

### LISTA 13 ZAD 4

Wykonaj poniżej obliczenia modulo 3,5 oraz 15.  
 Obliczanie  $(82^1)$  oznacza element odwrotny do 82  
 mod 11 w odpowiadającym 2m.

$$\therefore -(125 \cdot 18 + 32 \cdot 48)^{-1} \cdot (75 \cdot 27 - 16 \cdot 7) + (77 \cdot 21 - 18 \cdot 255)j$$

$$\therefore 15^7 - 343^{12} \cdot 241^4 + 175 \cdot 12^3 - (176^{-1}) \cdot 111^2$$

$$2_3 = -(0+2)^{-1}(0-1) + (2 \cdot 1 - 0) = (-2)(-1) + 2 = 1$$

$$2_5 = -(0+3)^{-1}(0-2) + (2 \cdot 3 - 0) = (-2)(-1) + 1 = 0$$

$$2_{15} = -(0+8)^{-1}(0-7) + (2 \cdot 13 - 0) = (-2)(-1) + 11 = 10$$

$$2_3 = 0-1^{12} \cdot 1^4 + 0-2^1 \cdot 1^2 = -1 + (-1) = 1$$

$$2_5 = 0-3^{12} \cdot 1^4 + 0-(1^{-1})^4 \cdot 1^2 = -1 + (-1) = 3$$

$$2_{15} = 0-15^{12} \cdot 1^4 + 0-11^4 \cdot 1^2 = -1 + (-1) = 13$$

### LISTA 13 ZAD 5

Rozpatrz obliczanie algorytmu Euklidesa na dwóch kolejnych liczbach Fibonacciego. Jak wygląda poniżej obliczanie po tym kroku? Uzasadnij, że dla pary liczb  $(F_{n+1}, F_n)$  algorytm wykonyje (przyjmując n kroki).

Pokaż, że algorytm Euklidesa (w którym następujemy aż do momentu, gdy nie ma reszty 0-6) wykonyje  $O(\log(a) + \log(b))$  kroków.

Jedna iteracja algorytmu Euklidesa dla dwóch kolejnych liczb Fibonacciego  $(F_{n+1}, F_n)$  sumuje się do  $(F_n, F_{n-1})$ . Po k krokach  $(F_{n+1}, F_n)$  zmniejsza się kolejno na  $(F_{n+k}, F_{n-k})$ .

Dla liczb Fibonacciego algorytm działa obliczanie pary  $(F_1, F_2)$ , bo  $F_1 \bmod F_2 = 0$ , ale dla  $i \geq 3$   $F_i \bmod F_{i-1} \neq 0$ . Algorytm wykonyuje więc  $((n+2)^3) + 1 = m$  kroków.

Algorytm dla pary  $(x, y)$  dla  $y > x$  po jednym kroku schodzi dla pary  $(x, y')$ , gdzie  $y' \leq y/2$ ,  $y' < x$ , bo:

$$1) \text{ jeśli } x \leq y/2 \text{ to } y' = (y \bmod x) < y/2$$

$$2) \text{ jeśli } x > y/2 \text{ to } y' = (y \bmod x) = y - x < y/2$$

Jeśli jednak z dwóch w pary  $(x, y)$  jest mniejsza lub równa zero to algorytm kończy działanie po maksymalnie jednym kroku.

Algorytm wykonyuje więc maksymalnie  $\lceil \log_2 7 + \lceil \log_2 6 \rceil \rceil + 1 = 10(\log(6) + \log(5))$  kroków.

### LISTA 13 ZAD 8

Oblicz mwd dla następujących par liczb. Przedstawie je jako kombinacje linowe (o współczynnikach całkowitych) tych liczb

$$f743, 342 \}, f3812, 71 \}, f1234, 321 \}$$

LEMAT 8.15 W moim algorytmie Euklidesa mówimy, że obliczane liczby przedstawiać jako kombinacje liniowe a oraz b.

LEMAT 8.16 Dla  $a, b \in \mathbb{Z}^+$  istnieje  $x, y \in \mathbb{Z}$ , takie że  $\text{mwd}(a, b) = x \cdot a + y \cdot b$ . Jakoś otoż jedno z tych liczb jest dodatnie i jedno nieodolotne. Wówczas liczby te można wybrać tak, że  $|x| \leq b$ ,  $|y| \leq a$ , jeśli  $\text{mwd}(a, b) = 1$  to są dodatnie dla taki wyrażenia (w jednym x jest dodatnie a w drugim ujemne).

$$1) \cdot f743, 342 \}$$

$$\begin{aligned} 743 &= 2 \cdot 342 + 59 \\ 342 &= 5 \cdot 59 + 47 \end{aligned}$$

$$59 = 1 \cdot 47 + 12$$

$$47 = 3 \cdot 12 + 11$$

$$12 = 1 \cdot 11 + 1$$

$$\underline{\text{NWD}(743, 342) = 1}$$

$$\begin{aligned} 1 &= 12 - 1 \cdot 11 = 12 - (47 - 3 \cdot 12) = -47 + 4 \cdot 12 = -47 + 4(59 - 47) \\ &= 4 \cdot 59 - 5 \cdot 47 - 4 \cdot 59 - 5 \cdot (342 - 5 \cdot 59) = -5 \cdot 342 + 28 \cdot 59 = \\ &= -5 \cdot 342 + 28 \cdot (743 - 2 \cdot 342) = \underline{28 \cdot 743 - 63 \cdot 342} \end{aligned}$$

$$2) \{ 3812, 71 \}$$

$$3812 = 53 \cdot 71 + 49$$

$$71 = 1 \cdot 49 + 22$$

$$49 = 2 \cdot 22 + 5$$

$$22 = 4 \cdot 5 + 2$$

$$5 = 2 \cdot 1 + 1$$

$$\underline{\text{NWD}(3812, 71) = 1}$$

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (22 - 5 \cdot 5) = -2 \cdot 22 + 9 \cdot 5 = -2 \cdot 22 + 9(49 - 2 \cdot 22) = \\ &= 9 \cdot 49 - 20 \cdot 22 - 9 \cdot 49 - 20 \cdot (71 - 49) = -20 \cdot 71 + 2 \cdot 49 = \\ &= -20 \cdot 71 + 28 \cdot (3812 - 53 \cdot 71) = \underline{28 \cdot 3812 - 1557 \cdot 71} \end{aligned}$$

$$3) \{ 1234, 321 \}$$

$$1234 = 3 \cdot 321 + 271$$

$$321 = 1 \cdot 271 + 50$$

$$271 = 5 \cdot 50 + 21$$

$$50 = 2 \cdot 21 + 8$$

$$21 = 2 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$\underline{\text{NWD}(1234, 321) = 1}$$

$$\begin{aligned} 1 &= 3 \cdot 2 = 3 - (5 - 3) = -5 + 2 \cdot (5 - 3) = 2 \cdot 8 - 3 \cdot 5 = \\ &= 2 \cdot 8 - 3(21 - 2 \cdot 8) = -3 \cdot 21 + 8 \cdot 8 = -3 \cdot 21 - 8(50 - 2 \cdot 21) = \\ &= 8 \cdot 50 - 18 \cdot 21 = 8 \cdot 50 - 18(271 - 5 \cdot 50) = -18 \cdot 271 + 103 \cdot 50 = \\ &= -18 \cdot 271 + 103(1234 - 3 \cdot 321) = 103 \cdot 321 - 122 \cdot 271 = \\ &= 103 \cdot 321 - 122(1234 - 3 \cdot 321) = \underline{-122 \cdot 1234 + 469 \cdot 321} \end{aligned}$$

### LISTA 13 ZAD 10

Oblicz φ dla następujących liczb: 7, 8, 27, 77, 163, 105.

w tym zadaniu wykorzystam wzór, o którym mowało się w zad. 8 czyli  $\varphi(p) = p^e - p^{e-1}$  dla  $p$  pierwszego o dodatniego.

$$a) \varphi(7) = \varphi(7^1) = 7^1 - 7^0 = 6$$

$$b) \varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 6$$

$$c) \varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 18$$

Skorzystam też z tego, że  $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$  dla  $n, m$  względnie niewspół-

$$a) \varphi(77) = \varphi(7) \cdot \varphi(11) = 6(11-1) = 60$$

$$e) \varphi(143) = \varphi(13 \cdot 11) = \varphi(13) \cdot \varphi(11) = (13-1) \cdot 10 = 120$$

$$f) \varphi(105) = \varphi(7) \cdot \varphi(15) = 6 \cdot \varphi(5) \cdot \varphi(3) = 6 \cdot (5-1)(3-1) = 48$$

### USTA 13 ZAD 11

Podaj dwojne rozwiążanie w liczbach naturalnych parzystych układów równań.

$$a) \begin{cases} x \bmod 7 = 1 \\ x \bmod 5 = 4 \end{cases} \quad b) \begin{cases} x \bmod 9 = 8 \\ x \bmod 11 = 3 \end{cases} \quad c) \begin{cases} x \bmod 13 = 3 \\ x \bmod 17 = 11 \end{cases}$$

$$x \in \mathbb{N}$$

$$a) \begin{cases} x = 7 \cdot z + 1 \\ x = 5 \cdot l + 4 \end{cases}, \begin{cases} z \in \mathbb{Z} \\ l \in \mathbb{Z} \end{cases}$$

$$7z + 1 = 5l + 4$$

$$7z - 5l = 3$$

$$z=4, l=5, \text{ wtedy } 7z - 5l = 7 \cdot 4 - 5 \cdot 5 = 3$$

$$\text{więc } x = 7 \cdot \underline{z} + 1 = 28 + 1 = 29$$

b) strong method

```
(define (find-solution-ext1-b)
  (define (iter x)
    (if (and (= (modulo x 9) 8)
              (= (modulo x 11) 3))
        x
        (iter (+ 1 x)))))
```

wyszło  $x = 80 \Rightarrow$  sprawdzamy

$$\begin{aligned} 80 \bmod 9 &= 8 \\ 80 \bmod 11 &= 3 \end{aligned}$$

c) ANALOGICZNIE

$$x = 188$$