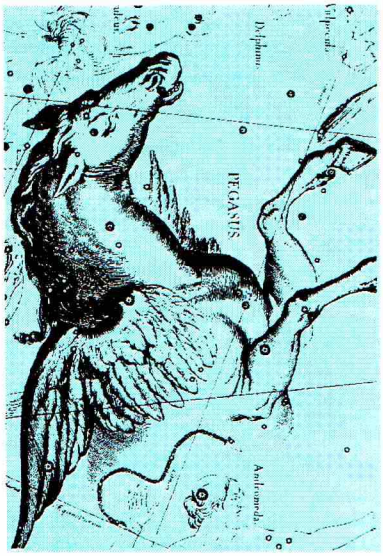


Jak rozpoznajemy liczby pierwsze?

Wojciech GUZICKI

Jak stwierdzić, czy dana liczba naturalna n jest liczbą pierwszą? Najprostszy algorytm polega na dzieleniu liczby n przez wszystkie liczby mniejsze od niej. Łatwo zauważymy, że wystarczy dzielić przez liczby nie większe niż $\sqrt{n}$, potem zauważymy, że nie trzeba dzielić przez liczby parzyste itp. Oczywiście, najkorzystniej byłoby dzielić tylko przez liczby pierwsze mniejsze od $\sqrt{n}$, ale jak z kolei je rozpoznać? Jednak chwila zastanowienia pokaże, że nawet najlepsze modyfikacje tego algorytmu będą całkowicie nieprzydatne w praktyce, gdy mamy do czynienia z bardzo dużą liczbą pierwszą n. Jeśli bowiem liczba n ma np. 200 cyfr dziesiętnych, to liczb pierwszych mniejszych od niej jest tak wiele, że w ciągu całego naszego życia nie zdążymy sprawdzić, czy n dzieli się przez nie wszystkie, nawet jeśli użyjemy do tego najlepszych znanych nam komputerów.

Czy jednak można stwierdzić, że liczba n jest pierwsza, inaczej niż wykazując, że nie dzieli się przez żadną liczbę mniejszą od niej? Zanim odpowiemy na to pytanie, zastanowimy się nad pytaniem „odwrotnym" do niego: jak stwierdzić, że liczba *nie jest* pierwsza? Oczywiście, najprościej wskazać dzielnik takiej liczby. Na przykład, wykazujemy, że liczba $n = 2454326562337695420831 07$ jest złożona, wskazując jej rozkład na czynniki:

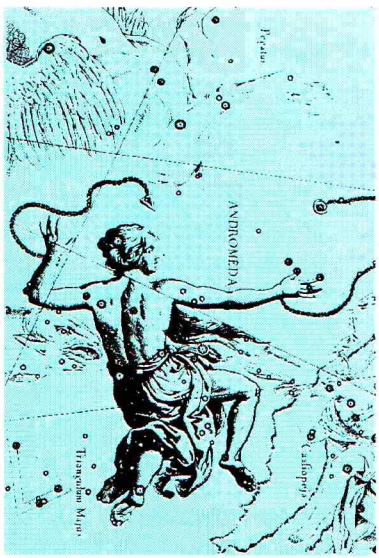
$$n = 245432656233769542083107 = 563389748759 \cdot 435635644373\,.$$

Sprawdzenie, że tak jest naprawdę, jest kwestią chwili dla niedużego komputera. Widzimy więc, jak można łatwo przekonać kogoś, że pewna liczba jest *złożona*. Wystarczy pokazać mu rozkład tej liczby na czynniki. Zupełnie inną kwestią jest sposób znalezienia tego rozkładu i tym problemem nie będziemy się tu zajmować. Przypomnę tylko, że dotychczas nie znamy dostatecznie szybkiego algorytmu, za pomocą którego moglibyśmy rozkładać na czynniki liczby mające już około 150 cyfr dziesiętnych.

Czy wskazanie rozkładu na czynniki jest jedyną metodą wykazania, że liczba jest złożona? Okazuje się, że nie. Możemy bowiem skorzystać z tzw. małego twierdzenia Fermata:

Twierdzenie. Jeśli liczba p jest pierwsza i liczba a nie dzieli się przez p, to $a^{p-1} \equiv 1 \pmod{p}$.

Twierdzenie to wynika natychmiast z twierdzenia Eulera, wspomnianego w poprzednim artykule. Weźmy teraz przykład. Liczba $n = 481$ jest złożona. Możemy się o tym przekonać, znajdując jej czynniki pierwsze: $481 = 13 \cdot 37$. Możemy jednak skorzystać z małego twierdzenia Fermata. Weźmy liczbę $a = 2$. Oczywiście, a nie dzieli się przez n. Gdyby liczba n była liczbą pierwszą, to musiałaby być spełniona kongruencja $2^{480} \equiv 1 \pmod{481}$. Wiemy, w jaki sposób można dość szybko obliczać wysokie potęgi modulo n. Jeśli obliczymy (za pomocą komputera) potęgę 2^{480} modulo 481, to przekonamy się, że $2^{480} \equiv 248 \pmod{481}$. A zatem liczba 481 *nie jest pierwsza*.



W tym przykładzie liczba n jest mała i trudności obliczeniowe związane z obliczeniem wysokiej potęgi liczby 2 modulo 481 nie przekonają nikogo o opłacalności tej metody. Dużo prościej byłoby spróbować podzielić n przez kilka początkowych liczb naturalnych. Jednak jeśli liczba n ma kilkaset cyfr i dzielenie nie może dać rezultatu wystarczająco szybko, podnoszenie do potęgi zaczyna się opłacać. Powstaje tylko pytanie, czy ta metoda zawsze jest skuteczna, tzn. czy zawsze możemy wykazać w ten sposób, że liczba n jest złożona.

Wybierzmy inną podstawę a, np. $a = 11$. Wtedy okaże się, że $a^{480} \equiv 1 \pmod{481}$. Liczba 481 jest złożona, a mimo to teza małego twierdzenia Fermata zachodzi. Pokazuje to, że ta metoda jest jednak zawodna. Mogą istnieć podstawy a, dla których $a^{n-1} \equiv 1 \pmod{n}$ i podstawy a, dla których $a^{n-1} \not\equiv 1 \pmod{n}$.

Rozwiązanie zadania F 449. Oznaczmy przez $\vec{p}$ i $\vec{p}_\gamma$ pędy cząstki i fotonu przed rozpraszaniem, a przez $\vec{p}'$ i $\vec{p}'_\gamma$ po rozproszeniu. Analogicznie E, E_γ, E' i E'_γ to energie cząstki i fotonu odpowiednio przed i po rozproszeniu. Dla prostoty rachunków wybierzmy układ jednostek, w którym $c = \hbar = 1$. Niech θ oznacza kąt rozpraszania fotonu. Zasada zachowania pędu ma postać:

$$\vec{p} + \vec{p}_\gamma = \vec{p}' + \vec{p}'_\gamma ,$$

a zasada zachowania energii:

$$E + E_\gamma = E' + E'_\gamma .$$

Związki między energią i pędem mają postać $E_\gamma = p_\gamma$ dla fotonu, oraz $E^2 = p^2 + m^2$ dla cząstki obdarzonej masą (analogicznie po rozproszeniu). Podnosząc do kwadratu obie strony równania wyrażającego zasadę zachowania pędu otrzymujemy

$$p'^2 = p^2 + E_\gamma^2 + E_\gamma'^2 - 2pE_\gamma + \\ + 2E'_\gamma(p - E_\gamma)\cos\theta .$$

Korzystając z zasady zachowania energii eliminujemy p' i E'. Otrzymujemy w ten sposób

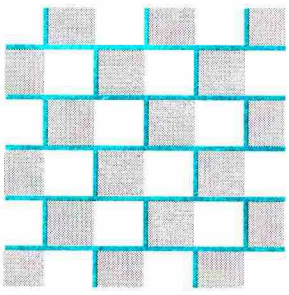
$$E'_\gamma = \frac{E_\gamma(E + p)}{E + E_\gamma + (p - E_\gamma)\cos\theta} .$$

Ponieważ $p > E_\gamma$, energia rozproszonego fotonu jest maksymalna dla $\theta = \pi$. Posługując się przybliżeniem $p = \sqrt{E^2 - m^2} \simeq E - \frac{m^2}{2E}$ (poprawnym dla dużych energii cząstki) i pamiętając, że początkowa energia fotonu jest dużo mniejsza od masy cząstki, a ta jest z kolei dużo mniejsza od początkowej energii cząstki, możemy to wyrażenie przybliżyć przez

$$E'_\gamma = \frac{E}{1 + \dfrac{m^2}{4E\omega}} .$$

Podstawiając dane liczbowe otrzymujemy wartość rzędu 10^{19} eV.

Rozwiązanie zadania M 805. Nie. Podzielmy szachownicę na „kostki domina" o rozmiarach 2×1 (tak, jak pokazuje to rysunek).



Wystarczy, aby drugi gracz po każdym ruchu gracza rozpoczynającego wstawiał swój znak do tego samego „domina", co przeciwnik – uniemożliwi to zwycięstwo rozpoczynającemu rozgrywkę, bo w każdym kwadracie 2×2 znajduje się jakieś domino.

Jeśli liczba n jest złożona, liczba a jest względnie pierwsza z n oraz zachodzi kongruencja $a^{n-1} \equiv 1 \pmod{n}$, to liczbę n nazywamy liczbą pseudopierwszą przy podstawie a. Liczby pseudopierwsze przy podstawie 2 dawniej nazywano po prostu liczbami pseudopierwszymi. Najmniejszą taką liczbą jest 341. Można udowodnić, że jest tych liczb nieskończenie wiele. Naturalnym pytaniem jest, czy dla każdej liczby złożonej n istnieje taka względnie pierwsza z nią podstawa a, że liczba n nie jest pseudopierwsza przy podstawie a. Gdyby tak było, to mielibyśmy nadzieję na sprawdzenie, czy liczba n jest pierwsza. Test mógłby wyglądać następująco: wybieramy liczbę a mniejszą od n i sprawdzamy, czy jest ona względnie pierwsza z n; jeśli znajdziemy wspólny dzielnik, to wiemy na pewno, że liczba n jest złożona, w przeciwnym przypadku podnosimy a do potęgi $n - 1$ modulo n – jeśli otrzymamy wynik różny od 1, to wiemy, że liczba n jest złożona, jeśli otrzymamy 1, to szukamy następnej podstawy a. Skuteczność tego testu będzie zależała przede wszystkim od tego, czy dla liczby n istnieje podstawa a, przy której liczba n nie jest pseudopierwsza, a następnie od tego, czy taką podstawę będziemy umieli znaleźć.

Okazuje się jednak, że istnieją liczby złożone n będące liczbami pseudopierwszymi przy każdej podstawie a względnie pierwszej z n. Przykładem takiej liczby jest 561. Można dość łatwo wykazać (np. za pomocą odpowiedniego programu komputerowego), że jeśli liczby a i 561 są względnie pierwsze, to $a^{560} \equiv 1 \pmod{561}$. Takie liczby nazywamy liczbami Carmichaela (czytamy „Karmajkla"). Istnienie liczb Carmichaela niweczy nasze nadzieje na prosty test sprawdzający, czy liczba jest złożona i korzystający wyłącznie z małego twierdzenia Fermata. Okazuje się jednak, że ten test można poprawić.

Przypuśćmy, że liczba p jest pierwsza i wiemy, że liczba x^2 daje resztę 1 przy dzieleniu przez p. Jaką resztę przy dzieleniu przez p daje sama liczba x? Jest to bardzo proste zadanie. Z założenia wiemy, że liczba p jest dzielnikiem liczby $x^2 - 1$, czyli liczby $(x - 1)(x + 1)$. Następnie korzystamy z twierdzenia mówiącego, że jeśli liczba pierwsza dzieli iloczyn dwóch liczb, to musi dzielić którąś z tych liczb. A więc albo liczba $x - 1$ dzieli się przez p, albo liczba $x + 1$ dzieli się przez p. W pierwszym przypadku $x \equiv 1 \pmod{p}$, w drugim $x \equiv -1 \pmod{p}$.

Okazuje się, że ta prosta obserwacja bardzo wiele wnosi do sprawdzania, czy liczba jest złożona. Popatrzmy na przykład. Wiemy już, że $11^{480} \equiv 1 \pmod{481}$. Ale $11^{480} = (11^{240})^2$. Niech więc $x = 11^{240}$. Wtedy $x^2 \equiv 1 \pmod{481}$. Gdyby liczba 481 była pierwsza, to liczba x musiałaby przystawać do 1 lub do -1 modulo 481. Sprawdźmy to. Okazuje się, że $11^{240} \equiv 1 \pmod{481}$. Jest więc tak, jak być powinno. Ale to nie koniec. Liczba 240 jest parzysta: $240 = 2 \cdot 120$, a więc 11^{240} też jest kwadratem, mianowicie $11^{240} = (11^{120})^2$. Możemy powtórzyć nasze rozumowanie. Okaże się, że znów $11^{120} \equiv 1 \pmod{481}$. Ale liczba 120 też jest parzysta, więc możemy to rozumowanie jeszcze raz powtórzyć. Niestety, znów okaże się, że $11^{60} \equiv 1 \pmod{481}$. Ale następnym razem już się uda: $11^{30} \equiv 38 \pmod{481}$. Nie otrzymaliśmy w wyniku ani liczby 1, ani liczby -1, a więc 481 jest liczbą złożoną.

Ten sposób postępowania, nazywany testem Millera–Rabina od nazwisk autorów, wygląda następująco. Mamy daną liczbę n i chcemy sprawdzić, czy jest ona złożona. Wybieramy podstawę a i sprawdzamy, czy liczby a i n są względnie pierwsze. Za pomocą algorytmu Euklidesa możemy to zrobić bardzo szybko. Jeśli znajdziemy wspólny dzielnik większy od 1, to liczba n na pewno jest złożona i mamy nawet jej rozkład na czynniki. Przypuśćmy więc, że liczby a i n są względnie pierwsze. Teraz podnosimy a do potęgi modulo n. Najpierw wybieramy wykładnik $k = n - 1$ i sprawdzamy, czy $a^k \equiv 1 \pmod{n}$. Jeśli nie, to wiemy na pewno, że liczba n jest złożona. Jeśli tak, to patrzymy na wykładnik k. Jeśli jest on parzysty (na początku na pewno tak będzie, bo liczba $n - 1$ jest parzysta), to zamiast k bierzemy liczbę $\frac{k}{2}$ i rozumowanie powtarzamy. Z tym tylko, że teraz dopuszczalnymi resztami są 1 i -1. Jeśli więc

$a^k \equiv 1 \pmod{n}$, to jest tak, jak być powinno i jeśli wykładnik k jest liczbą parzystą, to znów zastępujemy go dwa razy mniejszym. Jeśli jest liczbą nieparzystą, to kończymy test. Podobnie, jeśli $a^k \equiv -1 \pmod{n}$, to test kończymy, gdyż nic nie wiemy o liczbie x, gdy x^2 daje resztę -1 (dokładniej $n-1$) przy dzieleniu przez liczbę pierwszą n. Wreszcie, jeśli $a^k \not\equiv \pm 1 \pmod{n}$, to test również kończymy, wiedząc jednak tym razem, że liczba n jest złożona. Możliwe są więc trzy sposoby zakończenia testu:

1. Po kolejnych dzieleniach wykładnika k dojdziemy do sytuacji, gdy jest on liczbą nieparzystą i $a^k \equiv 1 \pmod{n}$. Wtedy nie rozstrzygnęliśmy, czy liczba n jest złożona.

2. Po kolejnych dzieleniach wykładnika k dojdziemy do sytuacji, gdy $a^k \equiv -1 \pmod{n}$. Wtedy również nie rozstrzygnęliśmy, czy liczba n jest złożona.

3. Po kolejnych dzieleniach wykładnika k dojdziemy do sytuacji, gdy $a^k \not\equiv \pm 1 \pmod{n}$. Wtedy wiemy na pewno, że liczba n jest złożona.

Popatrzmy na przykłady różnych zakończeń testu.

1. Niech $a = 100$. Wtedy
$$a^{480} \equiv a^{240} \equiv a^{120} \equiv a^{60} \equiv a^{30} \equiv a^{15} \equiv 1 \pmod{481}.$$

2. Niech $a = 36$. Wtedy
$$a^{480} \equiv a^{240} \equiv a^{120} \equiv a^{60} \equiv a^{30} \equiv 1 \pmod{481}$$
oraz
$$a^{15} \equiv -1 \pmod{481}.$$

Podobnie dla $a = 6$ mamy
$$a^{480} \equiv a^{240} \equiv a^{120} \equiv a^{60} \equiv 1 \pmod{481}$$
oraz
$$a^{30} \equiv -1 \pmod{481}.$$

3. Ten przypadek widzieliśmy wyżej. Inny przykład mamy dla $a = 27$:
$$a^{480} \equiv a^{240} \equiv a^{120} \equiv a^{60} \equiv a^{30} \equiv 1 \pmod{481}$$
oraz
$$a^{15} \equiv 443 \pmod{481}.$$

Ta metoda jest bardziej skomplikowana, niż zastosowanie tylko małego twierdzenia Fermata. Czy jest bardziej skuteczna? Okazuje się, że tak. Nie ma bowiem odpowiedników liczb Carmichaela. Jeśli liczba n jest złożona, to istnieje podstawa a, dla której test zakończy się tak jak w punkcie 3 powyżej, a więc będziemy wiedzieli na pewno, że liczba n jest złożona. Ale jak tę podstawę znaleźć? Pewnej metody nie znamy. Wiemy jednak, że takich podstaw jest dużo. Udowodniono, że co najmniej $\frac{3}{4}$ wszystkich liczb mniejszych od n to takie liczby a, dla których test zakończy się przypadkiem 3. Tych liczb szukamy losowo. Losujemy jakąkolwiek liczbę a mniejszą od n i przeprowadzamy test. Jeśli zakończy się on przypadkiem 3, to znamy odpowiedź: liczba n jest złożona. Jeśli test zakończy się przypadkiem 1 lub 2, to losujemy następną liczbę a. Powtarzamy ten test np. 50 razy. Jeśli za którymś razem dowiemy się, że liczba n jest złożona, to oczywiście testu już nie będziemy musieli powtarzać. Jeśli jednak 50 razy uzyskamy przypadek 1 lub 2, to będziemy mieli dwie możliwości. Albo liczba n jest pierwsza, albo mieliśmy niezwykle mało szczęścia w losowaniach podstaw a. Aż 50 razy z rzędu wylosowaliśmy liczbę ze stosunkowo małego zbioru „złych" liczb. Prawdopodobieństwo takiego nieszczęśliwego losowania jest bardzo małe: wynosi zaledwie $\frac{1}{2^{100}}$. Jest ono tak małe, że w praktyce możemy przyjąć, iż testowana liczba jest liczbą pierwszą.

Taki test nazywamy probabilistycznym. Z dowolnie dużym prawdopodobieństwem możemy „przekonać się", że liczba n jest pierwsza.

Rozwiązanie zadania F 450. Rozważmy najpierw sytuację, w której drgania są prostopadłe do płaszczyzny pajęczyny. Nitka wprawiona w drgania przez muchę wprawia w drgania punkt C, który z kolei wywołuje drgania wszystkich nitek, włącznie z tą, na której znajduje się mucha (fala odbita). Niech A oznacza amplitudę drgań nici wywołanych ruchami muchy, energia tych drgań jest proporcjonalna do kwadratu amplitudy. Gdy drgania odbywają się prostopadle do płaszczyzny pajęczyny, dzieli się ona po równo między wszystkie nici, a więc amplituda drgań każdej z nich jest taka sama i równa
$$\frac{A}{\sqrt{8}}.$$
W przypadku (b), gdy drgania zachodzą w płaszczyźnie pajęczyny, drgający punkt C nie pobudzi do drgań nici 1 (bo C porusza się właśnie wzdłuż niej); amplituda drgań nici 3 będzie taka sama jak nici, na której szamocze się mucha, a amplituda nici 2 będzie $\cos 45°$ razy taka. Z zasady zachowania energii otrzymujemy:
$$A^2 = 2A_3^2 + 4A_2^2 = 2A_3 + 4 \cdot \frac{1}{2}A_3^2 = 4A_3^2.$$
Wynika stąd, że
$$A_3 = \frac{1}{2}A, \quad A_2 = \frac{1}{\sqrt{8}}A.$$
W realnym życiu pająka (a przede wszystkim muchy) sytuacja jest bardziej skomplikowana, przede wszystkim z powodu bardziej złożonej geometrii pajęczyny. Poprzeczne nici powodują, między innymi, że drgania w płaszczyźnie sieci będą się jednak przenosić także i na nić 1.

Rozwiązanie zadania M 804. Skoczek stojący na białym polu atakuje tylko pola czarne. Podobnie, skoczek stojący na polu czarnym atakuje tylko pola białe. Albo co najmniej 1000 skoczków stoi na polach białych, albo co najmniej 1000 skoczków stoi na polach czarnych (zasada szufladkowa Dirichleta). Ponieważ skoczki stojące na polach tego samego koloru nie mogą się atakować, więc teza zadania jest prawdziwa.

Rozwiązanie zadania M 806.
Na mocy nierówności Bernoulliego $((1+x)^n \geq 1+nx$ dla $x > -1$ i dla naturalnych n) mamy

$$(1+\frac{m}{n})^n \geq 1+n\cdot\frac{m}{n} = m+1,$$

więc

$$\frac{1}{\sqrt[n]{m+1}} \geq \frac{n}{m+n}.$$

Podobnie,

$$\frac{1}{\sqrt[m]{n+1}} \geq \frac{m}{m+n}.$$

Dodając obie nierówności stronami, otrzymujemy stąd

$$\frac{1}{\sqrt[n]{m+1}} + \frac{1}{\sqrt[m]{n+1}} \geq$$
$$\geq \frac{n}{m+n} + \frac{m}{m+n} = 1.$$

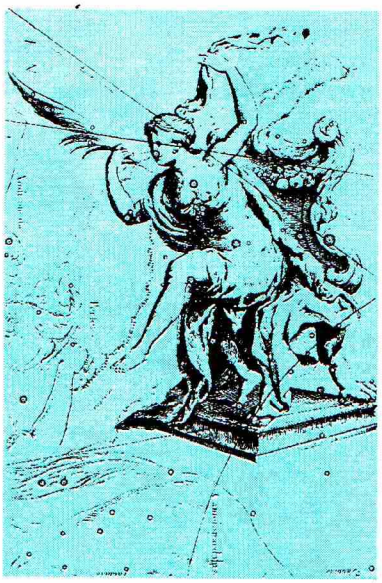
Jednak całkowitej pewności nie mamy. Chcielibyśmy mieć również testy dające pewność wyniku: albo liczba n jest pierwsza, albo jest złożona. Takie testy istnieją, choć są znacznie wolniejsze od testu opisanego wyżej. Za pomocą testu Millera–Rabina możemy na małym komputerze szybko testować liczby nawet kilkusetcyfrowe. Najprostsze znane testy deterministyczne (tzn. dające odpowiedź pewną) wymagają znacznie większych komputerów i działają znacznie wolniej.

Na zakończenie wspomnę jeszcze, że z pewnej nie udowodnionej dotychczas hipotezy, tzw. uogólnionej hipotezy Riemanna, wynika, że jeśli liczba n jest złożona, to istnieje podstawa $a < 70(\log_2 n)^2$, dla której test Millera kończy się przypadkiem 3. A więc wtedy mamy pewność, że liczba n jest złożona. Wystarczy w tym celu przebadać nie więcej niż $70(\log_2 n)^2$ podstaw. Jeśli liczba n ma około 100 cyfr dziesiętnych, to wystarczy zbadać około 8 milionów podstaw, a to można zrobić za pomocą stosunkowo niedużego komputera.

Patrz w niebo

Jowisz jest nagminnie cytowanym przykładem obiektu w Układzie Słonecznym, który znacznie więcej wyświeca energii, niż otrzymuje jej od Słońca. Obecnie wszyscy badacze zgodnie twierdzą, że ten nadmiar energii Jowisza pochodzi z bardzo powolnego kurczenia się całego globu (lub jego pewnych części), czyli nieznacznego osiadania „pod własnym ciężarem", choć różnią się co do szczegółów tego procesu.

Do niedawna wydawało się, że w Układzie Słonecznym jest jeszcze jeden glob zachowujący się do pewnego stopnia analogicznie, mianowicie satelita Jowisza, Io. Jego energiczny wulkanizm wywołany jest tym, że zmiany odległości od Jowisza powodują zmienne działanie pływowe planety, a to pociąga za sobą ustawiczne wyginanie skorupy satelity, a więc jego grzanie. Otóż pomiary promieniowania podczerwonego (wykonane już dawno przez Voyagery i kontynuowane do dziś) wykazały, że glob satelity jest średnio gorętszy, niż wynikałoby to z pływowego działania Jowisza. Nietrudno domyślić się, że wyjaśnienie tego faktu nastąpiło w wyniku uwzględnienia wpływu promieniowania słonecznego na warunki panujące na Io. Wpływ ten okazał się jednak nie tak oczywisty, jak się z początku zdawało.



Przede wszystkim stwierdzono, że większość termicznego promieniowania Io pochodzi wcale nie z zapadlisk wypełnionych płynną lub krzepnącą magmą o temperaturze od 600 K wzwyż. Najwięcej podczerwieni emitują wielkie, obejmujące tysiące kilometrów kwadratowych obszary niezbyt gorące, bo o temperaturze około 300 K, a więc o około 100 K wyższej, niż ma średnio grunt na dziennej stronie Io. Nawiasem mówiąc, obszarom tym nie odpowiadają żadne widoczne na powierzchni obiekty. Całkowita emisja podczerwieni przez satelitę gwałtownie spada, gdy wchodzi on w cień Jowisza, musi więc za nią odpowiadać w dużym stopniu Słońce, a zmiany temperatury mógłby tłumaczyć fakt, że widocznie powierzchnia Io pokryta jest warstwą pyłu o małej pojemności cieplnej. Jednak te wielkie ciepłe obszary pozostają ciepłe po wejściu satelity w cień Jowisza, ich energia musi więc pochodzić z głębi globu i hipoteza pyłu jest nie do obronienia.

Zasugerowano wreszcie, że za gwałtowne skoki emisji podczerwieni mogą być odpowiedzialne wspomniane już rozlewiska lawy. Choć są już gorące, to jednak jako czarne absorbują niemal całe padające na nie promieniowanie słoneczne. Stają się przez to gorętsze i przyczyniają się w ten sposób do zwiększenia emisji podczerwieni Io, a w cieniu Jowisza mogą szybko wystygnąć do poprzedniej temperatury. Problem był więc w zasadzie banalny – przeoczono absorpcję promieniowania słonecznego w samych rozlewiskach lawy. Ich powierzchnia jest w sumie niewielka, lecz przy dokładności współczesnych technik pomiarowych niezgodność obserwacji z teorią domagała się wyjaśnienia.

Tomasz KWAST