9/01 (45)

Γ limatias $n \to \infty$

DLACZEGO? (II/4)

Pytanie, **DLACZEGO** liczba a_{2040} nie jest całkowita, jest trochę niewłaściwie postawione. Nie jest całkowita, bo nie widać powodów, żeby była. Obliczając kolejne wyrazy ciągu (a_n), wykonujemy dzielenie, które wcale nie musi prowadzić do liczby całkowitej. To, co naprawdę wymaga wyjaśnienia, to **DLACZEGO** liczby a_n są całkowite dla $n \leq 2039$. Oczywiście, nie udowodnię tego bez liczenia, pokażę jednak powody, dla których całkowitość wielu wyrazów ciągu (a_n) nie powinna dziwić.

W celu dokładniejszego przeanalizowania procedury obliczania kolejnych wyrazów ciągu (a_n) wprowadźmy pomocniczy ciąg (S_n) zdefiniowany wzorem

$$S_n = a_0^{97} + a_1^{97} + a_2^{97} + \ldots + a_n^{97} .$$

Wówczas, wobec równości $a_{n+1} = \frac{S_n}{n}$, ciąg (S_n) możemy określić rekurencyjnie wzorami

$$S_0 = 1, \quad S_1 = 2, \quad S_{n+1} = S_n + \left(\frac{S_n}{n}\right)^{97} \quad \text{dla } n = 1, 2, 3, \ldots$$

Zależność rekurencyjna może być zapisana w postaci

$$(7\diamondsuit) \qquad S_{n+1} = \frac{S_n}{n}\left(n + \left(\frac{S_n}{n}\right)^{96}\right) .$$

Niech p będzie liczbą pierwszą. Przypuśćmy, że liczby a_n są całkowite dla $n \leq p$. Kolejny wyraz obliczamy ze wzoru $a_{p+1} = \frac{S_p}{p}$. Chcę wyjaśnić **DLACZEGO** jest bardzo duża szansa (ale tylko szansa!) na to, że S_p dzieli się przez p. Przyjrzyjmy się wzorowi $(7\diamondsuit)$. Wynika z niego, że jeżeli dla pewnego $n < p$ liczba S_n dzieli się przez p, to S_{n+1} i wszystkie następne, aż do S_p, także dzielą się przez p. Jeśli zaś S_n nie dzieli się przez p, to czynnik $n + \left(\frac{S_n}{n}\right)^{96}$ przez p się dzieli albo nie dzieli. Jest jednak pewna szansa, że się dzieli, a wtedy ciąg (S_n) „łapie" podzielność przez p i nie puszcza jej aż do wykonania dzielenia przez p przy obliczaniu a_{p+1}.

Jest też druga, mniej widoczna, ale silniejsza przyczyna, **DLACZEGO** S_p lubi dzielić się przez p. Otóż jeśli dla pewnego $n < p$ mamy $\left(\frac{S_n}{n}\right)^{96} \equiv 1 (\mathrm{mod}\ p)$, to

$$\frac{S_{n+1}}{n+1} = \frac{S_n}{n}\left(n + \left(\frac{S_n}{n}\right)^{96}\right) \cdot \frac{1}{n+1} \equiv$$

$$\equiv \frac{S_n}{n}(n+1) \cdot \frac{1}{n+1} \equiv \frac{S_n}{n} (\mathrm{mod}\ p) ,$$

skąd wynika, że także $\left(\frac{S_{n+1}}{n+1}\right)^{96} \equiv 1 (\mathrm{mod}\ p)$.

W konsekwencji $\left(\frac{S_{p-1}}{p-1}\right)^{96} \equiv 1 (\mathrm{mod}\ p)$, co daje

$$S_p = \frac{S_{p-1}}{p-1}\left(p - 1 + \left(\frac{S_{p-1}}{p-1}\right)^{96}\right) \equiv \frac{S_{p-1}}{p-1} \cdot p \equiv 0 (\mathrm{mod}\ p) .$$

Widzimy więc, że jeżeli $\left(\frac{S_n}{n}\right)^{96} \equiv 1 (\mathrm{mod}\ p)$, to $\left(\frac{S_{n+1}}{n+1}\right)^{96} \equiv 1 (\mathrm{mod}\ p)$ i mamy zagwarantowaną podzielność S_p przez p. Jeśli natomiast $\left(\frac{S_n}{n}\right)^{96} \not\equiv 1 (\mathrm{mod}\ p)$, to może być $\left(\frac{S_{n+1}}{n+1}\right)^{96} \not\equiv 1 (\mathrm{mod}\ p)$ lub $\left(\frac{S_{n+1}}{n+1}\right)^{96} \equiv 1 (\mathrm{mod}\ p)$. Jest pewna szansa, że zajdzie ten drugi przypadek, co oznacza, że ciąg (S_n) złapie gwarancję podzielności S_p przez p.

Podsumowując: są dwa rodzaje przyczyn, dla których S_p dzieli się przez p:

(i) dla pewnego $n < p$ liczba S_n dzieli się przez p,

(ii) dla pewnego $n < p$ zachodzi $\left(\frac{S_n}{n}\right)^{96} \equiv 1 (\mathrm{mod}\ p)$.

Oczywiście, te dwie przyczyny wzajemnie się wykluczają. Jeśli jednak dla pewnego n nie zachodzi żadna z nich, to jest pewna szansa, że przy $n+1$ jedna z nich się objawi. Jeśli więc śledzimy powstawanie ciągu (S_n), to do podzielności S_p przez p potrzeba, aby po drodze zaistniała jedna z powyższych przyczyn.

Jeśli przyjmie się założenie, że wedle naszej wiedzy reszty $S_n (\mathrm{mod}\ p)$ i $\frac{S_n}{n} (\mathrm{mod}\ p)$ są losowe, dopóki ciąg S_n nie złapie jednego z warunków (i) lub (ii), to można oczekiwać, że na każdym kroku prawdopodobieństwo złapania warunku (i) jest rzędu $\frac{1}{p}$, natomiast prawdopodobieństwo złapania warunku (ii) jest rzędu $\frac{NWD(p-1,96)}{p-1}$. Liczba $NWD(p-1, 96)$ to liczba reszt *modulo* p, których 96-ta potęga jest jedynką *modulo* p.

Jeśli więc $p - 1 | 96$, to warunek $\left(\frac{S_n}{n}\right)^{96} \equiv 1 (\mathrm{mod}\ p)$ jest spełniony od samego początku (poza $p = 2$). To dowodzi podzielności S_p przez p dla $p = 3, 5, 7, 13, 17, 97$.

Prześledźmy w pewnych szczególnych przypadkach, jakie są nasze przewidywania.

Przypadek $p \equiv 11 (\mathrm{mod}\ 12)$. Wtedy $NWD(p-1, 96) = 2$ i oczekujemy, że na każdym kroku ciąg (S_n) łapie warunek (i) z prawdopodobieństwem rzędu $\frac{1}{p}$ i warunek (ii) z prawdopodobieństwem rzędu $\frac{2}{p}$, co daje razem prawdopodobieństwo rzędu $\frac{3}{p}$ (interesują nas duże p i liczymy tylko rząd wielkości prawdopodobieństwa).

Nasze przewidywania:

1) warunek (ii) zajdzie około 2 razy częściej niż (i),
2) na zajście któregokolwiek z tych warunków trzeba czekać średnio około $\frac{p}{3}$ kroków,
3) S_p dzieli się przez p z prawdopodobieństwem rzędu $1 - \left(1 - \frac{3}{p}\right)^p \approx 1 - e^{-3} \approx 0{,}95$.

Podobnie w przypadku gdy $p \equiv 5 (\mathrm{mod}\ 24)$, czyli gdy $NWD(p-1, 96) = 4$, przewidujemy prawdopodobieństwo podzielności S_p przez p rzędu $1 - e^{-5} \approx 0{,}993$. Jakkolwiek z uwagi na przyjęte uproszczenia nasze przewidywania nie są dokładne ilościowo, to jakościowo dają dobry obraz zachowania ciągów (a_n) i (S_n). Oczekujemy, że podzielność S_p przez p dla liczb pierwszych $p \equiv 11 (\mathrm{mod}\ 12)$ zajdzie w 95%, a dla innych liczb pierwszych będzie jeszcze lepiej.

Skoro podzielność S_p przez p jest prawie (ale tylko prawie!) pewna, nie powinno dziwić, że wyrazy ciągu (a_n) są przez długi czas całkowite. Nie przeprowadzamy analizy podzielności przez liczby złożone, nietrudno jednak uwierzyć, że dochodzą wówczas do głosu podobne zjawiska.

JWR

Korespondencję do Γ-limatiasu prosimy kierować pod adresem:
Jarosław Wróblewski, Instytut Matematyki Uniwersytetu Wrocławskiego, Plac Grunwaldzki 2/4, 50-384 WROCŁAW; e-mail: jwr@math.uni.wroc.pl