LISTA 4

TW O CHIŃSKI RESZTACH

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \qquad x = a_{12} \pmod{\mathrm{nww}(m_1, m_2)}$$

ZAD 2

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{13} \end{cases}$$

parami względnie pierwsze (nwd ) = 1

$i, j, k, h, l \in \mathbb{Z}$

dowolne liczby całkowite

METODA GENEROWANIA KOLEJNYCH WIELOKROTNOŚCI

Ogólne rozwiązanie równania pierwszego

$2 + 5 \cdot i$

Zobaczmy jakie wartości przyjmuje równanie dla najmniejszych $i$.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| | 2 | 7 | 12 | 17 | 22 | 27 |

Tak samo rozpiszmy równanie drugie

$$3+j\cdot 7$$

| $j$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| | 3 | 10 | 17 | 24 | 31 | 38 |

Widzimy, że dla obu równań pojawia się to samo rozwiązanie 17.

Zapiszmy więc $17 \pmod{(5\cdot 7)}$

$$\Downarrow$$

$$17+k\cdot 35$$

| $k$ | 0 | 1 | 2 |
|---|---|---|---|
| | 17 | 52 | 87 |

Trzecie równanie też rozpiszmy. $x \equiv 4 \pmod{13}$

$$4+13\cdot h$$

| $h$ | 0 | 1 | 2 |
|---|---|---|---|
| | 4 | 17 | 30 |

Czyli najmniejsze rozwiązanie to 17, a ogólne $17+(5\cdot 7\cdot 13)l$

ZAD 1 OBLICZ DWIE OSTATNIE CYFRY W ROZWINIĘCIU DZIESIĘTNYM LICZBY $71^{71}$.

Z wykładu

$\underbrace{71^{71} \bmod 100}$ → bo interesują nas dwie ostatnie liczby

SPOSÓB I obserwacja ostatnich dwóch liczb

$71^1 = 71$
$71^2 = \ldots 41$
$71^3 = \ldots 11$
$71^4 = \ldots 81$
$71^5 = \ldots 51$
$71^6 = \ldots 21$
$71^7 = \ldots 91$
$71^8 = \ldots 61$
$71^9 = \ldots 31$
$71^{10} = \ldots 01$

10 liczb

dodajemy + 70 widać to dokładnie przy mnożeniu pisemnym

$$\begin{array}{r} 71 \\ \cdot\ 71 \\ \hline 71 \\ +497\ \ \\ \hline 5041 \end{array} \qquad \begin{array}{r} 5041 \\ 71 \\ \hline 5041 \\ +35287\ \ \\ \hline 357911 \end{array}$$

Ostatnie 2 cyfry to 71.

SPOSÓB II

$$x \equiv 71^{71} \pmod{100} \iff \begin{cases} x \equiv 71^{71} = (-1)^{71} = 3 \pmod 4 \\ x \equiv 71^{71} = 71 \cdot (71^5)^{14} = 71 \cdot 1^{14} = 71 \pmod{25} \end{cases}$$

$$\begin{cases} 1^\circ\ x \equiv 3 \pmod 4 \longrightarrow 3 + 4 \cdot i \\ 2^\circ\ x \equiv 71 \pmod{25} \longrightarrow 71 + 25 \cdot j \end{cases}$$

| i/j | 0 | 1 | 2 | | 17 |
|---|---|---|---|---|---|
| 1° | 3 | 7 | 11 | . . . . . . . . | 71 |
| 2° | 71 | | | | |

ZAD. 3 WYKAŻ, ŻE JEŚLI $2^n - 1$ JEST LICZBĄ PIERWSZĄ, TO N JEST LICZBĄ PIERWSZĄ

Zakładamy, że $2^n - 1$ jest liczbą pierwszą. Załóżmy nie wprost, że $n$ nie jest liczbą pierwszą, czyli $n = x \cdot y$.

Mamy więc $2^{x \cdot y} - 1 = (2^x)^y - 1$

$x, y > 1$

Rozpisujemy ze wzoru

$$a^x - 1 = (a-1)(a^{x-1} + a^{x-2} + \ldots + a + 1)$$

$$(2^x)^y - 1 = (2^x - 1)(2^{x(y-1)} + 2^{x(y-2)} + \dots + 2^x + 1)$$

Udało się nam rozpisać liczbę $2^n-1$ jako iloczyn 2 liczb całkowitych. Z założenia wiemy, że liczba $2^n-1$ nie jest pierwsza. Jest to więc sprzeczność.

**ZAD 4.** Wykaż, że jeśli $a^n-1$ jest ~~parzyste~~ pierwsza to $a=2$

Rozpiszmy $a^n-1$

$$(a^n-1) = \underbrace{(a-1)}(a^{n-1} + a^{n-2} + \dots + a + 1)$$

Jeśli $a$ nie będzie 2

to 1°) jeśli $a=1$ to wyjdzie zero

2°) w każdym innym przypadku wyjdzie nam liczba i sprawi, że $a^n-1$ zostanie zapisane jako iloczyn dwóch liczb co przeczy faktowi, że $a^n-1$ jest liczbą pierwszą.

**ZAD. 5.** WYKAŻ, ŻE JEŚLI $2^n+1$ JEST LICZBĄ PIERWSZĄ TO N JEST POTĘGĄ LICZBY 2.

Załóżmy, że $2^n+1$ jest liczbą pierwszą a $n$ nie jest potęgą 2.

$n = 2^a \cdot b \qquad b \neq 2$

używając wzoru*

$$2^n + 1 = 2^{2^a \cdot b} + 1 = (2^{2^a})^b + 1 = x \neq 1$$

$$= (\underset{\geq 3}{2^{2^a}} + 1)(2^{2^a(b-1)} - 2^{2^a(b-2)} + \dots - 2^{2a} + 1)$$

Z założenia wiemy, że liczba $2^n+1$ jest pierwsza, a teraz udało nam się ją przedstawić jako iloczyn 2 liczb. Sprzeczność.

$$*\ (a^n+1) = (a+1)(a^{n-1} - a^{n-2} + \dots - a + 1)$$

Scanned with CamScanner

$$x = \underbrace{2^{2^a(b-1)} - 2^{2^a(b-2)}} + \dots - 2^{2^a} + 1$$

$$2^{2^a(b-2)} \cdot 2^{2^a} - 2^{2^a(b-2)}$$

$$\underbrace{2^{2^a(b-2)}}_{\geq 2} \cdot \underbrace{\left(2^{2^a} - 1\right)}_{>1} +$$

ZAD. 6 (-) OKREŚL LICZBĘ PODZIELNĄ PRZEZ 7, KTÓRA LEŻY NAJBLIŻEJ LICZBY $10^{100000}$

$10^{100\,000} \bmod 7$

$10^1 \equiv_7 3$
$10^2 \equiv_7 2$
$10^3 \equiv_7 6$
$10^4 \equiv_7 4$
$10^5 \equiv_7 5$
$10^6 \equiv_7 1$ } można z tw. Fermata
$10^7 \equiv_7 3$

$a^p - a = 0 \pmod p$
$a^{p-1} = 1 \pmod p$

Który element cyklu wybieramy?

$100\,000 \bmod 6 = 40\,000 \bmod 6 = 4\,000 \bmod 6 = 400 \bmod 6 = 40 \bmod 6 = 4 \bmod 6$

$10^{100\,000} \bmod 7 = 10^4 \bmod 7 = 4$

$(10^{100\,000} - 4) \bmod 7 = 0$ $\quad |10^{100000} - 4 - 10^{100000}| = 4$

$(10^{100\,000} + 3) \bmod 7 = 0$ $\quad |10^{100000} + 3 - 10^{100000}| = 3$

liczba podzielna przez 7 najbliższa $10^{100000}$ to $10^{100000}+3$.

ZAD. 7 PODAJ DWIE OSTATNIE CYFRY LICZBY $9^{8^{7^{6^{5^{4^{3^{2^{1}}}}}}}}$ W ROZWIJANIU DZIESIĘTNYM

Zauważmy, że jeśli interesują nas 2 ostatnie cyfry, to dla potęgi 9 mamy okres 10 (w co 10 potędze ostatnie 2 cyfry są takie same)

Na podstawie tego, że 9 ma okres 10 możemy powiedzieć, że

$$9^x \bmod 100 = 9^{x \bmod 10} \bmod 100$$

8 ma okres 4 (ostatnia cyfra powtarza się w co 4 potędze, ostatnia, bo $x \bmod 10$).

7 ma okres 4 (ostatnie 2 cyfry powtarzają się w co 4 potędze ostatnie 2, bo $8^{y \bmod 4}$, a przy mod 4 patrzymy na ostatnie 2)

$9^1 = 9$
$9^2 = 81$
$9^3 = 29$
$9^4 = 61$
$9^5 = 49$
$9^6 = 41$
$9^7 = 69$
$9^8 = 21$
$9^9 = 89$
$9^{10} = 1$

więc: $8^y \bmod 10 = 8^{y \bmod 4} \bmod 10$

$$7^z \bmod 4 = 7^{z \bmod 4} \bmod 4$$

$$6^a \bmod 4 = 0$$

wszystkie potęgi 6 są podzielne przez 4, więc mod 4 da nam 0 $(a \geq 2)$

Zatem $z \bmod 4 = 6^a \bmod 4 = 0$
$y \bmod 4 = 7^0 \bmod 4 = 1$
$x \bmod 10 = 8^1 \bmod 10 = 8$

$$9^{x \bmod 10} \bmod 100 = 9^8 \bmod 100 = 21$$

ZAD 8. WYKAŻ, ŻE DWIE KOLEJNE LICZBY FIBONACCIEGO SĄ WZGLĘDNIE PIERWSZE.
WSKAZÓWKA: SKORZYSTAJ Z ALGORYTMU EUKLIDESA.

Podstawa: $F_0 = 0$

$n=1$ $\quad nwd(F_1, F_{n+1}) = nwd(F_1, F_2) = nwd(1,1) = 1$

Założenie:
Dla $n$ $NWD(F_n, F_{n-1}) = 1$ $n \in \mathbb{N}$

Krok:
Weźmy $n+1$ i sprawdźmy, czy dla niego też działa $NWD(F_{n+1}, F_n)$

Robimy alg. Euklidesa. W pierwszym kroku $F_{n+1} - F_n = F_{n-1}$, a z założenia wiemy, że wtedy działa.

Dla $n+1$ zatem działa.

Euklides dla $n+1$

$NWD(a,b) = NWD(a, b-a)$

| $F_n$ | $F_{n+1}$ | $F_n + F_{n-1} - F_n = F_{n-1}$ |
|---|---|---|
| $F_n$ | $F_{n-1}$ | $F_{n-1} + F_{n-2} - F_{n-1} = F_{n-2}$ |
| $F_{n-1}$ | $F_{n-2}$ | $F_{n-2} + F_{n-3} - F_{n-2} = F_{n-3}$ |
| $F_{n-2}$ | $F_{n-3}$ | $F_{n-3} + F_{n-4} - F_{n-3} = F_{n-4}$ |
| $\vdots$ | $\vdots$ | |
| $F_3$ | $F_2$ | $F_3 - F_2 = F_2 + F_1 - F_2 = F_1$ |
| $F_2 = 1$ | $F_1 = 1$ | $1 - 1 = 0$ |
| $1$ | $0$ | |

Zatem $nwd(F_n, F_{n+1}) = 1$

ZAD 9. UDOWODNIJ LUB OBAL NASTĘPUJĄCE STWIERDZENIE:
LICZBA NATURALNA A, KTÓREJ ZAPIS W SYSTEMIE DZIESIĘTNYM TO $a_n a_{n-1} \dots a_2 a_1 a_0$ DZIELI SIĘ PRZEZ 11 WTW GDY LICZBA
$\sum_{i=1}^{n/2} a_{2i-1} - \sum_{i=0}^{n/2} a_{2i}$ JEST PODZIELNA PRZEZ 11.

$x = a_n a_{n-1} \dots a_1 a_0$
$x = a_0 + 10a_1 + 100a_2 + \dots + 10^n a_n$
$x = a_0 + (11-1)a_1 + (99+1)a_2 + (1001-1)a_3 + \dots$
$x = \underbrace{(11a_1 + 99a_2 + 1001a_3 + \dots)}_{\text{jest podzielne przez 11}} + \underline{(a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 \dots}$

$\to$ musi być podzielna przez 11, żeby $11 | x$

Więc żeby $x$ było podzielne przez 11, to jeszcze pozostała część sumy musi być podzielna przez 11 i to zauważmy

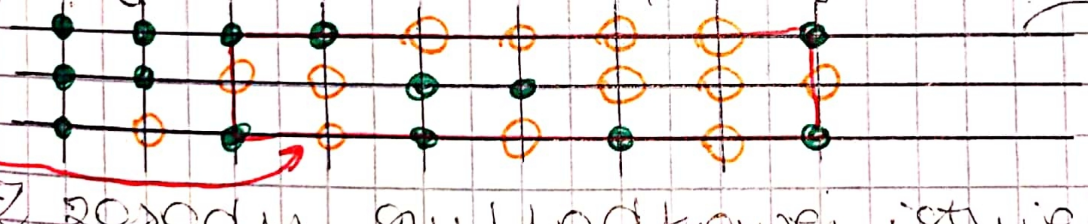
$$-(a_0 + a_2 + a_3 + \ldots) + (a_1 + a_3 + \ldots) =$$

$$= \sum_{i=1}^{M/2} a_{2i-1} - \sum_{i=0}^{M/2} a_{2i}$$

co ile?
[illegible] od 0
[illegible] od 1

ZAD. 11 KAŻDY PUNKT PŁASZCZYZNY POMALOWANO NA JEDEN Z DWÓCH KOLORÓW: PISTACJOWY LUB MORELOWY. POKAŻ, ŻE NA TEJ PŁASZCZYŹNIE ISTNIEJE PROSTOKĄT O WIERZCHOŁKACH TEGO SAMEGO KOLORU.

Weźmy 3 proste równoległe i 8 prostopadłych do tych prostych



→ 8 kolumn możliwości
→ $2^3 = 8$

Z zasady szufladkowej istnieją dwie kolumny o tak samo pokolorowanych punktach.

Z tych dwóch kolumn weźmy po 2 punkty o tym samym kolorze i połączmy.