Kelkaj rimarkoj pri la nombroj de Fermat

Jan Górowski, Adam Łomnicki*

En la artikolo troviĝas kelkaj konataj teoremoj pri la nombroj de Fermat kaj la teoremo de Gauss pri la klasika geometria konstruo de la regula n-latero. Plue la autoroj donas originalajn pruvojn de la malprimeco de la nombroj – sesa kaj sepa – de Fermat, de la malkompono en primojn de tiuj nombroj. Tiuj pruvoj baziĝas sur elementa matematiko kaj povas esti interesaj eĉ por mezlernejanoj kaj studentoj de matematiko.

Kapvortoj: *Fermat, nombroj de Fermat, Gauss, matematikaj pruvoj*

1 Enkonduko

La nombrojn $F_n = 2^{2^n} + 1$, kie $n \in \mathbb{N}$ oni nomas *la nombroj de Fermat* (P. Fermat 1601-1665). Kompreneble $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$, $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = (2^{16})^2 + 1 = 65\,536^2 + 1 = 4\,294\,967\,297$, $F_6 = 2^{2^6} + 1 = (2^{32})^2 + 1 = 4\,294\,967\,296^2 + 1$.

Evidente F_0, F_1, F_2, F_3, F_4 estas primaj. En matematika literaturo, speciale en tiu ligita kun historiaj esploroj kaj didaktikaj proponoj, oni ripetas la supozon, ke Fermat estis konvinkita, ke la nombroj F_n por ĉiu $n \in \mathbb{N}$ estas primaj.

La nombroj de Fermat trovis gravan lokon en matematikaj esploroj, kiam K. Gauss (1777-1855) pruvis, ke la klasika geometria konstruo (ligita kun nura uzado de rektilo kaj cirkelo) de regula n-latero estas ebla nur kiam $n = 2^t$ (kie $t \in \mathbb{N}_2 \setminus \{0, 1\}$) aŭ $n = 2^m p_1 \cdot p_2 \cdot \ldots \cdot p_s$ (kie $m \in \mathbb{N}$ kaj p_j estas pare diferencaj primaj nombroj de Fermat). El tiu teoremo facile sekvas, ke oni povas konstrui regulan n-lateron ekz. por $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40$. Kiam $n = 6$ tio estas ebla, ĉar $6 = 2 \cdot 3$ kaj 3 estas prima nombro de Fermat aŭ pli evidente, ĉar la konstruon de la regula seslatero ni konas (el elementa instruado de matematiko). El la teoremo de Gauss facile sekvas ankaŭ tio, ke oni ne povas konstrui regulan n-lateron, kiam ekz. $n = 7, 9, 11, 13, 14, 18, 19, 21, 22, 23, 25, 26, 27, 28, 29, 31, 33, 35, 36, 37, 38, 39, 41, 42, 43, 44$.

Oni povas do konstrui regulan 17-lateron, ĉar 17 estas prima nombro de Fermat; indas rimarki, ke la teoremo de Gauss ne donas la manieron de tiu konstruo, sed nur la informon, ke tio estas ebla.

Teoremo 1. *Ĉiu divizoro de la nombro F_n havas la formon $k \cdot 2^{n+2} + 1$*

*alomnicki@poczta.fm

Tiun teoremon pruvis L. Euler (1707- 1783) kaj supozeble dank' al tiu teoremo malkovris, ke la nombro $5 \cdot 2^7 + 1$, tio estas 641, estas divizoro de F_5. Nuntempe, uzante simplan kalkulilon ni povas trovi, ke $F_5 = 4\ 294\ 967\ 297 = 641 \cdot 6\ 700\ 417$. La nombro F_5 do ne estas prima. Sen tabelo de primoj ne estus facile konfirmi, ke la nombro 6 700 417 estas primo. Okazis, ke en la produto $641 \cdot 6\ 700\ 417$ ĉiu el la faktoroj estas primo. La elirpunkto por matematikistoj (ne nur tiuj de pasintaj jarcentoj) estis trovi, ĉu la fiksita nombro de Fermat estas prima. Se tio sukcesis, oni serĉis la produton de primoj, kiu egalas al tiu nombro.

La nombro F_6 estas jene malkomponebla en primojn:

$$F_6 = 274\ 177 \cdot 67\ 280\ 421\ 310\ 721$$

tiun malkomponon trovis T. Clansen en la jaro 1856 kaj F. Landry en la jaro 1880.

En ĉi tiu artikolo, dediĉita al lernantoj (ankaŭ al studentoj de matematiko), kiuj dezirus plilarĝigi la lernejan programon de la instruado de matematiko, ni montros la eblecon de la esplorado de primeco de la nombroj F_5 kaj F_6 surbaze de tre elementaj konoj de la "lerneja" matematiko. La iloj estas tre simplaj, sed el tio ne sekvas, ke la rezonado estas tre evidenta. La studado de matematika teksto preparas al pli profundaj studoj de matematiko, kaj se okazus en lernejoj, povus interesigi lernantojn pri matematiko - la "reĝino de sciencoj".

2 Konsideroj

Unue ni pruvos, ke

Teoremo 2. *La nombro $d = k \cdot 2^7 + 1$ estas divizoro de $F_5 = 2^{32} + 1$ se kaj nur se $d|(2^4 + k^4)$*[1].

Pruvo. Evidente[2] $\mathrm{PGKD}(d, k) = 1$. Tial la sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&d|F_5\\
&d|(2^4(k \cdot 2^7)^4 + k^4)\\
&d|(2^4(k \cdot 2^7)^4 - 2^4 + 2^4 + k^4)\\
&d|\left[2^4(k \cdot 2^7 + 1)(k \cdot 2^7 - 1)((k \cdot 2^7)^2 + 1) + (2^4 + k^4)\right]\\
&d|(2^4 + k^4)
\end{aligned}$$

□

Eluzante la teoremon 2 oni tuj povas trovi la divizoron de F_5. Por $k = 5$ ja $d = 5 \cdot 2^7 + 1 = 641$ kaj $2^4 + 5^4 = 641$.

[1] $a|b$ signifas, ke a estas divizoro de b.
[2] PGKD signifas "*p*lej *g*randa *k*omuna *d*ivizoro".

Ni trovis ankaŭ tri interesajn por esploroj de primeco de la nombro F_5 kondiĉojn, ekvivalentajn al tiu, donita en teoremo 2. Sube ili estas substrekitaj. Facile do estas konfirmi, ke la sekvaj kondiĉoj estas ekvivalentaj:

$$
\begin{aligned}
&d|F_5\\
&d|(2^4+k^4)\\
&d|2^7(2^4+k^4)\\
&d|(2^7k^4+k^3-k^3+2^{11})\\
&d|\left[k^3(k\cdot 2^7+1)+(2^{11}-k^3)\right]\\
&\underline{d|(2^{11}-k^3)}\\
&d|2^7(k^3-2^{11})\\
&d|(2^7k^3+k^2-k^2-2^{18})\\
&d|\left[k^2(k\cdot 2^7+1)-(k^2+2^{18})\right]\\
&\underline{d|(k^2+2^{18})}\\
&d|2^7(k^2+2^{18})\\
&d|(2^7k^2+k-k+2^{25})\\
&d|\left[k(2^7+1)+(2^{25}-k)\right]\\
&\underline{d|(2^{25}-k)}
\end{aligned}
$$

Tiamaniere estis pruvita 3.

Teoremo 3. *Estu $d=k\cdot 2^7+1$, kie $k\in\mathbb{N}$. Sekvaj kondiĉoj estas ekvivalentaj al $d|F_5$:*

$$d|(2^4+k^4) \tag{1}$$
$$d|(2^{11}-k^3) \tag{2}$$
$$d|(2^{18}+k^2) \tag{3}$$
$$d|(2^{25}-k) \tag{4}$$

Ni rimarku, ke la kondiĉo (4) el la teoremo 3 permesas "sen kalkulado" malkovri la duan divizoron de F_5. Estas ja

$$2^{25}-5=641\cdot 52347$$

Sekve

$$2^{25}-52347=640\cdot 52347+5$$
$$2^{25}-52347=5(52347\cdot 2^7+1)$$

Por $k=52347$ estas vera la kondiĉo (4) el la teoremo 3, do la nombro $d=52347\cdot 2^7+1$ estas divizoro de F_5.

Sube ni prezentos ok proprajn pruvojn, ke $641|F_5$, bazitajn sur elementaj teoremoj pri nombroj.

Pruvo I. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&641|F_5\\
&641|2F_5\\
&641|((2^{11})^3 - 125^3 + 125^3 + 2)
\end{aligned}$$

Pro tio, ke $641|(2^{11} - 125)$ kaj $641|(125^3 + 2)$, do $641|F_5$. □

Pruvo II. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&641|F_5\\
&641|2^4 \cdot 10^6 F_5\\
&641|(10^6(2^6)^6 + 2^4 \cdot 10^6)\\
&641|\left[(640^6 - 1) + (2^4 10^6 + 1)\right]
\end{aligned}$$

Pro tio, ke $641|(640^6 - 1)$ kaj $641|(2^4 \cdot 10^6 + 1)$, do $641|F_5$. □

Pruvo III. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&641|F_5\\
&641|\left[((2^{16})^2 - 154^2) + (154^2 + 1)\right]
\end{aligned}$$

Pro tio, ke $641|(2^{16} - 154)$ kaj $641|(154^2 + 1)$, do $641|F_5$. □

Pruvo IV. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&641|F_5\\
&641|4F_5\\
&641|((2^{17})^2 - 333^2 + 333^2 + 4)
\end{aligned}$$

Pro tio, ke $641 \mid (2^{17} + 333)$ kaj $641 \mid (333^2 + 4)$, do $641 \mid F_5$. □

Pruvo V. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&641|F_5\\
&641|\left[2^6((2^{13})^2 - 141^2) + (2^6 \cdot 141^2 + 1)\right]\\
&641|\left[2^6((2^{13})^2 - 141^2) + (2^6 \cdot 141^2 - 640)\right]\\
&641|\left[((2^{13})^2 - 141^2) + (141^2 - 10)\right]
\end{aligned}$$

Pro tio, ke $641|(2^{13} + 141)$ kaj $641|(141^2 - 10)$, do $641|F_5$. □

Pruvo VI. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&641|F_5\\
&641|5^4F_5\\
&641|[5^4(2^8)^4+5^4]\\
&641|\left[((5\cdot 2^8)^4-2^4)+(2^4+5^4)\right]\\
&641|\left[2^4((5\cdot 2^7)^4-1)+641\right]
\end{aligned}$$

Pro tio, ke $641 = 5\cdot 2^7+1$, do $641|F_5$. □

Pruvo VII. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&641|F_5\\
&641|2^4F_5\\
&641|(2^{36}+2^4)\\
&641|(64^6+2^4)\\
&641|(640^6+10^62^4)\\
&641|\left[(640^6-640^2)+(10^6\cdot 2^4+640^2)\right]\\
&641|\left[640^2(640^4-1)+10^2\cdot 2^8(5^4+2^4)\right]
\end{aligned}$$

Pro tio, ke $641 = 5^4+2^4$, do $641|F_5$. □

Pruvo VIII. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned}
&641|F_5\\
&641|2^8(2^{32}+1)\\
&641|(2^{40}+2^8)\\
&641|(2^{40}\cdot 5^4+2^8\cdot 5^4)\\
&641|\left[((5\cdot 2^{10})^4-8^4)+(8^4+5^4\cdot 2^8)\right]\\
&641|\left[8^4((5\cdot 2^7)^4-1)+2^8(2^4+5^4)\right]
\end{aligned}$$

Sekve $641|F_5$. □

Nun ni esploros la nombron $F_6 = 2^{64}+1$. Unue ni okupiĝos pri la

Teoremo 4. *Se* $d = k \cdot 2^8 + 1$, *kie* $k \in \mathbb{N}$, *la sekvaj kondiĉoj estas ekvivalentaj:*

$$d|(k^8 + 1) \tag{5}$$
$$d|(k^7 - 2^8) \tag{6}$$
$$d|(k^6 + 2^{16}) \tag{7}$$
$$d|(k^5 - 2^{24}) \tag{8}$$
$$d|(k^4 + 2^{23}) \tag{9}$$
$$d|(k^3 - 2^{40}) \tag{10}$$
$$d|(k^2 + 2^{48}) \tag{11}$$
$$d|(k - 2^{56}) \tag{12}$$

Pruvo. Sekvaj kondiĉoj estas ekvivalentaj:

$$\begin{aligned} &d|F_6 \\ &d|k^8 \cdot (2^{64} + 1) \\ &d|\left[((k \cdot 2^8)^8 - 1) + (k^8 + 1)\right] \\ &d|(k^8 + 1). \end{aligned}$$

La pruvo, ke estas ekvivalentaj la ceteraj kondiĉoj el tiu teoremo povas esti analoga al la pruvo de la teoremo 3 (por la kondiĉoj (6), (7), (8)). □

Korolario 1. *(el la teoremo 4): La nombro* F_6 *estas malprima kaj ĝia divizoro estas* $1071 \cdot 2^8 + 1$ *(do* 274177*).*

Pruvo. Sufiĉas konfirmi, ĉu por la nombro $d = 1072 \cdot 2^8 + 1$ estas vera unu el la kondiĉoj (5) ĝis (12), donitaj en la teoremo 4. Ni tion faros por la kondiĉo (5). Oni do devas konfirmi, ke $d|(1071^8 + 1)$. Estas

$$\begin{aligned} d &= 274177 \\ 1071^2 &= 4d + 50333 \\ 1071^4 &= 16d^2 + 8d \cdot 50333 + 50333^2 \\ 1071^4 &= 16d^2 + 402664d + 9240d + 15409 \\ 1071^4 &= s \cdot d + 15409 \text{ kie } s = 16d + 411904 \end{aligned}$$

Sekve $1071^8 + 1 = (sd + 15409)^2 = s^2d^2 + 2sd \cdot 15409 + 15409^2 + 1$.
Pro tio, ke $15409^2 + 1 = 866d$, do $d|(1071^8 + 1)$. □

Ni rimarku, ke

$$2^{56} = 72057594037927936$$

Sekve

$$2^{56} - 1071 = 72057594037926865$$

kaj

$$2^{56} - 1071 = d \cdot 262814145745$$

kie $d = 1071 \cdot 2^8 + 1$.
Plue

$$2^{56} - 262814145745 = 1071 \cdot 2^8 \cdot 262814145745 + 1071$$

kaj

$$2^{56} - 262814145745 = 1071(2^8 \cdot 262814145745 + 1)$$

De tio, surbaze de la teoremo 4 ni ricevas ankaŭ informon, ke la nombro $2^8 \cdot 262814145745 + 1$ estas divizoro de F_6.

Bibliografio

[1] *Arytmetyka i algebra*. Wojewódzki Ośrodek Metodyczny w Bielsku – Białej, Bielsko – Biała, 1993.

[2] *Arytmetyka teoretyczna*. PWN, Warzawa, 1969.

[3] *Number Theory for Computing*. Springer, Berlin Heidelberg, 2002.

[4] *Teroria libczb*. PWN, Warzawa, 1997.

[5] *Teroria libczb (część II)*. PWN, Warzawa, 1959.

Pri la aŭtoroj

Jan Górowski kaj Adam Łomnicki estas doktoroj de matematiko kaj laboras en Pedagogia Universitato en Krakovo (Pollando). Ambaŭ el ili skribis pli ol 80 sciencajn artikolojn kaj lernolibrojn. Adam Łomnicki estas esperantisto kaj instruisto de tiu lingvo.