

① Demonstrați că

$$\left. \begin{aligned} &\text{dacă } n = \prod_{i=1}^k p_i^{\alpha_i}, \\ &\forall p_i, \quad a^{p_i} \equiv a \pmod{p_i} \end{aligned} \right\} \Rightarrow a^n \equiv a \pmod{n}$$

Mine 1h. a lui Fermat:

$$\forall a \in \mathbb{Z}, \quad p = \text{prim}, \quad (a \text{ nedivizibil cu } p) \\ a^{p-1} \equiv 1 \pmod{p} \Rightarrow \boxed{a^p \equiv a \pmod{p}}$$

Se  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ , at.

$$a^{p_i} \equiv a \pmod{p_i} \Rightarrow a^n \equiv a \pmod{p_i^{\alpha_i}}$$

Leza chineză a resturilor:

Se  $n = \prod_{i=1}^k p_i^{\alpha_i}$ , cu  $p_i \in \mathbb{Z}_+^*$  și  $p_i = \text{prim}$   
 $p_i \neq p_j, \quad i \neq j$

at.

$$\begin{cases} x \equiv a \pmod{p_1^{\alpha_1}} \\ x \equiv a \pmod{p_2^{\alpha_2}} \\ \vdots \\ x \equiv a \pmod{p_k^{\alpha_k}} \end{cases} \quad \text{are sol. unică.}$$

~~pp. 11 și 12~~ ~~12 și 13~~ ~~13 și 14~~ ~~14 și 15~~ ~~15 și 16~~ ~~16 și 17~~ ~~17 și 18~~ ~~18 și 19~~ ~~19 și 20~~ ~~20 și 21~~ ~~21 și 22~~ ~~22 și 23~~ ~~23 și 24~~ ~~24 și 25~~ ~~25 și 26~~ ~~26 și 27~~ ~~27 și 28~~ ~~28 și 29~~ ~~29 și 30~~ ~~30 și 31~~ ~~31 și 32~~ ~~32 și 33~~ ~~33 și 34~~ ~~34 și 35~~ ~~35 și 36~~ ~~36 și 37~~ ~~37 și 38~~ ~~38 și 39~~ ~~39 și 40~~ ~~40 și 41~~ ~~41 și 42~~ ~~42 și 43~~ ~~43 și 44~~ ~~44 și 45~~ ~~45 și 46~~ ~~46 și 47~~ ~~47 și 48~~ ~~48 și 49~~ ~~49 și 50~~ ~~50 și 51~~ ~~51 și 52~~ ~~52 și 53~~ ~~53 și 54~~ ~~54 și 55~~ ~~55 și 56~~ ~~56 și 57~~ ~~57 și 58~~ ~~58 și 59~~ ~~59 și 60~~ ~~60 și 61~~ ~~61 și 62~~ ~~62 și 63~~ ~~63 și 64~~ ~~64 și 65~~ ~~65 și 66~~ ~~66 și 67~~ ~~67 și 68~~ ~~68 și 69~~ ~~69 și 70~~ ~~70 și 71~~ ~~71 și 72~~ ~~72 și 73~~ ~~73 și 74~~ ~~74 și 75~~ ~~75 și 76~~ ~~76 și 77~~ ~~77 și 78~~ ~~78 și 79~~ ~~79 și 80~~ ~~80 și 81~~ ~~81 și 82~~ ~~82 și 83~~ ~~83 și 84~~ ~~84 și 85~~ ~~85 și 86~~ ~~86 și 87~~ ~~87 și 88~~ ~~88 și 89~~ ~~89 și 90~~ ~~90 și 91~~ ~~91 și 92~~ ~~92 și 93~~ ~~93 și 94~~ ~~94 și 95~~ ~~95 și 96~~ ~~96 și 97~~ ~~97 și 98~~ ~~98 și 99~~ ~~99 și 100~~

Dem. că  $a^{p_i} \equiv a \pmod{p_i}$

$P(k): a^{p_i^k} \equiv a \pmod{p_i} \quad (A), \quad \forall k \geq 1$

Dem. că  $P(k+1): a^{p_i^{k+1}} \equiv a \pmod{p_i} \quad (A)$

$$a^{p_i^{k+1}} = a^{p_i \cdot p_i^k} = (a^{p_i^k})^{p_i}$$



$$(ip.) \left. \begin{aligned} p_i^k &\equiv a \pmod{p_i} \Rightarrow (a^{p_i^k})^{p_i} \equiv a^{p_i} \pmod{p_i} \\ a^{p_i} &\equiv a \pmod{p_i} \end{aligned} \right\} \Rightarrow$$

$$\Rightarrow a^{p_i^{k+1}} \equiv a \pmod{p_i} \quad \checkmark$$

$$\Rightarrow a^{p_i^{d_i}} \equiv a \pmod{p_i}$$

Aplicăm Lemma chineză a rest:

$$a^{p_i^{d_i}} \equiv a \pmod{p_i^{d_i}}, \quad \forall i$$

$$\Rightarrow a^n \equiv a \pmod{n} \quad \blacksquare$$

2) Folosind exercitiul anterior, arătați că următoarele numere sunt Carmichael:

pp.  $n = \text{prim}$ , al.  $\forall b \in \{1, 2, \dots, n-1\}$

$$b^n \equiv b \pmod{n} \Rightarrow n = \text{m. Carmichael}$$

• pl. 1828 —

$$1828 \div 8 = 228$$

$$\Rightarrow 1828 = 8 \cdot 13 \cdot 17$$

$$228 : 13 = 18$$

$$1828 - 1 = 1827$$

$$8 - 1 = 7 \Rightarrow 1827 \mid 7$$

$$13 - 1 = 12 \Rightarrow 1827 \mid 12$$

$$17 - 1 = 16 \Rightarrow 1827 \mid 16$$

$\Rightarrow 1828$  este m. Carmichael



$$\textcircled{1} \quad 10585 : 5 = 2117$$

$$2117 : 23 = 92$$

$$10585 = 5 \cdot 23 \cdot 92$$

$$10585 - 1 = 10584$$

$$5 - 1 = 4 : 10584$$

$$23 - 1 = 22 : 10584$$

~~$$92 - 1 = 91 : 10584$$~~

$\Rightarrow 10585$  este Carmichael

$$92 - 1 = 91 : 10584$$

$$\textcircled{2} \quad 45361 : 11 = 4123$$

$$4123 : 13 = 317$$

$$\Rightarrow 45361 = 11 \cdot 13 \cdot 317$$

$$317 : 17 = 19$$

$$45361 - 1 = 45360$$

$$11 - 1 = 10 : 45360$$

$$13 - 1 = 12 : 45360$$

$$17 - 1 = 16 : 45360$$

$$317 - 1 = 316 : 45360$$

$\Rightarrow 45361$  este Carmichael

$\textcircled{3}$  Arătați că dacă  $2^n - 1$  este prim, atunci  $n$  este prim.

R.A.  
Vom demonstra prin ~~inducție~~ afirmație

$$\text{d} \quad 2^n - 1 = \text{prim} \Rightarrow n = \text{compus}$$

$$n = \text{compus} \Rightarrow n = e \cdot b, \quad e, b \in (1, n)$$

$$\Rightarrow 2^n - 1 = 2^{eb} - 1$$

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

$$x = 2^e, \quad m = b$$

$$2^{eb} - 1 = (2^e)^b - 1 = (2^e - 1)((2^e)^{b-1} + (2^e)^{b-2} + \dots + 2^e + 1)$$



$$2^2 \Rightarrow 2^2 - 1 > 1$$

$$(2^2)^{b-1} + \dots + 2^2 + 1 > 1 \quad \text{pd. } b \geq 2$$

$\Rightarrow 2^n - 1$  este produs de 2 nr.  $> 1 \Rightarrow$  nu este prim

Deci în ipoteză,  $2^n - 1$  este prim

$\Rightarrow n$  nu poate fi compus

$\Rightarrow n = \text{prim}$

9 (14) Aplicați alg. lui Fermat pd. a  
de determinare primalității nr. 36891.

Fie  $n = \text{prim}$ . At.  $\forall b \in \{1, \dots, n-1\}$

$$b^{n-1} \equiv 1 \pmod{n} \quad (*)$$

Dacă găsim un  $b$  pd. care  $(*)$  nu este satisf.

at  $b \neq \text{prim}$ .

calculul sunt prea enervante,  
de aceea am făcut implementarea  
în Fermat Primality.cs.