Nr. 19 Tema 4 Bărbulescu Ionuț M533

5) 19) Care sunt factorii primi ai numărului 15569

$2 \nmid 15569$	$23 \nmid 15569$	$53 \nmid 15569$	$97 \nmid 15569$
$3 \nmid 15569$	$29 \nmid 15569$	$59 \nmid 15569$	$101 \nmid 15569$
$5 \nmid 15569$	$31 \nmid 15569$	$61 \nmid 15569$	$103 \nmid 15569$
$7 \nmid 15569$	$37 \nmid 15569$	$71 \nmid 15569$	$107 \nmid 15569$
$11 \nmid 15569$	$41 \nmid$ ~~379~~ 15569	$73 \nmid 15569$	$109 \nmid 15569$
$13 \nmid 15569$	$43 \nmid 15569$	$83 \nmid 15569$	$113 \nmid 15569$
$17 \nmid 15569$	$47 \nmid 15569$	$89 \nmid 15569$	$127 \nmid 15569$
$19 \nmid 15569$			$131 \nmid 15569$

Din $131 \cdot 131 = 17161 > 15569 \Rightarrow 15569$ este număr prim

$\Rightarrow$ Factorizarea în numere prime a nr. 15569 este: $15569 = 15569$

11) Realizați comparație între algoritmii de ~~factorizare~~ prezentați la seminar.

Algoritmul împărțirii succesive este un algoritm determinist neconditionat ce oferă descompunerea numărului în factori primi. Dacă este aplicat până la obținerea unui număr întreg prim se bazează pe faptul că un număr compus are un factor $\leq \sqrt{n}$, deci putem testa numerele prime până la $\sqrt{n}$ pentru a determina dacă n este compus. Dacă găsim ~~un număr~~ un factor putem aplica algoritmul lui $\frac{n}{p}$ (p factorul găsit anterior) până când nr. obținut în împărțire sau toți factorii găsiți nu sunt primi. Acest algoritm este exponențial fiind legat de nr. de nr. prime până la $\sqrt{n}$

Algoritmul lui Fermat este un algoritm probabilistic de testare a primalității care se bazează pe teorema lui Fermat, care spune că pentru n prim atunci $\forall\, b \in \{1, 2, \dots, n-1\}$

$b^{n-1} \equiv 1 \pmod{n}$ alternativ $b^{n} \equiv b \pmod{n}$.

Se alege martor $b \in \{1, 2, \dots, n-1\}$ și se testează dacă respectă condiția $b^{n-1} \equiv 1 \pmod{n}$. Dacă obținem că $b^{n-1} \equiv a \pmod{n}$ cu $a \neq 1$ atunci ~~algoritmul~~ n este număr compus. Dacă obținem $b^{n-1} \equiv 1 \pmod{n}$ testăm folosind un alt martor b. Există numere compuse pentru care $b^{n-1} \equiv 1 \pmod{n}$ are loc oricare ar fi $b \in \{0, 1, \dots, n-1\}$ deși numărul n este compus. Acestea s.n. numere Carmichael și sunt o infinitate de astfel de numere, ceea ce face testul incapabil a determina dacă un nr. e Carmichael sau nu.

Algoritmul Miller-Rabin

Folosim rezultatul $b^{n-1} \equiv 1 \pmod{n}$ și observăm că $n-1$ = par deci $n = 1 + 2^{r} t$ cu t impar, $r \in \mathbb{N}$

Dacă n e prim

$$b^{\frac{n-1}{2}} = b^{2^{r-1} t} \equiv a \Rightarrow a^{2} \equiv 1 \pmod{n} \Rightarrow a \in \{-1, 1\}$$

Își luăm un martor $b \in \{0, 1, \dots, n-1\}$ și îl descompunem pe $n-1$ sub forma $2^{r} t$, $r \in \mathbb{N}$, $t \in \mathbb{N}$ impar.

Calculăm b^{2t}, $b^{2^{2} t}$, $b^{2^{3} t}$, ..., $b^{2^{r-1} t}$, $b^{2^{r} t}$ și dacă obținem înainte de valoarea 1 a lui $b^{2^{r} t}$ o valoare diferită de $\{-1, 1\}$ ~~atunci înseamnă că~~ / valoarea a lui $b^{2^{r-1} t}$ atunci înseamnă că numărul n este compus, deci nu e nr. prim.