Wieczory z OM

Redukcja 'modulo coś'

Nawet nie ucząc się zbyt wielu metod można rozwiązać wiele zadań olimpijskich z teorii liczb. Potrzeba jednak do tego pewnej cierpliwości i pomysłowości. Dziś zajmiemy się kongruencjami. Bardzo często jest tak, że umiejętna redukcja pozwala błyskawicznie rozwiązać trudne z pozoru zadanie. Zanim przejdziemy do zadań olimpijskich, obejrzymy jeszcze kilka prościutkich zastosowań.

Przykład 1 *Udowodnić, że równanie* $x^3 + y^3 + z^3 = 2005^2$ *nie ma rozwiązań w liczbach całkowitych.*

Standardową metodą postępowania z trzecimi potęgami jest redukcja modulo 9. Trzeba to wiedzieć, inaczej może być niewesoło. A tak, 2005^2 przystaje 4 modulo 9. Trzecie potęgi mogą przystawać modulo 9... jak? Tylko na 3 sposoby: -1, 0, 1. Suma trzech takich reszt nie może dać 4, więc rozwiązań nie ma. □

Przykład 2 *Wykazać, że równanie* $15x^2 - 7y^2 = 1$ *nie ma rozwiązań w liczbach całkowitych.*

Trzeba popatrzeć na to równanie modulo 3. $15x^2$ jest oczywiście podzielne przez 3. A $7y^2$? Modulo 3 to to samo, co y^2. Wystarczy więc wiedzieć, że kwadrat liczby całkowitej jest albo podzielny przez 3, albo daje resztę 1. Zatem lewa strona nie przystaje 1 mod 3. □

Przykład 3 *Udowodnić, że kwadrat liczby całkowitej nieparzystej nie może być sumą pięciu kwadratów innych liczb nieparzystych.*

Standardowy test postępowania z kwadratami to działanie modulo 4. Wiadomo, że kwadrat przystaje 0 lub 1 mod 4. Ale tu mamy liczby nieparzyste. Możemy więc powiedzieć dokładniej: kwadrat liczby nieparzystej daje resztę 1. Ale nieszczęśliwie suma pięciu kwadratów nieparzystych też... Trzeba inaczej. Popatrzmy jednak dokładniej na dowód tego, jakie są reszty z dzielenia przez 4, uwzględniając założenie... Mamy:

$$(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

Łatwo widzieć, że niezależnie od k, pierwszy składnik otrzymanej sumy jest podzielny przez 8. A więc kwadrat liczby nieparzystej daje resztę 1 mod 8. A jak jest z sumą pięciu nieparzystych kwadratów daje resztę 5. □

Przykład 4 *Wykazać, że nie istnieje taka liczba naturalna* $n > 1$*, że* 2^n *jest dzielnikiem* $3^n + 1$*.*

I znowu redukcja. Przyjść nam może do głowy na przykład 4. W końcu potęgi 2 dzielą się przez 4 dość często, a jak jest z $3^n + 1$? Niestety, gdy n jest nieparzyste, stosowny wzór skróconego mnożenia podpowiada, że i $3^n + 1$ dzieli się przez 4. No dobrze... Ale moment! Całkiem sporo potęg dwójki dzieli się

przez 8. A jak jest z 3^n? Tu jak się okazuje, możliwe reszty to 1 lub 3. Zatem w przypadku $3^n + 1$ mamy możliwe reszty 2 lub 4. Podzielności nie ma. □

Chyba każdy już czuje smak tej zabawy. Przejdźmy więc do zadań z OM.

Zadanie 1 (LIX OM, 2. etap) *Wyznaczyć największą możliwą długość ciągu kolejnych liczb całkowitych, z których każdą można przedstawić w postaci $x^3 + 2y^2$ dla pewnych liczb całkowitych x, y.*

Kluczem do rozwiązania tego zadania jest odgadnięcie wyniku. Lub też, wyeksperymentowanie go. Można być pewnym, że przykład najdłuższego ciągu da się jakoś wskazać. Postać ogólna sugeruje, że nie mogą to być za wielkie liczby... No to spróbujmy z małymi. Oczywiście $0^3 + 2 \cdot 0^2 = 0$ jest w porządku. 1 też, a skoro ona, to i -1. Działa też $2 = 0^2 + 2 \cdot 1^2$. Widać, że -2 tak nie dostaniemy. Czy w ogóle możemy dostać -2? Gdybyśmy mieli $-2 = x^3 + 2y^2$, to $x^3 = 2(y^2 + 1)$. Stąd x dzieli się przez 2. Jeśli jednak $x = 2x'$, to $4x'^3 = y^2 + 1$, a więc kwadrat liczby całkowitej daje resztę 3 z dzielenia przez 4. Tak być nie może. A więc -2 nie działa. Skoro tak, to niżej nie musimy schodzić. A czy działa 3? Też działa. $3 = 1^3 + 2 \cdot 1^2$. A 4? Od razu nam nic nie przychodzi, a jeśli rozpiszemy: $4 = x^3 + 2y^2$, to znowu $x = 2x'$, a więc: $2 = 4x'^3 + y^2$, a więc znowu źle, bo kwadrat daje resztę 2 z dzielenia przez 4.

Naoczni świadkowie mówią więc, że ciąg 5 elementowy znajdziemy. Zauważmy, że na granicach nie zagrała nam 2 razy podzielność kwadratu przez 4. Za każdym razem zanim z niej skorzystaliśmy, skracaliśmy równanie przez 2. Tak więc dla ogólnego równania coś może być na rzeczy z podzielnością przez 8. W przykładzie nie pasowały nam reszty 2 i 3 z dzielenia przez 4, w dzieleniu przez 8 będą to reszty 4, 6.

No to spróbujmy pomyśleć ogólnie. Bierzemy 6 kolejnych liczb całkowitych, które są postaci $x^3 + 2y^2$. Patrzymy na reszty z dzielenia tych liczb przez 8. Feralne były 4 oraz 6, czy teraz znajdziemy takie reszty wśród wybranych sześciu liczb? Oczywiście tak, przynajmniej jedną z tych reszt znajdziemy. A dalej? A dalej dokładnie tak, jak eksperyment kazał. Jeśli wyłowiona liczba to m i $m = x^3 + 2y^2$, to dając resztę 4 lub 6 z dzielenia przez 8 liczba m jest parzysta. Skoro tak, to x też, więc $x = 2x'$. Dzielimy stronami i dostajemy: $m' = 4x' + y^2$, a więc $y^2 = m' \bmod 4$. No i koniec, ponieważ m' daje resztę 2 lub 3 z dzielenia przez 4. □

Wpadnięcie na rozważanie reszty 8 było punktem przełomowym w tym zadaniu. Często na OM trzeba wymyślać bardziej lub mniej egzotyczne liczby, względem których badamy podzielność. Czasem jednak można je dość łatwo wywnioskować z treści samego zadania.

Zadanie 2 (LV OM, 1. etap) *Roztstrzygnąć, czy istnieje liczba pierwsza p oraz liczby całkowite nieujemne x, y, z spełniające równanie:*

$$(12x + 5)(12y + 7) = p^z.$$

Patrząc na samo równanie widać jasno, że jeśli takie liczby istnieją, to z rozkłada się jakoś pomiędzy $12x + 5$ oraz $12y + 7$. Dokładniej, istnieją naturalne i większe od zera a, b, że $a + b = z$ oraz:

$$12x + 5 = p^a$$
$$12y + 7 = p^b$$

Co teraz? Przez co będziemy dzielić? Pewnie przez 12. Potęgi liczb pierwszych mają niewiele reszt z dzielenia przez 12. Istotnie, z postaci równań powyżej, widać, że p jest większa od 3. Stąd musi być jednej z dwóch postaci: $p = 6x \pm 1$. Nas interesują potęgi. No to do dzieła: $p^2 = (6x \pm 1)^2 = 36x^2 \pm 12x + 1 = 1 \bmod 12$. Świetnie! Kwadrat daje zawsze resztę 1. A sześcian? Pewnie resztę p. A czwarta potęga? Znowu 1! Ogólnie, dla $p > 3$ mamy:

$$p^n = \begin{cases} 1 \bmod 12, & \text{dla n parzystych,} \\ p \bmod 12, & \text{dla n nieparzystych.} \end{cases}.$$

No dobrze, ale co nam mówi zadanie? Mówi, że $p^a = 5 \bmod 12$, zaś $p^b = 7 \bmod 12$. Tak, jak widać, być nie może. □

A teraz stare zadanie...

Zadanie 3 (XVI OM) *Wyznacz wszystkie takie liczby pierwsze p, że* $4p^2+1$ *i* $6p^2+1$ *są również liczbami pierwszymi.*

Tym razem trzeba patrzeć modulo 5. Problem z OM jest taki, że czasem po prostu trzeba wiedzieć na jaką resztę patrzeć. 5 leży pomiędzy 4 i 6, a więc można liczyć na jakieś redukcje. Niech więc $A = 4p^2 + 1$, natomiast $B = 6p^2 + 1$. Wtedy:

gdy $p = 0 \bmod 5$ to $A = 1 \bmod 5$, $B = 1 \bmod 5$,
gdy $p = 1 \bmod 5$ to $A = 0 \bmod 5$, $B = 2 \bmod 5$,
gdy $p = 2 \bmod 5$ to $A = 2 \bmod 5$, $B = 0 \bmod 5$,
gdy $p = 3 \bmod 5$ to $A = 2 \bmod 5$, $B = 0 \bmod 5$,
gdy $p = 4 \bmod 5$ to $A = 0 \bmod 5$, $B = 2 \bmod 5$,

Oczywiście mamy tu pewne ułatwienie. Gdy $p = 2$, to widać, że 25 nie jest pierwsze. Zatem p jest nieparzyste. Odpada opcja z podzielnością przez 5, o ile oczywiście nie jest 5, a także z nieparzystą resztą. Tabelka mówi, że gdy $p = 2$ lub $p = 4$ modulo 5, to któraś z A lub B jest podzielna przez 5. Zatem zostaje już tylko sprawdzić $p = 5$. I rzeczywiście, wychodzi: 101, 151 – liczby pierwsze. To taki przykład zadania, że jak wymyślisz resztę, to robi się samo. Jak nie wymyślisz, to jest nie do zrobienia :) □

Rozwiążmy jeszcze jedno zadanie tego typu, znowu z pierwszego etapu:

Zadanie 4 (LV OM, 1. etap) *Znaleźć wszystkie takie rozwiązania równania* $a^2 + b^2 = c^2$ *w liczbach całkowitych dodatnich, że liczby a i c są pierwsze, a liczba b jest iloczynem co najwyżej czterech liczb pierwszych.*

Podobnie jak wcześniej trzeba troszkę pokombinować. Informacja, że a jest liczbą pierwszą bardzo nam się podoba, bo przecież $a^2 = (b - c)(b + c)$. Wobec tego $b - c$ musi być równe 1, czyli $b = c + 1$. Wiele rzeczy natychmiast się upraszcza: $a^2 = 2b+1$. Jest to więc liczba nieparzysta. Wykorzystaliśmy założenie o pierwszości a, teraz i c powinno się przydać. Niech $a = 2n + 1$. Wtedy

$$b = 2n(n + 1), \quad c = 2n^2 + 2n + 1.$$

Trzeba zatem zastanowić się, kiedy $c = 2n^2 + 2n + 1$ oraz $a = 2n + 1$ jest liczbą pierwszą? Parzystość i nieparzystość n to za mało, by wyrokować. Spróbujmy z resztami z dzielenia n przez 3 i przez 5. Jeśli n

daje przy dzieleniu przez 3 resztę 1, to a jest podzielne przez 3. Zatem $n = 1$, a jedyna trójka spełniająca równanie to $(3, 4, 5)$. Jak zaczniemy dzielić przez 5, to okaże się, że a robi się podzielne przez 5, gdy n daje resztę 2 z dzielenia przez 5a c staje się podzielne przez 5, gdy n daje resztę 1 lub 3. Wtedy dostajemy $n = 2$ i rozwiązanie (5,12,13).

Troszkę namieszaliśmy, ale z tego wszystkiego zostają nam przypadki, gdy n daje resztę 0 lub 2 z dzielenia przez 3 i resztę 0 lub 4 z dzielenia przez 5. Wtedy wkracza założenie ostatnie (z tym iloczynem max czterech liczb pierwszych). O a i c już nic nie wiemy, ale nagle $b = 2n(n + 1)$ staje się podzielne przez $2 \cdot 6 \cdot 5$, a więc przez 60. Ale 60 to iloczyn czterech liczb pierwszych, więc b=60. Tak oto powstaje trzecie i ostatnie rozwiązanie: $(11, 60, 61)$. $\square$

Jak widać, rozwiązanie to polegało na cierpliwym grzebaniu się w przypadkach. To, co było miłe, to fakt, że pierwsze z brzegu liczby pierwsze załatwiały problem, wystarczyło tylko cierpliwie wszystko obejrzeć. Oczywiście, im dalej zajdziemy, tym bardziej ukryta będzie prawda. Spójrzmy tym razem na zadanie finałowe:

Zadanie 5 (LVII OM, 3. etap) *Wyznaczyć wszystkie liczby całkowite k, dla których liczba* $3^k + 5^k$ *jest potęgą liczby całkowitej o wykładniku naturalnym większym od 1.*

Od czego by tu zacząć? Poza faktem, że $3 + 5 = 8$ jest trzecią potęgą, nic nam może nie przychodzić do głowy. Spróbujmy zatem może wymyślić chociaż coś a propos kwadratów liczb całkowitych. To w istocie załatwia 'połowę' zadania, bo przecież każda potęga liczby całkowitej albo jest kwadratem, albo nieparzystą potęgą. Czy $3^k + 5^k$ może być kwadratem? Ulubiony test na bycie kwadratem to sprawdzanie podzielności przez 4. No to patrzmy: 3^k daje resztę $(-1)^k$, zaś 5^k zawsze daje 1. A suma? Zależy od k. Jeśli k jest nieparzyste, to całość dzieli się przez 4, a kwadratom zdarza się to nader często. A jeśli k jest parzyste? Wtedy jest dobrze, $3^k + 5^k = 2 \bmod 4$, a takich kwadratów nie ma... Jakby się chwilkę zastanowić, to widać, że w ogóle nie ma potęg naturalnych większych od 1, które dają resztę 2 z dzielenia przez 4. Przecież liczby takie są parzyste, są potęgami i... nie dzielą się przez 4? Tak być nie może. Tak więc wiemy jedno: jak k jest parzyste, potęg nie ma. Zatem 4 się na coś przydało.

Gdy k jest nieparzyste, mamy dodatkowe narzędzie w postaci wzoru skróconego mnożenia:

$$3^k + 5^k = (3 + 5)(3^{k-1} - 3^{k-2} \cdot 5^1 + 3^{k-3} \cdot 5^2 - \ldots - 3^1 \cdot 5^{k-2} + 5^{k-1}).$$

Wniosek narzuca się sam: $3^k + 5^k$ dzieli się przez 8. Sztuka polega na tym, by zauważyć teraz, że nie dzieli się przez 16. Co mamy w drugim nawiasie? Nieparzyście wiele nieparzystych składników, prawda? No to dwójki tu nie wciśniemy. Jak coś jest potęgą liczby całkowitej o wykładniku naturalnym większym od 1, dzieli się przez 2^3, a przez 2^4 już nie, to jaką może być potęgą? Tylko trzecią. Mamy więc kolejny postęp – gdy k nieparzyste, suma $3^k + 5^k$ jest sześcianem. Wiemy już, że gdy $k = 1$ to tak jest. Niech więc $k \geqslant 3$

Jaki jest nasz ulubiony test na bycie sześcianem? Przypomnijmy, podzielność przez 9. Jak jest z $3^k + 5^k$? Gdy $k \geqslant 3$, to 3^k dzieli się przez 9, a 5^k? Tu trzeba porachować: modulo 5 mamy:

$$5^0 = 1, 5^1 = 5, 5^2 = 7, 5^3 = 8, 5^4 = 4, 5^5 = 2, 5^6 = 1.$$

Dalej cyklicznie. Do obrazka pasuje nam więc tylko sytuacja, gdy k dzieli się przez 3. Wiemy, że jest to liczba nieparzysta, zatem $k = 6n + 3$, gdzie n jest liczbą całkowitą nieujemną. Krąg podejrzanych się

zacieśnia, ale wciąż jest nieskończony. To źle...

Dotąd mógł dojść każdy, co robić dalej?. Mamy liczbę postaci $3^{6n+3} + 5^{6n+3}$. Jakie tu jeszcze reszty badać? Gdy w wykładniku mamy wyrażenie liniowe typu $(p-1)n + r$, warto badać reszty z dzielenia przez p. To tylko heurystyka, ale przecież chodzi o znane narzędzie: małe twierdzenie Fermata. Będziemy patrzeć na reszty z dzielenia przez 7.

$$3^3 = 5^3 = -1 \bmod 7, \quad 3^6 = 5^6 = 1 \bmod 7.$$

Zatem cała suma:

$$3^{6n+3} + 5^{6n+3} = 3^3 + 5^3 = 5 \bmod 7.$$

Okazuje się tymczasem, że sześcian nie może dać reszty 5 z dzielenia przez 7. Zatem gdy $k \geqslant 3$, $3^k + 5^k$ potęgą liczby całkowitej o wykładniku naturalnym większym od 1 być nie może. □

Zasada szufladkowa Dirichleta

Wczoraj przyglądaliśmy się przykładom zadań olimpijskich, w których istotną rolę grało redukowanie wyrażeń modulo pewna liczba. Jest to standardowa rodzina zadań. Drugi powracający często motyw, to zasada szufladkowa, obecna w zbiorach reszt z dzielenia. Są to niewątpliwie zadania trudniejsze. Dlatego zanim przejdziemy do przykładów olimpijskich, kilka prostych przykładów:

Przykład 5 *Udowodnij, że wśród dowolnych $n+1$ liczb całkowitych znajdą się dwie, których różnica dzieli się przez n.*

Jasne, mamy n+1 reszt, pewne dwie są równe, więc różnica tych liczb jest podzielna przez n. □

Przykład 6 *Mamy 2009 liczb całkowitych. Wykazać, że zawsze można wśród nich znaleźć takie trzy różne liczby a, b, c, że liczba $a(b-c)$ jest podzielna przez 2009.*

Oczywista sprawa: albo jedna z liczb jest podzielna przez 2009, albo pewne dwie dają taką samą resztę przy dzieleniu przez 2009. □

Przykład 7 *Dany jest ciąg liczb całkowitych $a_1, a_2, \ldots, a_n$. Wykazać, że można w tym ciągu wybrać kilka kolejnych liczb (być może jedną), których suma jest podzielna przez n.*

Określamy $b_1 = a_1, b_2 = a_1 + a_2, b_3 = a_1 + a_2 + a_3, \ldots$. Reszt z dzielenia przez n jest dokładnie n, a skoro tak, to albo wszystkie b_i mają różne reszty, a więc wsród nich jest ta poszukiwana, podzielna przez n, albo też istnieją $i < j$, że $n \mid b_j - b_i$. To oznacza, że suma $a_{i+1} + a_{i+2} + \ldots + a_j$ jest podzielna przez n. □

Przykład 8 *Spośród liczb $1, 2, \ldots, 2n$ wybrano $n+1$ liczb. Wykazać, że można wśród nich znaleźć takie dwie, że jedna jest dzielnikiem drugiej.*

Przyporządkujmy każdej z $2n$ liczb jej największy nieparzysty dzielnik. Z jakiego zbioru są te nieparzyste dzielniki? Oczywiście ze zbioru $\{1, 3, 5, \ldots 2n-1\}$. Ma on n elementów. Skoro my zatem wybraliśmy

$n+1$, to dla pewnych dwóch największy nieparzysty dzielnik jest taki sam. Widać zatem, że jedna z nich pomnożona przez potęgę dwójki daje drugą. □

Przykład 9 *Mamy $n = 2k$ liczb całkowitych. Suma tych liczb jest podzielna przez n. Wykazać, że w zbiorze tym można znaleźć pewne dwa elementy, których różnica jest podzielna przez n.*

Gdyby tak nie było, wszystkie elementy zbioru musiałyby dawać różne reszty z dzielenia przez n. Byłyby to więc kolejno $0, 1, \ldots, n-1$. Tymczasem suma tych reszt wynosi $n(n-1)/2$. Jako, że n jest parzyste, liczba ta nie jest wielokrotnością n, wbrew założeniu. □

Przejdźmy do zadań olimpijskich.Najpierw mix wczorajszej i dzisiejszej myśli szkoleniowej.

Zadanie 6 (LII OM, 1. etap) *Dowieść, że wśród 12 kolejnych liczb całkowitych dodatnich istnieje liczba nie będąca sumą 10 czwartych potęg liczb całkowitych.*

Zgodnie z wczorajszym biegiem wydarzeń wartoby mieć pod ręką ulubiony test do wykrywania czwartych potęg. Dla przypomnienia, przy kwadratach było to dzielenie przez 4, przy sześcianach – przez 9. A przy czwartych potęgach? Można spróbować z 16. Sprawdzimy łatwo, że każda czwarta potęga przystaje 0 lub 1 modulo 16. Wniosek jest prosty. Suma 10 czwartych potęg może przystawać modulo 16 na... 11 sposobów. Wspaniale, przecież w treści jest 12 liczb! Czuć w powietrzu zasadę szufladkową... Rzeczywiście, wśród 12 kolejnych liczb całkowitych nie ma naturalnie dwóch takich, które dawałyby tę samą resztę z dzielenia przez 16. Zatem któraś z tych 16 liczb nie daje jednej z reszt: $\{0, 1, \ldots, 10\}$ z dzielenia przez 16. Wniosek: liczba ta nie jest sumą 10 czwartych potęg. □

Pierwsze zadanie było oczywiście szczytem bezczelności i każdy szanujący się olimpijczyk musi umieć wyczuć tu, że chodzi o zasadę szufladkową. A teraz coś z okolicy zadań rozgrzewkowych, tym razem na poziomie OM.

Zadanie 7 (XLIII OM) *Udowodnij, że wśród dowolnych $n+2$ liczb całkowitych istnieją takie dwie, których suma lub różnica dzieli się przez $2n$.*

Początek argumentu jest standardowy. Patrzymy na reszty z dzielenia przez 2n elementów naszego zbioru. Gdyby jakieś dwie były równe... To naturalnie różnica byłaby podzielna przez 2n. A jeśli reszty są parami różne? Teraz ujawnia się czemu wybraliśmy $n+2$ liczby. Otóż, przynajmniej n z reszt jest różne od 0 oraz n. Jednym słowem, pewne n z wybranych $n+2$ liczb jest względnie pierwszych z $2n$. Sztuczka polega na umiejętnym spojrzeniu na zbiór, z którego pobieramy te n reszt.

$$\{0, 1, 2 \ldots, 2n-1\} \setminus \{0, n\} =$$
$$\{1, 2, \ldots, n-1\} \cup \{n+1, n+2, \ldots, 2n-1\} =$$
$$\{1, 2n-1\} \cup \{2, 2n-2\} \cup \{3, 2n-3\} \cup \ldots \cup \{n-1, n+1\}.$$

Zbiór możliwych reszt podzieliliśmy na n-1 rozłącznych pozbiorów. Skoro należy do niego n różnych elementów, to pewne dwie reszty są postaci $j, 2n-j$, dla ustalonego j takiego, że $0 < j < n$. Świetnie, bo suma tych reszt, to 2n, zatem suma liczb, które reszty te reprezentują jest podzielna przez 2n. □

Następne zadanie powinno się niektórym wydać znajome...

Zadanie 8 (LX OM, 1. etap) *Dana jest liczba całkowita $n \geqslant 2$. Niech $r_1, r_2, \ldots, r_{n-1}$ będą resztami z dzielenia liczb:*

$$1, \quad 1+2, \quad 1+2+3, \quad \ldots, \quad 1+2+\ldots+(n-1).$$

Znaleźć wszystkie wartości n takie, że $(r_1, r_2, \ldots, r_{n-1})$ jest permutacją ciągu $(1, 2, \ldots, n-1)$.

Zadanie to, jak wiele, polega na wymyśleniu jak powinno być i dowiedzeniu tego. Nie jest trudno sprawdzić kilka pierwszych liczb całkowitych i widać, że pasują tylko 1, 2, 4, 8. Nasuwa to jednoznaczny wniosek. Ale po kolei... Czy do tego, że chodzi o potęgi dwójki mozna jakoś dojść?

Patrząc na sumę $1+2+\ldots+(n-1)$ widać, że jest to po prostu $\frac{n(n-1)}{2}$. Jaka jest reszta z dzielenia tego przez n? Widać, że dla n nieparzystego, jest to 0, a więc wynik niedopuszczalny. Do potęg dwójki jeszcze daleko, ale nie za daleko. W końcu każda liczba naturalna nieparzysta większa od 1 jest postaci $2^k a$, gdzie a nieparzyste większe od 1 Gdyby więc tak pokazać, że n nie może mieć nieparzystego dzielnika pierwszego... Ale jak właściwie dojść do tego, że trzeba sprawdzić właśnie coś takiego?

Anomalią było to, że pojawiło się zero, i to tam, gdzie go nie powinno było być. Gdy n jest parzysta, to trzeba zajrzeć głębiej w liczbę. Może i tam będzie coś nie tak? Jak to wysłowić? Możemy pomyśleć tak: wezmę dzielnik pierwszy p liczby n. No i będę po kolei patrzył na reszty z dzielenia $1, 1+2, \ldots$ przez p. A właściwie nawet nie na nie. Wezmę ciąg $(r_1, r_2, \ldots, r_{n-1})$ i popatrzę, czy jakieś jego elementy dzielą się przez p. Po co? Wiadomo, że jeśli ciąg ten równy jest po permutacji $(1, 2, \ldots, n-1)$, to elementów r_i podzielnych przez p musi być dokładnie $\frac{n}{p} - 1$. A jak jest w rzeczywistości?

$$1+2+\ldots+(tp-1) = \frac{(tp)(tp-1)}{2}$$

$$1+2+\ldots+(tp-1)+tp = \frac{(tp+1)(tp)}{2}$$

Nie zawsze wiemy jaka jest reszta z dzielenia sumy kolejnych liczb przez p, ale gdy dochodzimy w sumie do wielokrotności p, wtedy nie ma wątpliwości. Skoro p jest nieparzyste, to suma dzieli się przez p. Zatem także r_{tp-1}, r_{tp} dzieli się przez p. A ile takich jest? Liczba t przebiega od 1 do $\frac{n}{p}$, pomijając r_n, a więc jest ich $2\frac{n}{p} - 1$. To więcej niż $\frac{n}{p} - 1$. A więc mamy sprzeczność, liczba n nie może mieć nieparzystego dzielnika pierwszego.

Pozostaje tylko sprawdzić,czy gdy $n = 2^k$, to rzeczywiście reszty spełniają wymagania. Możliwe są dwie sytuacje. Jeden z r_i okaże się zerem. Co to znaczy?

$$1+2+\ldots+m = \frac{m(m+1)}{2}$$

Powyższa liczba musi być podzielna przez 2^n. No tak, ale w liczniku jest liczba parzysta i nieparzysta, zatem dokładnie jedna z nich dzieli się przez 2^{n+1} (dochodzi jeszcze 2 z mianownika). Tymczasem $m < 2^n$, to o podzielności można zapomnieć.

Druga możliwa opcja jest taka: dwie reszty są równe. Postępujemy identycznie. Kto spróbuje? Trzeba odjąć dwie sumki, zwinąć i zobaczyć, że na górze jest liczba parzysta i nieparzysta... □

Gdzie tkwił klucz do rozwiązania? W zauważeniu, że wśród reszt pojawia się nadprogramowo wiele zer. Z punktu widzenia zasady szufladkowej, to nic się tu nie stało, ale samo zadanie wymagało przemyślenia... Teraz znacznie trudniejsze zadanie...

Zadanie 9 (LIV OM, etap 2.) *Wykazać, że dla każdej liczby pierwszej $p > 3$ istnieją liczby całkowite x, y, k spełniające warunki: $0 < 2k < p$ oraz*

$$kp + 3 = x^2 + y^2.$$

Zadanie sformułowane jak widać wydaje się niemal beznadziejne. O co tu właściwie chodzi? Dla każdej większej od 3 liczby pierwszej szukamy stosunkowo niewielkiej wielokrotności, która będzie o 3 mniejsza niż jakaś suma kwadratów. Co można z tego wyciągnąć? Możemy pytać kiedy $x^2 + y^2 - 3$ jest niewielką wielokrotnością p. Jak niewielką? W sumie mniejszą $\frac{p^2}{2}$. W takim razie sensownie jest założyć, że x, y możemy pobierać ze zbioru $0 \leqslant x, y < p/2$. Czy wtedy trafimy? Tu wchodzi element ilościowy.

Zamiast myśleć o sumie, pomyślimy o różnicy: $x^2 - (3 - y^2)$. Niech:

$$A = \{x^2 : 0 \leqslant x < p/2\}$$
$$B = \{3 - y^2 : 0 \leqslant y < p/2\}.$$

Wiadomo, że każdy element różnicy $x^2 - (3 - y^2)$ jest postaci $a - b$, gdzie $a \in A, b \in B$. Gdyby udało się pokazać, że istnieje para $(a, b) \in A \times B$, że $a = b \bmod p$, to bylibyśmy już blisko sukcesu.

Wykażemy, że każde dwa elementy zbioru A dają różne reszty z dzielenia przez p. Istotnie, gdyby p dzieliło $x_1^2 - x_2^2$, to dzieliłoby też $(x_1 - x_2)(x_1 + x_2)$. Ale $0 \leqslant x_1, x_2 < p/2$. Stąd sprzeczność. Podobnie wykazujemy, że każde dwa elementy zbioru Y dają różne reszty z dzielenia przez p.

Co to wszystko znaczy? Spójrzmy na zbiory A, B ich łączna ilość elementów to $p+1$. Zatem istnieją dwie liczby: x_1 z A oraz $3 - y_1$ z B, które dają te same reszty z dzielenia przez p (zasada szufladkowa). Skoro tak, to $x_1^2 + y_1^2 - 3 = kp$, dla pewnego k. Ile to k wynosi?

$$k = \frac{x_1^2 + y_1^2 - 3}{p} < \frac{(p/2)^2 + (p/2)^2}{2} = \frac{p^2}{2}.$$

Warunki podane w treści są zatem spełnione. □

Nie tak łatwo wpaść na ten trik. Dość powiedzieć, że w tamtej edycji OM tylko kilku osobom w kraju udało się to zadanie rozwiązać. Gdyby komuś było mało zadań z teorii liczb, polecam stronę członka KGOM, http://www.math.uni.wroc.pl/ s175509/matematyka.html, tam znajdzie ich więcej :)