. Gdy zaś $s = 1$, wtedy mamy wykazać, że:

$$\left[\frac{2p}{p}\right] = 2 > \left[\frac{k}{p}\right] + \left[\frac{2p-k}{p}\right].$$

Widać teraz po co nam założenie, że $(k, p) = 1$. Dzięki niemu, jeden ze składników po prawej stronie jest zerem, a drugi wynosi oczywiście 1. Koniec dowodu.
Na koniec jeszcze jedno zadanie, gdzie trzeba troszkę pokombinować z naszym twierdzeniem.

Zadanie 7 *Dane są liczby całkowite k, n takie, że $1 \leqslant k \leqslant \frac{n^2}{4}$, przy czym k nie ma dzielnika pierwszego większego od n. Udowodnij, że $n!$ dzieli się przez k.*

Zadanie wygląda na pozór dziwnie. Są jednak pewne jasne strony. Wiadomo, czemu k ma nie mieć dzielnika pierwszego większego od n. W przeciwnym razie $n!$ też nie miałoby tego dzielnika pierwszego i z podzielności nici. Tajemnicze jest to szacowanie przez $\frac{n^2}{4}$. Mimo to odzielnośc dowodzimy standardowo. Bierzemy $ord_p(k)$ i żądamy, by było ono zawsze niewiększe niż $ord_p(n!)$. Oczywiście:

$$ord_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots.$$

Chcemy, by liczba ta była niemniejsza od $ord_p(k)$. Wydaje się, że o tej ostatniej nie wiemy za wiele. Tu jednak pomoże nam szacowanie z założenia. Rozważymy dwa przypadki:

- Niech $ord_p(k) = 2x$. Wówczas $p^{2x} \leqslant k \leqslant \frac{n^2}{4}$. Łatwa manipulacja pozwala stwierdzić, ze $2p^x \leqslant n$. Jest to dla nas kluczowa informacja. Wróćmy do $ord_p(n!)$. Inaczej niż zwykle, interesować nas będzie tym razem jak długa jest ta suma. Dzięku pokazanemu szacowaniu wiemy, że dla $s \leqslant x$: $\left[\frac{n}{p^s}\right] \geqslant 2$. Oznacza to, że gdy spojrzymy na sumę:

  $$ord_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^x}\right] + \text{ 'reszta' }.$$

  to składników tej sumy, które są równe przynajmniej 2 jest przynajmniej x. Zatem $ord_p(n!) \geqslant 2x = ord_p(k)$.

- Niech $ord_p(k) = 2x + 1$. Tu będzie zupełnie podobnie. Mamy: $p^{2x+1} \leqslant k \leqslant \frac{n^2}{4}$. Teraz szacowanie będzie bardziej odpychające, postaci: $2\sqrt{p}p^x \leqslant n$. Widzimy zatem, że dla $s \leqslant x$ wyrażenie $\left[\frac{n}{p^s}\right] \geqslant 2\sqrt{p}$. Zatem:

  $$ord_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^x}\right] + \text{ 'reszta'}$$

  równe jest przynajmniej $2x\sqrt{p}$, a to na pewno nie mniej niż $2x + 1 = ord_p(k)$.

W ten sposób zadanie zostało rozwiązanie. Trudno powiedzieć, jak byśmy je atakowali gdyby nie nasze twierdzenie... Na pierwszy wykład, tyle powinno wystarczyć.