

## CÂTEVA REZULTATE DESPRE NUMERELE LUI FERMAT

CORNELIU M NESCU-AVRAM

*Lucrare prezentat la Sesiunea de comunicări metodice științifice a profesorilor de matematică din Prahova, ediția a XXXVI-a, Sinaia, 22 mai 2010*

*Because the  $F_m$  grow rapidly in size, a method which factors  $F_m$  may be inadequate for  $F_{m+1}$  ... Thus, the difficulty of completely factoring  $F_m$  by the fastest known method is not a monotonic function of  $m$ .*

Richard P. Brent

**Sumar.** Lucrarea prezintă unele metode de investigare a numerelor lui Fermat  $F_m = 2^{2^m} + 1$  și arată cum pot fi factorizate direct, folosind fracțiile continue sau polinoamele cu coeficienți întregi. Numerele  $F_5$  și  $F_6$  sunt studiate în detaliu.

### NUMERELE $F_5$ ȘI $F_6$

Numerele lui Fermat  $F_m$  sunt prime pentru  $0 \leq m \leq 4$ . Celelalte numere Fermat sunt compuse sau nu se cunoaște natura lor. Vom prezenta în continuare câte patru demonstrații ale faptului că numerele  $F_5$  și  $F_6$  sunt compuse. Fiecare demonstrație pune în lumină alte aspecte ale problemei.

Numărul  $F_5$ :

I. Sunt adevărate egalitățile  $641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4$ , deci  $2^{32} + 1 = 2^{28} \cdot 2^4 + 1 = (2^7)^4(2^7 \cdot 5 + 1 - 5^4) + 1 = (2^7 \cdot 5 + 1)[2^{28} - (2^7 \cdot 5 - 1)(2^{14} \cdot 5^2 + 1)]$ , adică  $F_5$  se divide cu 641.

II. Numărul  $F_5 = 2^{32} + 1 = (2^{16})^2 + 1^2 = 62264^2 + 20449^2$  admite două reprezentări diferite ca sumă de două pătrate. Se știe însă<sup>[14]</sup> că un număr congruent cu 1 modulo 4 este prim dacă și numai dacă admite o reprezentare unică sub forma unei sume de două pătrate de numere naturale, abstracte fiind când de ordinea termenilor. Rezultă că  $F_5$  este un număr compus. Folosind aceste reprezentări, se poate determina un factor, egal cu  $(62264 + 2^{24} \cdot 20449, F_5) = 641$ .

III. Dacă  $x = 2^4 + 2^3 + 1$ ,  $y = 2^2$ ,  $z = 2^{11} + 2^9 - 2^2$ ,  $w = 2^8 + 2^7 + 2^4 + 2^3 + 1$ , atunci  $xw - yz = 1$ ,  $xz + yw = 2^{16}$ , de unde  $(x^2 + y^2)(z^2 + w^2) = (xz + yw)^2 + (xw - yz)^2 = 2^{32} + 1$ , deci  $F_5$  este un număr compus.

IV. Fie  $f = X^{32} + 1$ ,  $g = X^9 + X^7 + 1$ . Din teorema împărțirii cu rest se obține  $f = gq + r$ , cu  $q \in \mathbb{Z}[X]$  și  $r = -9X^8 - 9X^7 + 5X^6 - 6X^4 + 2X^3 + 7X^2 - 5X - 7$ . Atunci  $r(2) = -5g(2)$ , deci  $2^{32} + 1 = f(2) = g(2)q(2) + r(2) = g(2)q(2) - 5g(2)$  se divide cu  $g(2) = 641$ .

Numărul  $F_6$ :

I. Este adevărat descompunerea  $2^{64} + 1 = (2^8a + 1)(2^8b + 1)$ , unde  $a = 1071$ ,  $b = 2^{56}c - 2^{48}a^7 + 2^{40}a^6 - 2^{32}a^5 + 2^{24}a^4 - 2^{16}a^3 + 2^8a^2 - a$ ,  $c = \frac{a^8 + 1}{2^8a + 1}$ . Vom arăta că numărul  $c$  este natural.

Într-adevăr, restul împărțirii polinomului  $f = [(X^3 - 1)(X^2 + 1)]^8 + 1$  la polinomul  $g = X^4(X^3 - 1)(X^2 + 1) + 1$  este  $r = 188X^8 - 153X^7 + 308X^6 - 437X^5 + 350X^4 - 466X^3 + 374X^2 - 298X + 239$ , iar  $f(4) = a^8 + 1$ ,  $g(4) = 2^8a + 1 = p$ ,  $r(4) = 39p$ , adică  $f(4)$  se divide cu  $p$ , deci numărul  $c$  este natural. Rezultă că numărul  $F_6$  este compus.

II. Numărul  $F_6 = 2^{64} + 1 = (2^{32})^2 + 1^2 = 4046803256^2 + 1438793759^2$  admite două reprezentări ca sumă de două pătrate de numere naturale, deci nu este un număr prim. Un factor al lui  $F_6$  este  $p = 2^8 \cdot 1071 + 1 = (4046803256 + 2^{25} \cdot 1438793759, F_6)$ .

III. Dacă  $x = 2^9 + 2^2$ ,  $y = 2^6 + 2^4 + 2^3 + 1$ ,  $u = 2^8 - 2^3 + 1$ ,  $v = 2^{11} + 2^7 + 2^2$ , atunci  $-xu + yv = 2^{16}$ ,  $xv + yu = 1071^2$ ,  $x^2 + y^2 = 2^8 \cdot 1071 + 1 = p$  și  $2^{32} + 1071^4 = (-xu + yv)^2 + (xv + yu)^2 = (x^2 + y^2)(u^2 + v^2)$ , de unde  $1071^4 \equiv -2^{32} \pmod{p}$ . Dar  $2^8 \cdot 1071 \equiv -1 \pmod{p}$ , deci  $2^{32} \cdot 1071^4 \equiv 1 \pmod{p}$ , de unde  $2^{32} \cdot (-2^{32}) \equiv -2^{64} \equiv 1 \pmod{p}$ .

IV. Fie  $f = X^{32} + 1$ ,  $g = X^9 + X^7 - X^6 - X^4 + 1$ , atunci  $f = gq + r$ , unde  $q \in \mathbb{Z}[X]$  și  $r = -7X^8 + 12X^7 - 3X^6 + X^5 - 4X^4 + 5X^3 - 3X^2 - 6X + 7$ . Rezultă  $r(4) = -g(4)$ , deci  $2^{64} + 1 = f(4) = g(4)q(4) + r(4) = g(4)q(4) - g(4)$  se divide cu  $g(4) = 274177$ .

Vom arăta în continuare că aceste procedee pot fi generalizate, dacă se cunoaște un factor prim al numărului  $F_m$ ,  $m$  oarecare.

#### METODA POLINOMIAL

Această metodă este sugerată de a patra demonstrație, dar procedeul a fost folosit și la prima demonstrație a faptului că  $F_6$  este compus.

Fie  $p = 2^n k + 1$  un număr prim impar oarecare,  $n, k \in \mathbb{N}^*$ ,  $k$  impar. Este evident că orice număr prim admite o astfel de reprezentare. Se știe [14] că dacă  $p$  este divizor al lui  $F_m$ , atunci

$n \geq m + 2$  (teorema lui *Lucas*). Deducem că  $p$  admite reprezentarea  $p = 2^{n_1} + 2^{n_2} + \dots + 2^{n_t} + 1$ , unde  $n_1, n_2, \dots, n_t \in \mathbb{N}$ ,  $n_1 > n_2 > \dots > n_t \geq m + 2$ .

**Teorema 1.** Fie  $f, g \in \mathbb{Z}[X]$ ,  $f = X^{2^m} + 1$ ,  $g = X^{n_1} + X^{n_2} + \dots + X^{n_t} + 1$  și  $r \in \mathbb{Z}[X]$  restul împărțirii lui  $f$  la  $g$ . Atunci  $F_m$  se divide cu  $p$  dacă și numai dacă  $r(2)$  se divide cu  $p$ .

DEMONSTRAȚIE: Din teorema împărțirii cu rest în  $\mathbb{Z}[X]$  obținem  $f = gq + r$ , unde  $q \in \mathbb{Z}[X]$ , deoarece coeficientul termenului de grad maxim al lui  $g$  este egal cu 1. Rezultă  $f(2) = g(2)q(2) + r(2)$ . Dar  $f(2) = F_m$ ,  $g(2) = p$ , deci  $F_m \equiv r(2) \pmod{p}$ .

EXEMPLE. 1. Fie  $f = X^{128} + 1$ ,  $g = X^{55} + X^{54} + X^{52} + X^{50} - X^{45} + X^{43} + X^{41} + X^{40} - X^{34} + X^{30} - X^{27} + X^{25} + X^{24} - X^{20} + X^{16} + X^{14} + X^{10} + X^9 + 1$ ,  $p = 2^9 \cdot 116503103764643 + 1$ . Pe această cale nu putem obține un rezultat concludent, deoarece numerele care intervin sunt prea mari.

2. Fie  $f = X^{32} + 1$ ,  $g = X^4 + 3X + 1$ ,  $p = 2^7 \cdot 5 + 1$ . Atunci  $g(5) = p$  și  $\bar{r} = -300X^3 - 12X^2 + 217X + 178$ , unde  $\bar{r}$  se obține prin reducerea modulo  $p$  a coeficienților lui  $r$ , deci  $\bar{r}(5) \equiv 0 \pmod{p}$ . Dar  $5^{32} - 2^{32}$  se divide cu  $5^4 + 2^4 = p$ , deci  $F_5 \equiv f(5) \equiv 0 \pmod{p}$ .

3. Fie  $f = X^8 + 1$ ,  $g = X^2 - 47X + 4$ ,  $p = 2^8 \cdot 1071 + 1$ . Atunci  $g(1071) = 4p$ ,  $\bar{r} = -71294X + 134668$ , deci  $f(1071) \equiv \bar{r}(1071) \equiv 0 \pmod{p}$ . Am văzut însă că de aici se obține  $F_6 \equiv 0 \pmod{p}$ .

4. Fie  $f = X^{32} + 1$ ,  $g = X^4 + 11X^3 - 5X^2 + 9X + 1$ ,  $p = 2^{16} \cdot 37 + 1$ . Atunci  $g(37) = p$ ,  $\bar{r} = -164013X^3 - 300182X^2 - 1041991X + 1181351$ , deci  $f(37) \equiv \bar{r}(37) \equiv 0 \pmod{p}$ . Vom vedea în paragraful următor că de aici rezultă  $F_9 \equiv 0 \pmod{p}$ .

5. Fie  $f = 4X^{170} + 1$ ,  $g = X^7 + X^6 + 2X^5 + 1$ ,  $p = 2^{16} \cdot 37 + 1$ . Atunci  $f(8) = F_9$ ,  $g(8) = p$ . Metoda nu este eficientă nici în acest caz.

#### DESCOMPUNEREA DIRECTĂ

Prima demonstrație a faptului că numărul  $F_6$  este compus poate fi extinsă la un cadru mai general.

**Teorema 2.** Fie  $p = 2^n a + 1$  un număr prim,  $n, a \in \mathbb{N}^*$ ,  $a$  impar și  $n = 2^s$ ,  $s \in \mathbb{N}$ . Atunci  $F_m$  se divide cu  $p$  dacă și numai dacă  $F_{m-s}(a) = a^{2^{m-s}} + 1$  se divide cu  $p$ .

DEMONSTRAȚIE: Presupunem că  $F_m$  se divide cu  $p$ . Din  $2^n a = 2^{2^s} a \equiv -1 \pmod{p}$  rezultă, prin ridicare la puterea  $2^{m-s}$

$$(F_m - 1) a^{2^{m-s}} \equiv 1 \pmod{p},$$

deci  $F_{m-s}(a) = a^{2^{m-s}} + 1 \equiv 0 \pmod{p}$ .

Dacă  $F_{m-s}(a)$  se divide cu  $p$ , atunci  $a^{2^{m-s}} \equiv -1 \pmod{p}$ . Din  $2^{2^s} a \equiv -1 \pmod{p}$  se obține

$$1 \equiv (2^{2^s} a)^{2^{m-s}} \equiv 2^{2^m} \cdot (-1) \equiv -F_m + 1 \pmod{p},$$

deci  $F_m$  se divide cu  $p$ .

EXEMPLUL 6. Dacă  $m = 9, n = 16, a = 37$ , atunci  $s = 4$  și  $F_9$  se divide cu  $p = 2^{16} \cdot 37 + 1$  dacă și numai dacă  $F_5(37) = 37^{32} + 1$  se divide cu  $p$ .

Acest fapt explică de ce unii divizori primi ai numerelor lui *Fermat* sunt și divizori ai unor numere *Fermat* generalizate. Avem, de exemplu, următoarea

**Teorema 3.** Dacă  $a, b \in \mathbb{N}$  și  $a + b$  este impar, atunci  $F_5(2^a 5^b) = (2^a 5^b)^{32} + 1$  se divide cu 641.

DEMONSTRAȚIE: Am văzut că  $2^{32} \equiv 5^{32} \equiv -1 \pmod{641}$ , deci  $F_5(2^a 5^b) \equiv (-1)^a (-1)^b + 1 \equiv 0 \pmod{641}$ .

#### METODA FRACȚIILOR CONTINUE

O demonstrație simplă a faptului că numărul  $F_6$  este compus este dată de F. Dyson<sup>[12]</sup>, folosind argumente similare cu cele din prima demonstrație pentru  $F_5$ . Dacă

$$p = 1 + 2^8 f \quad \text{și} \quad f = (2^6 - 1)(2^4 + 1), \tag{1}$$

atunci

$$2^{24} - 1 = fg, \quad \text{unde} \quad g = (2^6 + 1)(2^8 - 2^4 + 1). \tag{2}$$

Cu o factorizare de forma

$$2^{64} + 1 = (x^2 + y^2)(z^2 + w^2), \quad 2^{32} - i = (x + iy)(z - iw), \tag{3}$$

condiții care sunt îndeplinite dacă

$$xz + yw = 2^{32}, \quad xw - yz = 1, \quad x^2 + y^2 = p. \tag{4}$$

Pentru  $z = gx, w = gy$ , obținem în (3)  $(x + iy)g(x - iy) = gp$  și  $gp = 2^{32} + a$  este apropiat de  $2^{32}$ , cu diferența  $a = g - 2^8 = 15409$  calculat din (1) și (2). Rezultă că rapoartele  $\frac{z}{x}$  și  $\frac{w}{y}$  sunt apropiate de  $g$ , deci putem încerca

$$z = gx - s, \quad w = gy - t, \tag{5}$$

cu  $s, t$  numere întregi relativ mici. Atunci (3) are loc numai dac

$$x^2 + y^2 = p, \quad xs + yt = a, \quad ys - xt = 1. \tag{6}$$

Din (6) rezult

$$a^2 + 1 = pu, \quad u = s^2 + t^2. \tag{7}$$

Cum întregii  $p$  și  $a$  sunt cunoscute și relativ mici, putem găsi prin încercări soluția pentru (6) și (7), anume  $x = 516, y = 89, s = 29, t = 5, u = 866$ . Soluția pentru (6) și (7), cu  $z$  și  $w$  dați de (5) furnizează soluția pentru (3). Factorizarea (2) pentru  $2^{24} - 1$  ne conduce direct la factorizarea (3) a numărului  $F_6 = 2^{64} + 1$ .

Sistemul de ecuații (6) și (7) poate fi rezolvat folosind o teoremă a lui Serret<sup>[12]</sup> despre fracțiile continue. Fie  $p$  și  $a$  două numere întregi prime între ele,  $0 < a < p$ . Frația ordinară  $\frac{p}{a}$  poate fi reprezentată ca o fracție continuă cu cânturile pariale  $(a_j, j = 1, \dots, n)$  în exact două moduri, cu  $n$  par sau impar. Într-o reprezentare, ultimele două cânturi sunt  $[c, 1]$ , cu  $c$  număr natural. În cealaltă reprezentare, ultimele două cânturi sunt înlocuite de un singur cânt, anume  $[c + 1]$ , celelalte cânturi rămân neschimbate. Frația continuă cu  $n$  cânturi corespunde toare fracției ordinare  $\frac{p}{a}$  se numește *palindromic* dac  $a_j = a_{n+1-j}, j = 1, \dots, n$ .

**Teorema 4 (Serret).** Frația continuă cu  $n$  cânturi pariale corespunde toare fracției ordinare  $\frac{p}{a}$  este palindromic dac și numai dac există un întreg  $u$  astfel încât  $pu = a^2 + (-1)^n$ .

Pentru demonstrație se poate consulta<sup>[12]</sup>.

Fie  $A$  o mulțime ordonată de numere naturale nenule și  $S(A)$  numărul fracțiilor continue ale  $c$  rei cânturi pariale sunt elementele lui  $A$ . De exemplu,  $S(\emptyset) = 1, S(a) = a, S(a, b) = 1 + ab, S(a, b, c) = a + c + abc$ , etc. Dac  $p$  este un număr prim care divide numărul  $a^2 + 1$ , unde  $0 < a < p$  și  $a \equiv 2^{2^{m-1}} \pmod{p}, m \in \mathbb{N}^*$ , atunci  $a^2 + 1 \equiv F_m \equiv 0 \pmod{p}$ , deci  $p$  este divizor al numărului *Fermat*  $F_m$ . Conform teoremei lui Serret, fracția continuă corespunde toare fracției ordinare  $\frac{p}{a}$  este palindromic

$$\frac{p}{a} = [a_1, \dots, a_k, a_k, \dots, a_1]$$

și soluția sistemului (6) este<sup>[12]</sup>

$$\begin{aligned}
 p &= S(a_1, \dots, a_k, a_k, \dots, a_1), & a &= S(a_2, \dots, a_k, a_k, \dots, a_1), \\
 x &= S(a_1, \dots, a_k), & y &= S(a_1, \dots, a_{k-1}), \\
 s &= S(a_2, \dots, a_k), & t &= S(a_2, \dots, a_{k-1}).
 \end{aligned} \tag{8}$$

EXEMPLE. 7. Dacă  $m = 5, p = 641, a = 154$ , atunci  $154 \equiv 2^{16} \pmod{641}$  și  $154^2 + 1 = 37 \cdot 641$ , deci  $F_5 = 2^{32} + 1$  se divide cu 641. Avem

$$\frac{641}{154} = 4 + \frac{1}{6 + \frac{1}{6 + \frac{1}{4}}} = [4, 6, 6, 4], \text{ deci } p = S(4, 6, 6, 4) = 641, a = S(6, 6, 4) = 154,$$

$$x = S(4, 6) = 25, y = S(4) = 4, s = S(6) = 6, t = S(\emptyset) = 1.$$

8. Dacă  $m = 6, p = 274177, a = 15409$ , atunci  $15409 \equiv 2^{32} \pmod{274177}$  și  $15409^2 + 1 = 866 \cdot 274177$ , deci  $F_6 = 2^{64} + 1$  se divide cu 274177. Avem

$$\begin{aligned}
 \frac{274177}{15409} &= [17, 1, 3, 1, 5, 5, 1, 3, 1, 17], \text{ deci } p = S(17, 1, 3, 1, 5, 5, 1, 3, 1, 17) = 274177, a = \\
 &= S(1, 3, 1, 5, 5, 1, 3, 1, 17) = 15409, x = S(17, 1, 3, 1, 5) = 516, y = S(17, 1, 3, 1) = 89, s = S(1, 3, 1, 5) = 29, \\
 &t = S(1, 3, 1) = 5.
 \end{aligned}$$

F. Dyson <sup>[12]</sup> observă că pentru  $m = 5$  toate câturile pariale sunt numere pare, pe când pentru  $m = 6$  toate câturile pariale sunt impare și pune întrebarea dacă există o regulă generală sau acest fapt este întâmplător. După cum se constată din calculele prezentate în Anexă, al doilea răspuns este cel corect.

#### CUM GĂSIM UN FACTOR PRIM?

Orice număr prim impar  $p$  poate fi reprezentat în mod unic sub forma  $p = 2^n k + 1, n, k \in \mathbb{N}^*, k$  impar. Dacă  $p$  este un divizor al lui  $F_m$ , atunci  $n \geq m + 2$  (Lucas, <sup>[14]</sup>). Să arătăm cum poate fi găsit divizorul 641 al lui  $F_5$ . Un divizor oarecare al lui  $F_5$  este de forma  $128k + 1$ . Avem  $128 \cdot 1 + 1$  se divide cu 3,  $128 \cdot 2 + 1 = 257 = F_3$ , se vede însă <sup>[14]</sup> că numerele lui *Fermat* sunt prime între ele, deci  $F_3$  nu este divizor al lui  $F_5$ ,  $128 \cdot 3 + 1$  se divide cu 5,  $128 \cdot 4 + 1$  se divide cu 3. Rezultă că primul candidat este  $128 \cdot 5 + 1 = 641$  și am văzut că acest număr prim este într-adevăr divizor al lui  $F_5$ .

Investigarea numerelor *Fermat* mai mari se face cu ajutorul calculatorului (a se vedea bibliografia). S-au obținut rezultate practice spectaculoase, dar ele nu au fost încă incluse într-o teorie. Se pot da însă condiții necesare pe care trebuie să le satisfacă divizorii numerelor lui *Fermat*.

**Teorema 5.** Dacă  $m = 4t + 1$ ,  $t \in \mathbb{N}^*$  și  $p = 2^{m+2}k + 1$  este un divizor prim al lui  $F_m$ , atunci  $k \geq 5$ .

DEMONSTRARE : Avem

$$2^{4t+3} + 1 = (15 + 1)^t \cdot (9 - 1) + 1 \equiv -1 + 1 \equiv 0 \pmod{3},$$

$2^{4t+3} \cdot 2 + 1 = 2^{4t+4} + 1$  este prim numai dacă este număr *Fermat*, dar în acest caz el nu este divizor al lui  $F_m$ , deoarece numerele *Fermat* sunt prime între ele,

$$2^{4t+3} \cdot 3 + 1 = (15 + 1)^t \cdot (5 + 3) \cdot 3 + 1 \equiv 3 \cdot 3 + 1 \equiv 0 \pmod{5},$$

$$2^{4t+3} \cdot 4 + 1 = 2^{4t+5} + 1 = (15 + 1)^t \cdot (33 - 1) + 1 \equiv -1 + 1 \equiv 0 \pmod{3}.$$

Evident, de aici se obține  $k \geq 5$ .

Există numeroase exemple de divizori  $p = 2^n \cdot 5 + 1$  ai numerelor lui *Fermat*  $F_m$ , cu  $n - m = 2$ , dar și exemple în care  $n - m > 2$ . Teorema precedentă poate fi formulată mai general astfel :

Dacă  $p = 2^n k + 1$  este un divizor prim al lui  $F_m$  și  $n \equiv 3 \pmod{4}$ , atunci  $k \geq 5$ .

*Note.* Descompunerea în factori a numerelor lui *Fermat* începe cu *Leonhard Euler* ( $F_5$ , 1732) și continuă până astăzi <sup>[14],[15]</sup>.

O alternativă de calcul a lui  $a$  din (7) este  $a \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$ . Pentru conversia fracțiilor ordinare în fracții continue am folosit calculatorul lui *Dario Alpern* <sup>[16]</sup>.

#### ANEX

Tabelul conține cel mai mic divizor prim  $p$  al numărului  $F_m$ ,  $5 \leq m \leq 23$ ,  $a \equiv 2^{2^{m-1}} \pmod{p}$  și soluția  $x$  a sistemului de ecuații  $x^2 + y^2 = p$ ,  $xs + yt = a$ ,  $ys - xt = 1$ . Valorile  $p$ ,  $a$ ,  $y$ ,  $s$ ,  $t$  se obțin din egalitățile (8).

$m$	$p$	$x$
5	$2^7 \cdot 5 + 1$	$S(4,6)$

6	$2^8 \cdot 1071 + 1$	$S(17,1,3,1,5)$
7	$2^9 \cdot 116503103764643 + 1$	$S(309,3,1,33,1,1,3,4,1,2,2,1,3,3,1,1,6,4,1,1,1,1)$
8	$2^{11} \cdot 604944512477 + 1$	$S(2,3,4,6,13,2,27,9,19,1)$
9	$2^{16} \cdot 37 + 1$	$S(2,6,1,1,4,12)$
10	$2^{12} \cdot 11131 + 1$	$S(11,2,4,1,2,1,3,1,2)$
11	$2^{13} \cdot 39 + 1$	$S(5,1,1,3,4,3)$
12	$2^{14} \cdot 7 + 1$	$S(2,21,5,1)$
13	$2^{16} \cdot 41365885 + 1$	$S(1,3,3,3,4,1,3,7,1,2,1,1,14,1,1)$
14	$2^{16} \cdot 178 \dots 717 + 1$ <sup>[15]</sup>	$S(?)$
15	$2^{21} \cdot 579 + 1$	$S(2,10,1,1,1,6,1,1,1,23)$
16	$2^{19} \cdot 1575 + 1$	$S(2,1,1,10,2,1,10,11,1)$
17	$2^{19} \cdot 59251857 + 1$	$S(2,2,4,1,8,1,70,1,3,4,17)$
18	$2^{20} \cdot 13 + 1$	$S(8,2,1,147)$
19	$2^{21} \cdot 33629 + 1$	$S(1,4,1,1,1,2,1,2,5,1,1,4,2,1,3,2)$
20	e compus, dar nu se cunoaște niciun factor prim <sup>[15]</sup>	
21	$2^{23} \cdot 534689 + 1$	$S(1,11,11,11,1,1,2,25,1,2,3)$
22	$2^{24} \cdot 385 \dots 211 + 1$ <sup>[15]</sup>	$S(?)$
23	$2^{25} \cdot 5 + 1$	$S(2,1,1,3,98,1,1,3)$

## Bibliografie

[1] Kraitchik, M., *Théorie des nombres*, vol. 2, Gauthier-Villars, Paris, 1926.

[2] Hardy, G. H., Wright, E. M., *An introduction to the theory of numbers*, Clarendon Press, Oxford, 1945, 1954, 1960, 1979, MR 16,673c, MR 81i:10002.

- [3] Robinson, R. M., *Factors of Fermat numbers*, Math. Tables Aids Comput. **11** (1957a), 21-23, MR 19,14d.
- [4] Sierpiński, W., *Ce timp i ce nu timp despre numerele prime*, Editura tiinific , Bucure ti, 1966.
- [5] Chandrasekharan, K., *Introduction to analytic number theory*, Springer-Verlag, Berlin Heidelberg New York, 1968.
- [6] Rouse Ball, W. W., Coxeter, H. S. M., *Mathematical recreations and essays*, Twelfth Edition, University of Toronto Press, 1974.
- [7] Brent, R. P., Pollard, J. M., *Factorization of the eighth Fermat number*, Math. Comp. **36** (1988), 627-630, MR 83h:10014.
- [8] Sierpiński, W., *Elementary theory of numbers*, 2<sup>nd</sup> Engl. ed. revised and enlarged by A. Schinzel, Pa stwowe Wydaw. Naukowe, Warszawa, 1988, MR 89f:11003.
- [9] Brent, R. P., *Factorization of the eleventh Fermat number*, Abstracts. Amer. Math. Soc. **10** (1989), 176-177.
- [10] Williams, H. C., *How was  $F_6$  factored?*, Math. Comp. **61** (1993), 463-474, MR 93k:01046.
- [11] Brent, R. P., *Factorization of the tenth Fermat number*, Math. Comp. **68** (1999), 429-451, MR 99e:11154.
- [12] Dyson, F., *The sixth Fermat number and palindromic continued fractions*, Enseign. Math. (2) **46** (2000), 385-389.
- [13] Brent, R. P., Crandall, R. E., Dilcher, K., Van Halewyn, C., *Three new factors of Fermat numbers*, Math. Comp. **69** (2000), 1297-1304, MR 2000j:11194.
- [14] Křížek, M., Luca, F., Somer, L., *17 Lectures on Fermat Numbers*, Springer-Verlag, 2001.
- [15] Keller, Wilfrid, *Prime Factors of Fermat Numbers*, ProthSearch.net.
- [16] Alpern, D., *Continued Fractions Calculator*, [www.alpertron.com.ar](http://www.alpertron.com.ar).