511.28
511.213

PRI NOMBROJ PRIMAJ

de KIRIL FABO (Anglujo).

En antaŭa artikolo ni diskutis problemon, kiun solvis *Fermat,* pri la disfaktorigo de iu granda nombro; la manieron de ĝia disfaktorigo ni malkaŝis sed pri la dua parto de la problemo, nome kiel li rekonis, ke la ricevitaj ses-ciferaj nombroj estas primaj, ni diris nenion.

De la plej fruaj tempoj de la grekaj matematikistoj nombroj primaj estas alloga temo; ĝi estas temo simpla kaj facile komprenebla laŭ siaj bazaj konceptoj — tiel simpla ke ĝi posedas iujn kvalitojn de mistero. Malgraŭ ĉi tiu simpleco ĝi tamen generas certajn problemojn de karaktero plej malfacila kaj almenaŭ iun kiu tute rezistis solvadon. Ni aludas precipe al la fama konjekto de *Goldbach,* ke ĉiu para nombro estas la sumo de du primoj.

Nia nuna temo dividas sin en du partojn, nome (a) pri la distribuo, klasifiko kaj entabeligo de primoj kaj (b) pri metodoj por konstati sen tabelo, ĉu donita nombro estas prima aŭ ne.

Al la antikvaj grekoj *Eŭklido* kaj *Eratosteno* ni ŝuldas la fundamenton por la studado de primoj. *Eŭklido* pruvis tute ne memevidentan teoremon, ke ekzistas senfine granda nombro da primoj dum *Eratosteno* inventis la metodon kiu eĉ hodiaŭ estas uzata por konstrui tabelojn de primoj. La pruvo de la teoremo de *Eŭklido* estas eble el ĉiuj pruvoj la plej eleganta kaj subtila kaj bone meritas ripeton: 1 plus la produto de ĉiuj entjeroj de 1 ĝis n ne povas esti oblo de n nek de ajna nombro (krom nur 1) malpli ol n. Tial ĝi estas aŭ prima aŭ oblo de primo pli granda ol n; ambaŭ alternativoj postulas la ekzistadon de primo pli granda ol n; do, estu n kiom ajn granda, ekzistas primo eĉ pli granda.

Eratosteno inventis praktikan metodon por listigi primojn, la tiel nomatan *Koskinon* aŭ kribrilon. La sistemo estas simpla kaj preskaŭ memevidenta; por trovi ĉiujn primojn inter m kaj n oni simple skribas la sinsekvajn entjerojn de m ĝis n en la ĉelojn de kvadrata krado kaj forstrekas, unue ĉiujn parajn nombrojn, tiam ĉiujn oblojn de tri, poste de kvin ktp. ĝis la kvadratradiko de n kiam la serĉataj primoj estas kompreneble la nombroj nestrekitaj. La provprimoj oni supozeble estis jam trovintaj per antaŭa apliko de la procedo. Estas interese, ke kiam en la deknaŭa jarcento estis konstruataj tabeloj de primoj ĝis 10 000 000 oni uzis esence saman metodon sed kun litografitaj nombrokradoj kaj ŝablonoj en kiuj estis tranĉitaj taŭge lokitaj fenestretoj (vidu *British Association Reports on Mathematical Tables* 1878, p. 172).

La entabeligo de primnombroj, eĉ se ĝi ne estas tasko tre utila de praktika vidpunkto, tamen estas de granda akademia intereso. Ŝajnas, ke la unua tabelo kiu presiĝis aperis en la jaro 1657; ĝin verkis iu *Francis Schooten* kaj ĝi montris ĉiujn primojn malpli ol 10 000. Dum la sekvantaj 150 jaroj multaj aliaj aritmetikistoj eldonis tabelojn kaj la limo puŝiĝis ĉiam pli kaj pli alten ĝis en 1811 *Chernac* eldonis liston de la 78 499 primoj malpli ol 1 000 000 kaj de la malplej grandaj faktoroj de la ceteraj nombroj. *Burckhardt* en 1814 kontrolis ĉi tiun tabelon kaj reeldonis ĝin kun listo de la primoj kaj malplej grandaj faktoroj de la nombroj de la dua miliono. La sama aŭtoro publikigis en 1816 similan tabelon por la tria miliono; en la dua miliono troviĝas 70 433 primoj kaj en la tria 67 885. En 1862 *Dase* eldonis tabelon por la sepa miliono (63 799 primoj) kaj en 1863 por la oka miliono (63 158 primoj) sed li mortis antaŭ ol li povis finlabori la naŭan milionon. La tasko tamen kompletigis *Rosenberg* kies listo de la primoj de la naŭa miliono, kiu eldoniĝis en 1865, enhavas 62 760 primojn. Ĉiuj ĉi tiuj tabeloj montris ankaŭ la malplej grandajn faktorojn de la neprimaj nombroj.

Oni rimarkas, ke kiam la tabeloj por la naŭa miliono jam publikiĝis ankoraŭ ne estis tabeloj por la kvara, kvina kaj sesa milionoj. La kaŭzo estis, ke *Dase* entreprenis sian monumentan laboron instigite de *Gauss,* kiu en 1850 skribis al li pri la dezirindeco, ke ekzistu tabeloj ĝis 10^7 kaj aldonante, ke jam ekzistas en manskribita formo tabeloj kalkulitaj de *Crelle* por la kvara ĝis sesa milionoj; *Dase* do komencis sian tabelon ĉe la sepa miliono. Aŭ tiuj tabeloj efektive neniam ekzistis, aŭ ili perdiĝis. Tiel okazis, ke listoj de la mankantaj primoj ne aperis ĝis 1879 kaj la sekvantaj jaroj, kiam *J. W. L. Glaisher* entreprenis kaj plenumis la taskon. Li trovis en la kvara miliono 66 329 primojn, en la kvina 65 369 kaj en la sesa 64 336.

Jam en la jaro 1880 do estis kompletaj la tabeloj ĝis 10^7 kaj tio ankoraŭ restas la limo de publikigitaj prim- kaj faktortabeloj; la tuta tabelaro estas lastatempe represita de *The Carnegie Institution of Washington (Publications* 105 *and* 106).

La ekzistado de fidindaj tabeloj ĝis 10^7 ebligis, ke oni faru kelkajn interesajn esplorojn pri la distribuo de la primoj — distribuo kiu eble laŭ unua ekvido devus esti tute kaprica, kia verdire ĝi ja estas se oni konsideras nur mallongajn seriojn; ekzistas tamen iuj proksimumaj ĝeneralaĵoj kaj iuj hazardaj kuriozaĵoj. Kvankam la nombro de primoj estas senfina estas tamen evidente, ke la proporcio de primoj fariĝas ĉiam pli kaj pli malgranda dum oni supreniras la nombroserion.

Legendre en 1808 trovis proksimuman esprimon por la nombro (n) de primoj malpli grandaj ol x; lia formulo estas: —

$$n = x/(\log_e x - 1{,}08366)$$

Neklara estas la signifo de la konstanto kaj oni devas supozi, ke li

alĝustige elektis ĝin post konsiderado de la jam eldonitaj listoj.

Jam frue en la 19-a jarcento ankaŭ *Gauss* estis esplorinta la saman problemon kaj alvenis al la formulo:

$$n = \int_0^x dx/(\log_e x) = \text{li } x$$

Liaj rezultoj tamen ne publikiĝis ĝis 1863 kaj dume *Ĉebiĉef* (1848) kaj *Hargreave* (1849) estis proponintaj la saman formulon. Ĝis $5 \cdot 10^6$ la esprimo de *Legendre* estas iom pli preciza ol li x; la eraro tamen pligrandiĝas pli rapide ol tiu de li x, kiu super $5 \cdot 10^6$ pli bone harmonias kun la faktoj. Eĉ pli preciza tamen estas funkcio de *Riemann*, nome:

$$n = \text{li } x - \text{li } x^{1/2}/2 - \text{li } x^{1/3}/3 - \text{li } x^{1/5}/5 + \text{li } x^{1/6}/6 \ldots\ldots$$

La ĝenerala termo estas li $x^{1/m}/m$, en kiu m estas nombro ne dividebla per kvadrato, nome nombro de la formo $abc\ldots$ kie a kaj b kaj $c\ldots$ estas malsamaj primoj; se la nombro de la faktoroj estas para la signo estas pluso, se nepara minuso.

La jena tabelo montras la verajn valorojn de n por diversaj x, kune kun la diferencoj inter ĉi tiuj valoroj kaj tiuj kalkulitaj de la tri menciitaj funkcioj.

		Diferencoj		
$x/10^6$	n	*Legendre*	*Gauss*	*Riemann*
0,1	9 593	-5	37	-6
0,2	17 985	-3	51	-3
0,3	25 998	26	89	26
1,0	78 499	44	129	29
2,0	148 932	44	123	-8
3,0	216 817	96	154	-1
4,0	283 146	177	206	33
5,0	348 515	129	123	-66
6,0	412 851	270	226	22
7,0	476 650	262	177	-40
8,0	539 808	320	192	-37
9,0	602 568	282	108	-132

Estas eble iom etendi ĉi tiun tabelon, ĉar, malgraŭ ke tabeloj de primoj pli grandaj ol $9 \cdot 10^6$ ne ekzistas, *Meissel (Mathematische Annalen* 1870 kaj 1871) kalkulis n por $x = 10^7$ kaj 10^8 per metodo ekvivalenta al vera nombrado. La rezultoj, montritaj kiel supre, estas jenaj:

10.0	664 580	560	368	87
100.0	5 761 461	6543	748	90

Estas videble el ĉi tiuj ciferoj kiom pli preciza ol la aliaj estas la

funkcio de *Riemann* kaj ŝajne estas apenaŭ eble, ke kontinua funkcio, sen periodaj termoj povus pli precize reprezenti tiajn neregulajn nombrojn.

Plidetala esploro de ĉi tiu nereguleco malkaŝas iujn kuriozaĵojn, kaj pri primo-riĉaj, kaj pri primo-malriĉaj regionoj. Kompreneble neniuj centoj tiel dense enhavas primojn kiel la du unuaj, kiuj entenas respektive 26 kaj 21; efektive neniuj aliaj centoj enhavas pli ol 17 primojn. Da tiaj 17-primaj centoj estas nur 4; unu estas la 5-a, alia la 15-a dum tria troviĝas en la unua miliono. La kvara, tute strange, okazas en la *tria* miliono.

Pri primo-malriĉaj centoj ni trovas, ke en la unua miliono estas neniu cento tute sen primoj sed en la dua ĝis deka milionoj estas respektive 1,1,2,2,4,6,4, kaj 4 centoj sen primoj. Ĉi tiuj 24 centoj tute el neprimaj nombroj estas tiuj kiuj komenciĝas per la jenaj nombroj:

1 671 800	5 837 400	7 129 900
2 637 800	5 845 200	7 565 200
3 117 300	6 012 900	7 803 500
3 933 600	6 085 000	7 826 900
4 640 600	6 333 800	8 027 700
4 652 400	6 376 200	8 367 400
5 178 200	6 789 800	8 421 300
5 518 700	6 958 700	8 905 200

La plej longaj sinsekvoj de neprimaj nombroj inter 1 kaj 10^7 estas la 153 nombroj inter 4 652 353 kaj 4 652 507 kaj la 151 nombroj inter 8 421 251 kaj 8 421 403. Estas entute 16 sinsekvoj el pli ol 131 neprimaj nombroj, el kiuj nur du estas malpli ol 2×10^6, nome 1 357 201 — — 1 357 333 kaj 1 561 919 — 1 562 051.

Ni nun venas al eble la plej interesa parto de nia temo — nome pritrakto de la metodoj por decidi ĉu donita nombro estas prima aŭ ne. Jam en alia artikolo ni pritraktis la simplan rektan „palpadan" metodon, kiu konsistas simple el prov-dividoj de N per ĉiuj primoj malpli ol $\sqrt{N}$ kaj ni montris, ke la necesa laboro estas nepritrakteble granda se N estas ekz. pli granda ol 2 aŭ 3×10^6; krome, la metodo antaŭpostulas tabelon de primoj.

Ni povas diri tuj en la komenco, ke ja ekzistas certa kaj rekta metodo, kiu ne necesigas prov-palpadojn; ĝi tamen necesigas por nombroj escepte de la plej malgrandaj, kalkuladon preter ĉiu ajn homa aŭ eĉ maŝina kapablo; ŝajne ne estas metodo por eviti la laboregon. La metodo baziĝas sur interesa teoremo trovita antaŭ preskaŭ 200 jaroj de la angla matematikisto *Wilson*, nome ke se, kaj nur se, p estas prima
$(p-1)! \equiv -1 \pmod{p}$. Ekzemple, se $p = 7$, $6! = 720$ kio estas unu malpli ol oblo de 7.

La teoremo de *Wilson* estas la sola rekta metodo kiun ni posedas por konstati ĉu nombro estas prima aŭ ne — ĝi estas efektive preskaŭ la sola ĝenerala teoremo kiu asertas „... se, kaj nur se p estas prima ...". Estas tamen multaj teoremoj kiuj asertas „... se p estas prima, tiam ..." kaj tiaj teoremoj devas fariĝi la iom necerta bazo por aliaj metodoj por rekoni primojn.[1]) El tiaj teoremoj eble la plej bone konata estas tiu de *Fermat* kiu asertas „se p estas prima, $a^{p-1} \equiv 1 \pmod{p}$ kie a estas ajna entjero." Kutime ne necesas konsideri valorojn por a pli grandajn ol 2 aŭ 3, ekzemple $2^6 \equiv 1 \pmod 7$. Ni ne povas doni ĉi tie la pruvon de ĉi tiu unuavide iom mistera teoremo; sufiĉas diri, ke ĝi efektive estas speciala kazo de pli ĝenerala teoremo trovita de *Euler* proksimume cent jarojn post *Fermat*. Ĝi asertas „Se a kaj n estas entjeroj sen komunaj faktoroj kaj se $f(n)$ estas la nombro de la nombroj malpli grandaj ol n kiuj ne havas komunajn faktorojn kun n, tiam $a \equiv 1 \pmod{n}$". Ekzemple, $f(9) = 6$ kaj $2^6 = 63+1 = 9\times7 + 1$. Kompreneble se n estas prima $f(n) = (n - 1)$ kaj ni ricevas la teoremon de *Fermat*.

Oni rimarku, ke la teoremo de *Fermat* diras, „se p estas prima tiam la restaĵo estas 1" kaj ne „se la restaĵo estas 1, p estas prima". Nu la ĥinaj matematikistoj iom antaŭiris *Fermat* ĉar jam antaŭ 25 jarcentoj ili havis teoremon kiu asertis (tamen false) ke „se $2^{n-1} - 1$ estas oblo de n, tiam n estas prima"[2]). Estas strange, ke ĉi tiu teoremo staris pli ol 2000 jarojn sen konata escepto, ĉar nur en 1819 *Sarrus* rimarkis, ke $2^{340} \equiv 1 \pmod{341}$, malgraŭ ke $341 = 11 \times 31$[3]). La afero statas do jene: se ni konstatas, ke la *Fermat*-a restaĵo por donita n ne estas 1 tiam n certe ne estas prima; se la restaĵo estas 1 kredeble n estas prima sed eble ne.

Al esceptoj de la inverso de la teoremo de *Fermat* ni poste revenos, antaŭe tamen ni priskribos metodon por kalkuli la *Fermat*-ajn restaĵojn — tasko kiu eble unuavide ŝajnas timiga pro la vere grandegaj nombroj pritraktendaj. La metodo baziĝas sur la fakto, ke oni povas manipuli kongruaĵojn tute kiel ekvaciojn, krom ke oni ne povas senkondiĉe dividi ambaŭ membrojn per faktoro. Por trovi ekzemple x en $2^{p-1} \equiv x \pmod{p}$ do ni povas ekiri de malaltaj potencoj de 2; se ni duobligas la dekstran

---

[1]) Preskaŭ memevidenta ekzemplo estas la jena: se p estas primo sed ne 2 aŭ 3 ĝi havas la formon $(6n\pm1)$. Aliaj estas: se p estas primo pli granda ol 3 tiam $p^2 \equiv 1 \pmod{24}$, se pli granda ol 5 tiam $p^4 \equiv 1 \pmod{240}$, se pli granda ol 3 kaj ne $= 7$ tiam $p^6 \equiv 1 \pmod{168}$.

[2]) Vidu *Messenger of Mathematics* vol. **27** (1897—8) p. 174.

[3]) Malgraŭ ke 2^{340} estas ege granda nombro estas tre facile pruvi tion. $2^5 \equiv -1 \pmod{11}$, tial $2^{10} \equiv 1 \pmod{11}$; $2^5 \equiv 1 \pmod{31}$, tial $2^{10} \equiv 1 \pmod{31}$; tial $2^{10} \equiv 1 \pmod{11 \times 31}$. Levante la dekstran kaj maldekstran membrojn al la 34-a potenco ni ricevas $2^{340} \equiv 1 \pmod{341}$.

membron ni rajtas aldoni unu al la potenco; se ni kvadratigas la dekstran membron ni rajtas duobligi la potencon. La jena simpla ekzemplo, en kiu ni kalkulos x por $p = 561$, eble klarigos facilan metodon por efektivigi la kalkulojn.

Potencoj de 2	Restaĵo (mod 561)
560	1
280	1
140	67
70	166
35	263
17	359
8	256
4	16

En la maldekstran kolonon skribu $p-1$, dividu ĝin per 2 kaj tuj sube enskribu la kvocienton; tiel daŭrigu, preterlasante tamen ĉiujn restaĵojn, ĝis oni atingis nombron k por kiu oni scias 2^k. Kontraŭ k, en la dekstran kolonon, skribu 2^k, sed se ĝi estas pli granda ol p skribu anstataŭe la restaĵon de la divido de 2^k per p. Tiam kvadratigu la restaĵon kaj denove kalkulu la restaĵon, laŭ modulo p, de la kvadrato kaj skribu la rezulton tuj supre. Kiam suprengrimpante la maldekstran kolonon oni renkontas neparan nombron estas tamen necese duobligi la kvadraton antaŭ ol oni kalkulas la restaĵon ĉar, formante la maldekstran oni preterlasis la restaĵojn kiam oni dividis la neparan nombrojn per 2. Se oni volas kalkuli restaĵojn de potencoj de b anstataŭ 2 la procedo estas tute sama, krom ke oni ekiru de b^k kaj b-obligu la kvadratojn antaŭ enskribo kontraŭ nepara potenco. Por grandaj valoroj de p la laboro, kvankam iom peza estas tamen sufiĉe facile farebla per simpla kalkulmaŝino; efektive laŭ la sperto de la aŭtoro ĉi tiu estas unu el la plej belaj kalkuloj kiujn oni povas fari, precipe kiam temas pri longa serio dum kiu aperadis grandegaj restaĵoj kaj jen, ĉe la lasta etapo ĉio kvazaŭ mirinde malaperas krom nur sola 1. Tia kalkulo kun sufiĉe granda konata primo povas esti bona kaj iom severa provo kaj por maŝino kaj por ĝia funkciiganto.

Ni nun konsideru pli detale esceptojn de la inverso de la teoremo de *Fermat;* tiun trovitan de *Sarrus* ni jam menciis kaj al tio oni povas aldoni la jenajn simplajn ekzemplojn:

$3^{90} \equiv 1 \pmod{91 = 7\times13}$ $\qquad$ $4^{14} \equiv 1 \pmod{15}$

$3^{120} \equiv 1 \pmod{121 = 11^2}$ $\qquad$ $2^{2046} \equiv 1 \pmod{2047 = 23\times89}$

$2^{3276} \equiv 1 \pmod{3277 = 29\times113}$

La esceptoj evidente ne estas tiel maloftaj, ke oni povas ignori ilin, efektive estas eble montri, ke ekzistas senfine granda nombro kaj ne

estas malfacila afero trovi tutajn ĝeneralajn klasojn. El tiuj ni pritraktos tri, sed ekzistas aliaj. Por formi la unuan klason oni ekiras de $a \equiv -1 \pmod{a+1}$; tial $a^2 \equiv 1$ kaj $a^{2n} \equiv 1$. Se $(a+1)$ estas nepara kaj neprima do $a^a \equiv 1 \pmod{a+1}$; ekz. $8^8 \equiv 1 \pmod 9$ kaj $14^{14} \equiv 1 \pmod{15}$. Simila klaso estas derivebla de la fakto, ke $(2n)^2 - 1 \vdots (2n+1)(2n-1)$ ni diru, $r \times s$. Tial $(2n)^2 \equiv 1 \pmod{rs}$ kaj, ĉar rs estas nepara, $(2n)^{rs-1} \equiv 1 \pmod{rs}$. Ekzemple, $6^2 \equiv 1 \pmod{35}$; tial $6^{34} \equiv 1 \pmod{35}$. La tria klaso estas malpli ĝenerala formo de la aliaj, sed estas interesa, ĉar ĝi ebligas, ke oni elektu malgrandan valoron por a, ekz. $a \vdots 2$. Se $a^n \equiv 1 \pmod{bc}$, kaj se n estas faktoro de $(bc - 1)$, evidente $a^{bc-1} \equiv 1 \pmod{bc}$, kio estas escepto. La ekzemplo de *Sarrus* apartenas al ĉi tiu klaso ($a \vdots 2$, $n \vdots 10$), kiel ankaŭ la ĉi-supra ekzemplo kun modulo 2047 por kiu $a \vdots 2$, $n \vdots 11$.

Eble ŝajnus ne tute neeble fari kontentigan teston por primoj kalkulante la restaĵojn donitajn de kelkaj malsimilaj valoroj de a; verdire se oni konstatus, ke la restaĵo estas ĉiam 1 por diversaj a, fariĝus tre kredeble, ke la nombro ja estas prima. La testo tamen ne estus tute certa ĉar ekzistas iu klaso de rimarkindaj neprimaj nombroj kies *Fermat*-aj restaĵoj estas 1 por *ĉiuj* valoroj de a kiuj ne posedas komunan faktoron kun la nombro. Efektive 561 ($\vdots 3 \times 11 \times 17$), kiun ni jam prikalkulis, apartenas al ĉi tiu klaso. Ĉiu tia nombro devas esti la produto de almenaŭ 3 malsamaj primoj kaj proksimume 200 membrojn de la klaso estas konataj.

Euler pruvis, ke se p estas prima kaj nepara $a^{(p-1)/2} \equiv \pm 1 \pmod p$, depende ĉu a respektive estas aŭ ne estas kvadrata restaĵo de p. Tial se ni konstatas, ke la *Fermat*-a restaĵo estas 1 kaj ankaŭ, ke la restaĵo je potenco $(p-1)/2$ estas nek 1 nek -1, p certe ne estas prima. Ĉi tiu testo malkaŝas la neprimecon de du el la ses esceptoj kiujn ni jam citis, nome 15 kaj 91. 561, 341, 121, kaj 2047 ($a \vdots 2, 2, 3$; kaj 2 respektive) donas 1 kiel restaĵon dum 3277 donas -1 kiuj estas rezultoj nedecidigaj.

Venis en 1896 la ĝis tiam plej grava paŝo al praktika testo por primeco kiam *Lucas (Assoc. Franç. Avanc. Sc.* vol **5**, p. 6) proponis la jenan (iom miskomprenigan) teoremon: „Se $a^x - 1$ estas oblo de p kiam $x \vdots (p-1)$ sed ne kiam x estas malpli ol $(p-1)$, tiam p estas prima". Li poste modifis ĝin al la jena: „Se $a^x - 1$ estas oblo de p kiam $x \vdots (p-1)$ sed ne kiam x estas faktoro de $(p-1)$, tiam x estas prima." La miskompreniga parto de ĉi tiu teoremo estas la vortoj „estas faktoro de $(p-1)$", ĉar efektive ne sufiĉas montri, ke la restaĵo ne estas 1 por hazarde elektita faktoro de $(p-1)$ por pruvi, ke p estas prima (ekz. $2^{17} \equiv 128 \pmod{341}$; kontraŭe estas necese montri, ke la restaĵo estas

alia ol 1 por *ĉiuj* faktoroj de $(p-1)$ [4]). Plue, se hazarde elektita faktoro de $(p-1)$ donas restaĵon 1, tio kompreneble ne pruvas, ke p estas neprima (ekz. $2^5 \equiv 1 \pmod{31}$. En tiaj okazoj estus necese rekomenci la tutan laboron kun nova a por demonstri la primecon de p. Ĉi tiuj kondiĉoj postulas, se oni volas utiligi la teoremon kiel bazon por testo por primeco, ne nur grandegan kalkuladon sed ankaŭ, ke oni povu tute disfaktorigi $(p-1)$ kio povas esti tasko preskaŭ tiel malfacila kiel la disfaktorigo de p mem.

Ĉi tiun nekontentigan aferstaton *Lehmer* antaŭnelonge multe plibonigis, unue per entabeligo de esceptoj de la inverso de la Teoremo de *Fermat* ($a \vdots 2$) kaj due, per eltrovo de interesa varianto de la teoremo de *Lucas*.

Jam en 1926 *P. Poulet (Sphinx—Oedipe* vol. 23) listigis ĉiujn neprimajn nombrojn (n) malpli ol 5×10^7 por kiuj $2^{n-1} \equiv 1 \pmod n$ sed *Lehmer (Amer. Math. Monthly* **43** [1936] 347) etendis ĉi tiun laboron en modifita formo al 10^8 pretigante liston de la 526 neprimaj nombroj inter 10^7 (la limo de la eldonitaj faktortabeloj) kaj 10^8 por kiuj la *Fermat*-a restaĵo ($a=2$) estas 1 kaj kies malplej granda faktoro estas pli granda ol 313. (Vidu *Sc. Rev.* **1** 52). Kun ĉiu nombro li citis ĝian malplej grandan faktoron. Ĉi tiu listo kune kun tiu de *Poulet* do ebligas, ke oni facile decidu ĉu ajna nombro malpli ol 10^8 estas prima aŭ ne; se la *Fermat*-a restaĵo ne estas 1, ĝi estas neprima; se la restaĵo estas unu, kaj ĝi ne posedas faktoron malpli ol 313 kaj ankaŭ ne aperas en la listoj, ĝi estas prima.

La nova teoremo de *Lehmer (Bull. Amer. Math. Soc.* **34** [1928] 54) tekstas jene: „Okaze ke $a^{n-1} \equiv 1 \pmod n$ kaj $a^{(n-1)/p} \equiv r \neq 1 \pmod n$, ĉ i u j faktoroj de n/d apartenas al la klaso $(mp^k + 1)$, kie k estas la plej alta potenco de la p r i m o p per kiu $(n-1)$ estas dividebla kaj d estas la plej granda komuna faktoro de $(r-1)$ kaj n".

La valoro de ĉi tiu teoremo troviĝas en tio, ke se la *Fermat*-a restaĵo estas 1 kaj se oni povas trovi prim-faktoron de $(n-1)$, la kampo traserĉenda por trovi faktorojn de n fariĝas trakteble mallarĝa. Kompreneble, ju pli granda la p kiun oni povas trovi, des malpli multaj estas la eblaj faktoroj de la formo (mp^k+1) kiujn oni devas provi. Denove, kiel ĉe la teoremo de *Lucas*, necesas trovi faktorojn de $(n-1)$, sed ĉi tie la disfaktorigo ne necese estu kompleta.

---

[4]) Tio plej ofte nur okazus se a estus primitiva radiko de p, ĉar laŭ difino, se a estas tia, la malplej granda valoro de la potenco kiu donas restaĵon 1 estas $(p-1)$. La solaj nombroj kiuj posedas primitivajn radikojn estas 2, 4, primoj, potencoj de neparaj primoj, kaj la duobloj de potencoj de neparaj primoj.

Ni jam ekvidis iom de la stranga, kaprica kaj „nekaptebla" karaktero de primoj kaj eble estos interese esplori la generadon de primoj. Ekzemple, se oni formetus el la menso ĉiun scion pri jam konataj primoj, ĉu estus eble kalkuli kelkajn primojn sen uzado de „kribrilaj" aŭ „palpadaj" metodoj? Alivorte, ĉu estas eble generi primojn el neprimoj? La respondo estas, ke ne. Malgraŭ ke multaj algebraj esprimoj povas generi senfine grandan nombron da primoj, estas facile demonstri, ke neniu algebra esprimo povas generi ekskluzive primojn per enmeto de miksitaj naturaj nombroj. Malgraŭ tio, ekzistas iuj algebraj esprimoj kiuj generas surprize longajn sinsekvojn de primoj; eble el tiaj la plej bone konata estas $n^2 - n+41$, kiun *Euler* trovis. De $n = 1$ ĝis $n = 40$ ĝi generas seninterrompan serion de 40 primoj. Se tamen oni permesas al si ekiri de kelkaj malgrandaj primoj estas eble generi multajn pligrandajn primojn sur bazo de la jena interesa, sed preskaŭ memevidenta teoremo: „Kaj la sumo de kaj la diferenco inter ajnaj du faktoroj kies produto estas la produto de ĉiuj primoj malpli grandaj ol N, estas mem primaj, kondiĉe ke la rezulto estas malpli ol la kvadrato de la unua primo pli granda ol N." Ekzemple, kun $N=6$ ni havas $(2\times3\times5) \pm 1 = 31$ aŭ 29; kaj $(3\times5) \pm (1\times2) = 17$ aŭ 13; kaj $(5\times2) \pm (1\times3) = 13$ aŭ 7 ktp. $N = 12$ generas la jenajn primojn malpli ol 13^2: —1, 13, 19, 31, 37, 43, 47, 83, 89, 97, 101, 103, 107, 127, 131; 139, kaj 151. Kvankam interesa, ĉi tiu metodo videble ne taŭgas por la konstruado de vere grandaj primoj kaj la nombro 2^{127} —1 kiun ni jam menciis, ŝajne ankoraŭ posedas la rekordon inter konataj primoj.

Pri la dua parto de la disfaktoriga problemo, kiun *Fermat* ricevis de sia korespondanto, nome kiel li konstatis, ke la nombroj 112 303 kaj 898 423 estas primaj — pri la problemo ĉe kiu ni ekiris —, ni ankoraŭ diris preskaŭ nenion. Verdire ni devas konfesi, ke ĝi ankoraŭ aspektas tiel mistere kiel ĉe la komenco. Ĉu oni rajtas supozi, ke li esploris ilin per la inverso de sia propra teoremo por kelkaj valoroj de a — aŭ ĉu li antaŭiris *Chernac* kaj posedis propran privatan tabelon de la primoj de la unua miliono? Eble ĉi lasta supozo estas la plej kredebla.

PAPERFORMATOJ

389.63 : 676.3

de G. P. DE BRUIN (Nederlando).

Kiu kutimas labori super paperaĵoj kaj profesie aŭ amatore prizorgas ties aranĝon, ordigon kaj konservadon, tiu spertas la maloportunon de la multeco de formatoj. Libroj, gazetoj, revuoj, leteroj; poŝtkartoj kaj ĉiaj formularoj havas la plej diferencajn dimensiojn, kio kaŭzas perdon de spaco en ŝrankoj kaj tirkestoj, malfaciligas bonordan konservadon kaj entute malhelpas efikan kaj tempoŝparan laboradon.

Ĉi tiu situacio estas nepre ŝanĝenda. Necesas krei ordon kaj sistemecon en la kaoso de paperformatoj. Kaj ĉi tio estas ebla per plia popularigo kaj plia uzado de la t.n. „normformatoj".

La normformata sistemo konsistas el ne granda nombro da science kalkulitaj formatoj, adaptitaj al la postuloj de la praktiko kaj taŭgaj por ĉiaj celoj. Ĝia baza formato estas rektangulo kun areo de unu kvadratmetro, kies lateroj rilatas unu al la alia kiel 1: 1,414 kaj kies dimensioj estas 1189 × 841 milimetroj. Duonigo rezultigas formaton kun la sama interlatera rilato kaj ĉiuj pliaj duonigoj same. Per ĉi tiuj sinsekvaj duonigoj oni akiras entute 14 diversajn formatojn. Ili formas la serion A kaj estas numeritaj A 0 ĝis A 13.

Ĉi tiuj A-formatoj estas la ĉefaj kaj oni rekomendas kiel eble plej multe uzi nur ĉi tiujn. Sed por konformiĝi al la postuloj de la praktiko, kiu nuntempe disponas pri multe pli ol 14 formatoj, oni kreis nombron da interformatoj, dividitaj en tri serioj: B., C., D. Helpe de ili oni povas akiri ĉiujn aliajn formatojn kun diferenco de nur 9 procentoj. Oblongaj formatoj formiĝas per duonigo laŭ la longo.

NORM-FORMATARO. — Mezuro: milimetroj.

Kvarobla foliego ...	A0 841×1189	B0 1000×1414	C0 917×1297	D0 771×1090
Duobla foliego ...	A1 594×841	B1 707×1000	C1 648×917	D1 545×771
Foliego	A2 420×594	B2 500×707	C2 458×648	D2 385×545
Duona foliego ...	A3 297×420	B3 353×500	C3 324×458	D3 272×385
Kvarona foliego ...	A4 210×297	B4 250×353	C4 229×324	D4 192×272
Folio	A5 148×210	B5 176×250	C5 162×229	D5 136×192
Duona folio	A6 105×148	B6 125×176	C6 114×162	D6 96×136
Kvarona folio	A7 74×105	B7 88×125	C7 81×114	D7 68×96
Okona folio	A8 52×74	B8 62×88	C8 57×81	D8 48×68
	A9 37×52	B9 44×62		
	A10 26×37	B10 31×44		
	A11 18×26	B11 22×31		
	A12 13×18	B12 15×22		
	A13 9×13	B13 11×15		

La formatoj A4 kaj A5 estas destinitaj por leterpapero, A6 por poŝtkartoj. A5 estas ankaŭ la formato por ordinaraj libroj. Por grandaj libroj oni povas uzi A4.

La normformato naskiĝis en Germanio jam en la komenco de la nuna jarcento. Ĝi trovis aprobon ankaŭ en aliaj landoj kaj nuntempe oni jam akceptis kaj uzas ĝin sur pli aŭ malpli granda skalo en Belgio, Bulgario, Ĉeĥoslovakio, Finlando, Germanio, Grekio, Hispanio, Hungario, Italio, Japanio, Nederlando, Norvegio, Polio, Rumanio, Sovetio kaj Svisio.