5/00 (29)

Γ $\lim\limits_{n\to\infty}$atias

MIĘDZY NAMI OSZUSTAMI (21″)

Wyjaśnienie oszustwa (21′): Dla $n = 21$ dowód twierdzenia się nie udał, ale samo twierdzenie jest prawdziwe, gdyż np. $5^3 \equiv -1 \pmod{21}$.

Okazuje się bowiem, że twierdzenie jest prawdziwe dla prawie wszystkich liczb nieparzystych n.

Idea poprawnego dowodu jest następująca.

Rozkładamy n na iloczyn potęg różnych liczb pierwszych, $n = p_1^{w_1} p_2^{w_2} \dots p_s^{w_s}$.

Mamy znaleźć takie a i k, aby $a \not\equiv -1 \pmod{n}$ oraz $a^k \equiv -1 \pmod{n}$. Korzystając z chińskiego twierdzenia o resztach zauważamy, że jest to równoważne znalezieniu takich liczb $a_1, a_2, \dots, a_s$ i k, że $a_i^k \equiv -1 \pmod{p_i^{w_i}}$ dla wszystkich $i \in \{1, 2, \dots, s\}$, a przy tym $a_j \not\equiv -1 \pmod{p_j^{w_j}}$ dla co najmniej jednego $j \in \{1, 2, \dots, s\}$. Jak znaleźć takie liczby $a_1, a_2, \dots, a_s$ i k? Otóż wybieramy takie j, aby liczba $p_j^{w_j}$ nie była liczbą pierwszą Fermata (tj. liczbą pierwszą postaci $2^{2^m} + 1$). Wystarczy, na przykład, aby $w_j > 1$. Wówczas znajdziemy takie k nieparzyste oraz $a_j \not\equiv -1 \pmod{p_j^{w_j}}$, że $a_j^k \equiv -1 \pmod{p_j^{w_j}}$. Wynika to z faktów teorioliczbowych, których omawianie pominiemy. Wystarczy teraz przyjąć $a_i = p_i^{w_i} - 1$ dla $i \neq j$.

To kończy dowód twierdzenia w przypadku, gdy w rozkładzie liczby n na potęgi liczb pierwszych występuje liczba pierwsza w potędze większej od 1 lub liczba pierwsza nie będąca liczbą pierwszą Fermata.

Jeśli n jest iloczynem różnych liczb pierwszych Fermata większych od 3, to możemy przyjąć $k = 2$ i wówczas uda się dobrać $a_1, a_2, \dots, a_s$ o własnościach podanych powyżej. Znowu pomijamy teorię, która za tym stoi.

Jeśli n jest iloczynem różnych liczb pierwszych Fermata, wśród których występuje liczba 3, wówczas (i tylko wówczas) twierdzenie jest fałszywe. Wynika to z faktu, że dla żadnej liczby pierwszej Fermata p kongruencja $a^k \equiv -1 \pmod{p}$ nie może być spełniona przez $a \not\equiv -1 \pmod{p}$ i k nieparzyste. Gdyby zatem twierdzenie było prawdziwe dla n będącego iloczynem różnych liczb pierwszych Fermata, k musiałoby być parzyste. Tymczasem dla k parzystego kongruencja $a^k \equiv -1 \pmod{3}$ zachodzić nie może.

Znanych jest 5 liczb pierwszych Fermata: 3, 5, 17, 257 i 65537. Wobec tego twierdzenie jest fałszywe dla następujących 15 liczb nieparzystych $n > 3$: 15, 51, 255, 771, 3855, 13107, 65535, 196611, 983055, 3342387, 16711935, 50529027, 252645135, 858993459, 4294967295.

I tylko dla tych 15 liczb, o ile nie istnieją liczby pierwsze Fermata poza wymienionymi powyżej.

JWR

GRY (13)

Poprzednio podaliśmy sposób obliczania liczby Grundy'ego $r(n)$ gry RÓŻNE STOSY rozpoczynającej się od jednego stosu złożonego z n bierek i obliczyliśmy $r(n)$ dla $n \le 10$. Dalsze wartości $r(n)$ podane są w poniższej tabeli (numer kolumny jest cyfrą jedności liczby n, a numer wiersza jest równy $\left[\frac{n}{10}\right]$).

	0	1	2	3	4	5	6	**7**	8	9
0		0	0	1	0	2	1	0	2	1
1	0	2	1	3	2	1	3	2	4	3
2	0	4	3	0	4	3	0	4	1	2
3	3	1	2	4	1	2	4	**1**	2	4
4	1	5	4	1	5	4	1	5	4	1
5	0	2	1	0	2	1	5	2	1	3
6	2	1	3	2	4	3	2	4	3	2
7	4	3	2	4	3	2	4	3	2	4
8	5	2	4	5	2	4	3	7	4	3
9	7	4	3	7	4	3	5	2	3	5
10	2	3	5	2	3	5	2	3	5	2
11	3	5	2	3	5	2	3	5	2	3
12	5	2	3	5	2	4	5	2	4	5
13	2	4	5	2	4	5	2	4	8	2
14	4	8	2	4	3	2	6	3	2	6
15	3	2	6	3	2	8	3	2	11	3
16	2	11	3	2	11	3	2	11	3	2
17	8	3	5	8	3	5	7	3	5	7
18	3	12	7	3	8	7	3	8	7	3
19	12	5	3	12	5	3	10	5	3	4
20	5	3	4	2	3	4	2	3	4	2
21	3	4	2	3	4	2	3	4	2	3
22	4	2	3	4	2	3	4	2	3	4
23	2	10	1	2	5	1	2	5	1	2
24	5	3	2	5	3	4	5	3	4	5
25	3	4	5	3	4	2	3	4	2	3

	0	1	2	3	4	5	6	**7**	8	9
26	4	2	3	4	2	3	4	2	3	4
27	0	3	4	0	3	4	0	3	4	2
28	3	1	0	14	1	0	14	1	0	5
29	1	13	5	1	13	5	1	13	2	1
30	13	2	1	13	2	1	13	2	1	13
31	2	3	13	2	3	13	0	3	14	2
32	3	16	2	3	1	2	16	1	2	16
33	1	2	16	1	0	16	1	0	12	1
34	0	12	1	5	2	1	0	2	1	5
35	2	1	5	2	8	3	2	4	3	0
36	8	5	0	3	5	0	3	5	2	3
37	5	2	4	5	2	4	5	2	4	12
38	7	4	3	7	4	3	0	4	3	0
39	2	3	0	2	3	5	2	3	5	2
40	3	5	2	3	5	2	3	5	2	3
41	5	2	3	5	2	3	5	2	4	5
42	2	4	5	2	4	5	2	4	5	2
43	4	16	2	4	3	2	4	3	2	8
44	3	2	8	3	2	8	3	2	8	3
45	2	11	3	2	11	3	7	11	3	5
46	11	3	5	4	3	5	14	3	5	7
47	3	5	2	3	7	2	3	8	2	3
48	8	2	3	8	2	3	16	2	3	16
49	2	3	4	2	3	4	2	3	4	8
50	11	4	2	11	9	2	4	6	5	4
51	6	5	13	6	2	13	6	2	16	6

Z pomocą tej tabeli odpowiemy na pytania zadane przed miesiącem. Po pierwsze odczytujemy, że $r(37) = 1$, więc rozpoczynający ma strategię wygrywającą. Po drugie stwierdzamy, że dobre posunięcia pierwszego gracza to podział stosu 37 bierek na dwa stosy o licznościach 3 i 34, 5 i 32, 6 i 31, 8 i 29 lub 9 i 28.

Tak więc dobrych posunięć jest aż 5. Na przykład liczba Grundy'ego pozycji złożonej ze stosów mających 8 i 29 bierek jest równa $r(8) +_2 r(29) = 2 +_2 2 = 0$, więc istotnie pozycja ta jest wygrywająca dla drugiego gracza.

I wreszcie, skoro nasz przeciwnik popełnił błąd w pierwszym ruchu, dokonując podziału wyjściowego stosu na stosy liczące 17 i 20 bierek, to mamy możliwość zapewnienia sobie wygranej. Jest tylko jeden ruch wygrywający, a mianowicie podział stosu z 17 bierkami na stosy mające 10 i 7 bierek. Podajemy więc przeciwnikowi pozycję złożoną z trzech stosów mających odpowiednio 20, 10 i 7 bierek. Pozycja ta jest wygrywająca dla drugiego gracza, gdyż jej liczba Grundy'ego wynosi $r(20) +_2 r(10) +_2 r(7) = 0 +_2 0 +_2 0 = 0$.

I na koniec jeszcze jedna uwaga. W grze RÓŻNE STOSY na ogół strategię wygrywającą ma gracz rozpoczynający. Wyjątkiem są te liczności n wyjściowego stosu, dla których $r(n) = 0$. Oto pełna lista takich $n \le 1000$:

1, 2, 4, 7, 10, 20, 23, 26, 50, 53, 270, 273, 276, 282, 285, 288, 316, 334, 337, 340, 346, 359, 362, 365, 386, 389, 392, 566, 630, 633, 636, 639, 673, 676, 682, 685, 923, 926, 929, 932.

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