rekta estas barita, plenumi certajn manipuladojn por akiri ne tuj atingeblan nutraĵon ktp. Kompreneble tiaj eksperimentoj kun ofte tre nenaturaj kaj artefaritaj situacioj estas dube fidindaj. Nur tiuj, kiuj priatentas la etologion, t.e. la heredajn agojn, la kondiĉojn por ilia efektiviĝo kaj la medion en kiu la koncerna besto vivas, — nur tiuj eksperimentoj estas taŭgaj por studi la lernkapablon kaj la inteligenton.

Kiam oni ekz. vidas, ke en zoologia ĝardeno gruo ne serĉas ŝirmon kontraŭ la pluvo sub elstara tegmento aŭ sub arbo, sed kontraŭe la kokinoj faras, oni ne konkludu ke la gruo estas malpli inteligenta ol la kokino. En la natura pejzaĝo de la gruo ja ne troviĝas arboj aŭ ŝirmejoj kontraŭpluvaj, dum la koko, estante praarbara birdo, eble herede „konas" la ombrelan funkcion de arboj. Simile: kiam ĉe perdrikoj, kiujn *Heinroth* (1928) tenadis en la domo, ne venis en la kapon transflugi barilon de nur 45 cm da alto inter unu ejo kaj la najbara, sed fazanoj, tetroj kaj urogaloj tuj faras, oni ne rajtas deklari la perdrikon stulta kompare kun la aliaj galusoj[1]), ĉar la perdriko estas birdo de la senarbara pejzaĝo kaj la fazano, la tetro kaj la urogalo loĝas regionojn kun arboj, sur kiujn ili kutimas flugi.

En la supraj konsideroj mi klopodis montri ke prijuĝi la konduton de bestoj ne estas facile: oni devas esti ne nur objektiva, sed plue sena de homspeciaj konsiderinklinoj. Scio pri la etologio de la koncerna besto kaj pri la leĝoj, laŭ kiuj ĝenerale bestoj kondutas, estas nepre necesa.

LITERATURO.

Heinroth, O. & Frau M. Heinroth: Die Vögel Mitteleuropas 1924—28.
Krätzig, H.: Journ. f.Ornithol. 1940: 139.
Lorenz, K.: Journ. f.Ornithol. 1935: 137, 289.
MacDougall, W.: An introduction to social psychology, 1931.
Martinet, J. F.: Katechismus der natuur, 1827.
ter Pelkwijk, J. J. & N. Tinbergen: Zeitschr. f. Tierpsychol. 1937: 193.
Portielje, A. F. J.: Dieren zien en leren kennen, 1938.
Tinbergen, N.: The Wisconsin Bull. 1948: 6.
v. Uexküll, J.: Umwelt und Innenwelt der Tiere, 1921.
v. Uexküll, J. & G. Kristat: Streifzüge durch die Umwelten von Tieren und Menschen, 1934.

[1]) Nova vorto por subordo *Galli* el la *Galliformes*.

PRI LA DISFAKTORIGO DE GRANDAJ NOMBROJ

KIRIL FABO (Anglujo).

Korespondanto de *Pierre de Fermat* (1601—65) proponis al tiu Majstro de Nombroj la malfacilan problemon, ĉu la nombro 100 895 598 169 estas prima. Per revenanta poŝto Fermat respondis ke ne; ĝi ne estas prima, sed ĝi estas la produto de du sesciferaj nombroj (kiujn li donis), kiuj mem estas primaj.

La solvo de la problemo restis tamen triumfo mistera, ĉar Fermat neniam klarigis sian metodon, kio igis iujn matematikistojn konjekti, ke eble li eltrovis ian novan, potencan metodon. Tia konjekto eble ne estas tiel nekredebla kiel unuavide ŝajnas, ĉar oni scias, ke Fermat emis ne eldoni siajn eltrovojn al la mondo. La plej bone konata ekzemplo estas kompreneble lia teoremo ke la ekvacio $x^n + y^n = z^n$ ne havas solvon, se x, y, kaj z estas entjeroj kaj n estas pli granda ol 2. Ĝi troviĝis skribita en la marĝeno de lia ekzemplero de *„Diophantus"* de *Bachet* kun la anonco, ke li trovis „mirinde simplan pruvon". Nu, malgraŭ, ke matematikistoj multe klopodis dum tri jarcentoj por trovi ĝeneralan pruvon por ĉiuj valoroj de n, la problemo ankoraŭ restas nesolvita. Verdire la tiutempa franca skolo de nombroteoriistoj produktis aliajn misterajn rezultojn; ekzemplo estas la strangaj asertoj de *Mersenne* (tamen ne ĉiuj pravaj) pri la primeco aŭ neprimeco de iuj grandaj nombroj de la formo (2^n-1); efektive nur dum la lasta jaro iĝis k o n t r o l i t a j ĉiuj liaj asertoj. Li malpravis kiam li asertis, ke $(2^{257}-1)$ estas prima, sed li pravis pri $(2^{127}-1)$, kaj ĉi-lasta 39-cifera nombro estas la plej granda k o n a t a primo.

Ni revenu tamen al la unue menciita problemo, kiu efektive konsistas el du problemoj; la unua estas rekoni ĉu granda nombro estas prima aŭ ne; la dua estas disfaktorigi ĝin se ĝi ne estas prima. La unuan problemon ni eble poste havos okazon pritrakti, sed en la nuna artikolo ni konsideru iomete la duan.

Estas tre bone konate, ke nombroj povas esti dividataj en du klasojn: tiuj kiuj ne estas senrestaĵe divideblaj per iu ajn nombro krom si mem kaj unu, kaj tiuj kiuj povas esti esprimataj kiel la produto de nombroj de la unua klaso. Nur en unu sola maniero estas eble fari tion, ekzemple 1001 disfaktoriĝas unike al la primfaktoroj $7 \times 11 \times 13$. La problemo, do, kiun ni konsideros estas kiel trovi la primfaktorojn de grandaj nombroj, kun la antaŭsupozo, ke tiuj ja ekzistas, nome, ke la nombro ne estas prima.

Ĉi tiu disfaktorigo de nombroj eble estas la plej fundamenta procedo

de la aritmetiko, sed estas stranga fakto, ke ekzistas neniuj certaj rimedoj por efektivigi ĝin. Ĉi estas la plej simpla ekzemplo de problemo inversa, kiaj kutime estas pli malfacilaj ol problemoj rektaj. Konsideru la problemon trovi la produton de du donitaj nombroj — kiam oni komencas oni antaŭscias, ke oni nepre povos atingi la celon sen ajna divenado aŭ palpado aŭ malsukcesaj provoj — ĉiu paŝo estos paŝo celen kaj neniu paŝo estos vana — ĝi estas problemo rekta.

Konsideru tamen preskaŭ saman problemon en formo inversa — oni havas antaŭ si grandan nombron, ni diru 100 000 001, — la problemo estas trovi (se tia ekzistas) entjeron per kiu oni povas senrestaĵe dividi ĝin. Ni jam diris, ke certaj metodoj kiuj kondukos rekte al la dezirata nombro, ne ekzistas — oni devas palpe traserĉi ĉiujn eblojn — eble oni bonŝance trafos; sed se oni malsukcesas, aŭ la nombro estas prima, aŭ oni ie faris eraron ..... Verdire, tamen, estas metodoj (kiujn ni poste diskutos) per kiuj oni povas iom mallongigi la aferon montrante, ke en certaj klasoj de nombroj ne troviĝas solvoj, kaj aliaj metodoj en kiuj oni pli-malpli kaŝe traserĉas la eblojn laŭ sinsekvo nekutima.

Kiuj do estas la ebloj? De la citita nombro evidente nek 2, nek 3 estas faktoroj; ne necesas esplori ĉu 4 estas faktoro ĉar, pro tio ke 2 ne estas, ankaŭ 4 ne povas esti; 5 ne estas faktoro; ne estas necese provi 6, ĉar ĝi estas nombro neprima kaj se ĝi estus faktoro ni jam malkaŝus tion per niaj provoj pri 2 kaj 3. La ebloj do estas la primnombroj mem. Sed nur la primnombroj ĝis la kvadratradiko de la esplorata nombro M, ĉar la plej malfavora cirkonstanco estas, se M posedas nur du, preskaŭ egalajn, primfaktorojn, unu super kaj unu sub ĝia kvadratradiko. Estas evidente, ke ili ne povas esti ambaŭ pli grandaj ol la radiko; do se M ne posedas primfaktoron malpligrandan ol $\sqrt{M}$, ĝi estas prima. Nu, la kvadratradiko de 100 000 001 estas proksimume 10 000, kaj estas proksimume 1230 primoj malpli grandaj ol 10 000; do, eĉ se ni posedus tabelon de primoj ĝis 10 000 necesus en la plej malfavora okazo 1230 apartaj, tedaj dividoj (ne utilas logaritmoj) por kovri ĉiun eblon! Ni tamen kuraĝe faru kelkajn pluajn provojn — 7, 11 kaj 13 malsukcesas, sed, provante 17, ni konstatas kun plezuro, ke $17 \times 5\,882\,353 = 100\,000\,001$. Nu, 5 882 353 estas prima, sed necesus 351 pluaj provoj por montri tion.

En la plej malfavora okazo tabelo de primoj ĝis 317 640 kaj proksimume 27 460 provdividoj estus necesaj por solvi la problemon kiun *Fermat* ricevis de sia korespondanto, sed efektive (antaŭsciante la solvon) ni povas kalkuli, ke necesus proksimume 10 650 provoj, antaŭ ol oni renkontus la malpligrandan faktoron de 100 895 598 169. Ekzistas tamen aliaj rimedoj, al kiuj ni revenos post mallonga, sed eble interesa, flankenvagado.

Preskaŭ ĉiu lerneja knabo scias kiel konstati sen dividado ĉu nombro estas senrestaĵe dividebla per 2, 3, 4, 5, 6, 8, 9 aŭ 11; por 7 ekzistas almenaŭ du metodoj, kiuj tamen ne estas tiel bone konataj. Ne estas tamen ĝenerale konate, ke ekzistas simpla metodo per kiu oni povas konstati ĉu nombro estas senrestaĵe dividebla per iu ajn nombro N. La lasta cifero de N estu b, kaj N egalu al $(10n + b)$. Ĉiuj primoj finiĝas per 1, 3, 7, aŭ 9; do nur necesas konsideri ĉi tiujn 4 valorojn por b, kvankam la metodo estas egale aplikebla al aliaj valoroj. Se p kaj q estas ajnaj aliaj entjeroj oni povas ŝanĝi N en alian entjeron $T(N)$ per la procedo $T(N) = (np + bq)$. Estas tamen eble, elekti tiajn valorojn por p kaj q, ke $T(N) = N$. Se ekzemple $p = (10 - b)$ kaj $q = (n + 1)$, tio okazas. Se oni tiel traktas grandan oblon, lN de N oni ricevas alian malpli grandan oblon, kN de N, do per ripetado de ĉi tiu procedo oni finas aŭ per N mem aŭ per simpla oblo de N kiu ne plu ŝanĝiĝas. Se la granda nombro kiun oni tiel traktas, ne estas oblo de N, la serio de ricevitaj nombroj ne atingas tian fiksitan finon, sed la valoroj pli-malpli frue denove pligrandiĝas. De praktika vidpunkto estas avantaĝe, se p estas kiel eble plej malgranda; se $b = 1$ aŭ 3 aŭ 9, p povas esti 1, sed se $b = 7$ kaj N estas prima, la plej malgranda valoro por p estas 3. La respondaj valoroj por q estas montrataj en la jena tabelo:

b	p	q
1	1	$(N - n)$
3	1	$(N - n)/3$
7	3	$(n + 1)$
9	1	$(n + 1)$

La jenaj ekzemploj eble klarigos la metodon.

1) Ĉu 1843 estas oblo de 19? $N = 19$, $n = 1$, $b = 9$;
   tial $q = 2$ kaj $p = 1$.
   $T(1843) = 184 + 6 = 190$; $T(190) = 19 + 0 = 19$, do 1843 estas oblo de 19.
2) Ĉu 4559 estas oblo de 47? $N = 47$, $n = 4$, $b = 7$;
   tial $q = 5$ kaj $p = 3$.
   $T(4559) = 455 \times 3 + 9 \times 5 = 1410$; $T(1410) = 141 \times 3 + 0 = 423$.
   $T(423) = 42 \times 3 + 5 \times 3 = 141$; $T(141) = 14 \times 3 + 5 = 47$ do 4559 estas oblo de 47.

Kvankam interesa, ĉi tiu metodo tamen apenaŭ multe valoras en tiaj grandskalaj nombrooperacioj kiajn ni nun konsideras, sed antaŭ ol ni lasos la metodojn de simpla prov-dividado, menciinda estas ankoraŭ la jena, pli potenca, metodo kiu permesas, ke oni kunfandu tutan serion da prov-dividadoj en unu operacion.

La metodo baziĝas sur la fakto, ke, se m kaj N havas komunan faktoron, tiu faktoro reaperas en la restaĵo de la dividado de m per N, aŭ inverse; se m kaj N estas reciproke primaj (sen komuna faktoro) tiaj ankaŭ estas N (aŭ m) kaj la restaĵo. La nombro $P(13, 101) =$ 612 591 634 509 533 516 853 313 421 030 971 751 estas la produto de ĉiuj primoj de 13 ĝis 101 inkluzive. Estas facila afero per kalkulmaŝino trovi la restaĵon (r) de la dividado de $P(13, 101)$ per donita granda N. Facile ankaŭ estas trovi la plej grandan komunan faktoron de r kaj N per la bela algoritmo de *Eŭklido* [1]). Se la komuna faktoro estas pli granda ol 1, ĝi estos faktoro de N; se ne, oni montris, ke N ne havas faktoron malpli grandan ol 102 (supozante, ke oni antaŭe elprovis ĝin por primoj malpl grandaj ol 13). Se oni ne trovis faktoron malpli grandan ol 102 on. povas fari pluajn provojn kun aliaj P-oj, ekzemple $P(103, 199) =$ 33 495 846 626 702 153 279 106 918 423 727 531 393 773 883. La Usona matematikisto *D. H. Lehmer,* fama specialisto en ĉi tiu kampo, konstatis, ke ĉi tiu metodo estas la plej taŭga por antaŭaj provoj ĉe grandaj nombroj kaj, ke post nur sepminuta laboro kun kalkulmaŝino estas eble eltrovi ĉu granda nombro havas faktorojn malpli grandajn ol 313. Por atingi 313 necesas alia P, nome $P(211, 313)$ kaj ni aldonu, ke ĝi estas: 7 830 453 835 247 682 568 266 635 066 915 629 203 174 553 741.

La metodoj kiujn ni ĝis nun diskutis, estas metodoj de prov-dividado, sed ni nun venas al traktado de malpli rektaj, tamen pli potencaj metodoj. Verdire eĉ en ĉi tiuj metodoj ankoraŭ necesas „palpado", sed temas pri palpado de speco malpli kruda. La unua metodo, kiu baziĝas sur la fakto, ke ĉiu kvadrata restaĵo [2]) de nombro neprima estas samtempe

[1]) La algoritmo de *Eŭklido* mem baziĝas sur la supre menciita principo. La jena simpla ekzemplo klarigos la procedon: ĉu 574 kaj 2993 havas komunan faktoron? La restaĵo de la dividado de 2993 per 574 estas 123; tiu de divido de 574 per 123 estas 82; tiu de divido de 123 per 82 estas 41; divido de 82 per 41 donas nulon; do 41 estas komuna faktoro. Se la procedo ne finiĝas per 0 la nombroj estas reciproke primaj.
La tuta procedo estas simple farebla per kalkulmaŝino sen ajna skribado.

[2]) Rilate al ajna entjero q, aliaj entjeroj povas esti dividataj en du klasojn: tiuj kiuj povas, kaj tiuj kiuj neniel povas esti la restaĵoj de la dividado de kvadrata nombro per q; ili estas respektive la kvadrataj rastaĵoj kaj ne-restaĵoj de q. Ni esprimas tion per kongruaĵo $n^2 \equiv r \pmod q$, nome n^2 kongruas kun r laŭ modulo q, kie n estas ajna entjero, kaj r estas kvadrata restaĵo de q. r povas esti negativa, aŭ pli granda ol q, sed kompreneble ĉiuj tiaj valoroj povas esti reduktataj al pozitivaj nombroj malpli grandaj ol q. Se q estas prima kaj pli granda ol 2, la reduktitaj pozitivaj restaĵoj kaj ne-restaĵoj formas egalampleksajn klasojn kaj plue la produto de du restaĵoj aŭ du ne-restaĵoj faras restaĵon, dum tiu de restaĵo (escepte de nulo) kaj ne-restaĵo estas mem ne-restaĵo. Nulo kompreneble estas ĝenerala restaĵo. Kiel ekzemplo, 0,1,2, kaj 4 estas restaĵoj de 7; 3,5, kaj 6 estas ne-restaĵoj. Kompreneble ankaŭ -6, -5 kaj -3 estas restaĵoj, -4, -2 kaj -1 nerestaĵoj.

kvadrata restaĵo de ĉiuj ĝiaj primfaktoroj, ŝajne ne estas tre utila por la disfaktorigo de grandaj nombroj kaj tial ni ne plu diskutos ĝin.

La dua metodo tamen estas pli interesa kaj baziĝas sur la simpla fakto, ke se ni povas esprimi N kiel la diferencon inter du kvadratoj, ni jam disfaktorigis ĝin, ĉar $(a^2 - b^2) = (a - b)(a + b)$. Kompreneble se $(a - b) = 1$, la solvo estas banala. La procedo estas jena: por disfaktorigi N, esprimu ĝin kiel diferencon inter la kvadrato de la unua entjero pli granda ol la kvadratradiko de N kaj alia nombro B. Se okazas, ke B mem ankaŭ estas perfekta kvadrato, ni jam sukcesis disfaktorigi N, ĉar ni havas $N = A^2 - B = a^2 - b^2 = (a + b)(a - b) = p.q$. Se B ne estas perfekta kvadrato esprimu N en la formo $N = (A + 1)^2 - B_1$ kaj daŭrigu ĉi tiun procedon ĝis B fariĝas kvadrato. (Parenteze ni rimarkigu, ke se dum ĉi tiu procedo ni konstatus, ke la kvadrata parto kaj B posedus komunan faktoron tiu ĉi estus ankaŭ faktoro de N; trafan utiligon de ĉi tiu fakto ni poste renkontos). Nu, helpas la fakto, ke la kuranta sumo de sinsekvaj neparaj nombroj estas perfekta kvadrato $(i = 1 \sum n)(2i - 1) = n^2$, ĉar tial $B_1 = (B + 2A + 1)$, kaj $B_2 = (B_1 + 2A + 3)$, ktp., ĝenerale: $B_n = B(/n - 1)^*) + 2A + 2n - 1$. La jena ekzemplo klarigos la metodon: N estu 1829; la unua entjero super la radiko de N estas 43, do $N = 43^2 - 20 = 44^2 - (20 + 87) = 44^2 - 107 = 45^2 - (107 + 89) = 45^2 - 196 = 45^2 - 14^2$. Tial $1829 = (45 + 14) \times (45 - 14) = 59 \times 31$. Necesas nur rekoni kiam la ricevita B estas perfekta kvadrato, kion oni plej facile povas fari per bona tabelo de kvadratoj; estas ankaŭ utile memori, ke neniu kvadrato finiĝas per 2, 3, 7, aŭ 8 kaj, ke se nombro ne finiĝas per unu el la sekvantaj 22 ciferparoj, ĝi ne povas esti kvadrato: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, aŭ 96.

La ekzemplo kiun ni elektis, estis (intence) favora kaj bezonis nur kelkajn etapojn pro la fakto, ke ne estis granda diferenco inter la du faktoroj de N; ju pli granda la diferenco, des pli multe da etapoj estos necesaj. La metodo estas tial utila komplemento por la metodo de rektaj provoj, ĉar favora por ĉi tiu ĝenerale estas granda diferenco inter la faktoroj, kiel ni trovis ĉe 100 000 001. Estas facile kalkuli kiom da etapoj estas necesaj. A, kiel antaŭe, estu la unua entjero super la radiko de N, x estu la nombro de etapoj necesaj por ke B fariĝu kvadrato, kaj D estu la plej malgranda diferenco inter du faktoroj, p kaj q de N. Ĉe la fino de la procedo ni havos:

$$N = (A + x)^2 - B = (A + x)^2 - b^2 = (A + x + b)(A + x - b) = pq.$$

Do, $D = (p - q) = 2b$, tial $N = (A + x)^2 - D^2/4$,
kaj $x = \frac{1}{2}\sqrt{(D^2 + 4N)} - A$.

*) Pri ĉi tiu simbolo vidu Sc. Rev. **1** 23.

Estas evidente, ke, se D kaj N estas grandaj, tia estas ankaŭ x, do la procedo fariĝas nepritrakteble longa. Por 100 000 001, kiun ni jam menciis, x ekzemple estas preskaŭ 3 000 000! Ekzistas tamen rimedo por iom faciligi la aferon ĉe tiaj kazoj, sed antaŭ ol ĝin pritrakti, ni priskribos elegantan metodon per kiu oni povas montri, ke la plimulto de la ŝajne eblaj valoroj de x estas efektive neeblaj, do povas esti preterpasataj. Ĉi tiu metodo estas ne nur interesa en si mem, sed kondukas al la plej potenca disfaktoriga metodo, kaj estas efektive ankaŭ la bazo de la tiel nomata Elektra Kribrilo de *D. H. Lehmer*.

Kiam ĉe la supre priskribita metodo oni fine sukcesis fari el B perfektan kvadraton, la ekvacio staras jene:

$$N = (A + x)^2 - b^2, \quad \text{aŭ} \quad (A + x)^2 - N = b^2.$$

Estas evidente, ke, se ni dividas la maldekstran flankon per malgranda nombro m, la restaĵo devas esti kvadrata restaĵo de m, ĉiun el kiuj ni povas facile kalkuli. Kongruaĵe esprimite tio estas:

$(A + x)^2 - N \equiv r \pmod{m}$, kie r estas restaĵo de m.

Nu, kongruaĵoj posedas multajn el la kvalitoj de ordinaraj ekvacioj, kaj ni povas solvi la kongruaĵon por x. La solvo kompreneble ne konsistas el difinita valoro por x, sed nur montras ĝian formon; per elekto de alia m ni povas dedukti alian formon por x, tiel ke fine ni konstatas, ke la pli multaj el la ŝajne eblaj valoroj por x estas netaŭgaj. La jena simpla ekzemplo eble klarigos la procedon: N disfaktorigenda estu 3959. Per la supre klarigita metodo do $(x + 63)^2 - 3959 =$ iu kvadrato. Tial, laŭ modulo 3, $(x + 0)^2 - 2 \equiv 0, 1$, ĉar 0 kaj 1 estas la solaj kvadrataj restaĵoj de 3. Tial $x^2 \equiv 2, 3$ aŭ $\equiv 2, 0 \pmod 3$. Sed ĉio en la dekstra membro ankaŭ devas esti kvadrata restaĵo de 3, do 2 povas esti forstrekata. Tial $x^2 \equiv 0 \pmod 3$ kaj $x \equiv 0 \pmod 3$; alivorte x estas oblo de 3. Denove, laŭ modulo 7 ni konstatas el la originala ekvacio, ke $(x + 0)^2 - 4 \equiv 0, 1, 2, 4$, ĉar 0, 1, 2, 4 estas la solaj kvadrataj restaĵoj de 7. Tial $x^2 \equiv 4, 5, 6, 1 \pmod 7$; 5 kaj 6 ne estas restaĵoj kaj povas esti forigataj, do $x \equiv \pm 2, \pm 1$ aŭ $x \equiv 1, 2, 5, 6 \pmod 7$. Alivorte x estas aŭ 1, aŭ 2, aŭ 5, aŭ 6 pli granda ol oblo de 7. Ni povas ripeti ĉi tiun procedon laŭplaĉe kun aliaj malgrandaj nombroj, ĝis la kampo en kiu ni devas serĉi nian x estas taŭge mallarĝa; ekzemple laŭ modulo 10 ni konstatas, ke $x \equiv 0, 2, 4, 5, 7, 9$, do ni povas forstreki el la sinsekvo de l' entjeroj, komencante per 1, ĉiujn nombrojn kiuj finiĝas per 1, 3, 6, aŭ 8; el la restantaj nombroj ĉiujn kiuj ne estas obloj de 3, kaj el la tiam restantaj ĉiujn kiuj estas obloj de 7 aŭ pli grandaj ol oblo de 7 je 3 aŭ 4. Post tio, el la nombroj ĝis 40, restas nur 9, 12, 27, kaj 30.

La unua provo montras, ke 9 estas la serĉata valoro de x, ĉar

$$(63 + 9)^2 - 3959 = 1225 = 35^2.$$

Tial $3959 = (72 + 35)(72 - 35) = 37 \times 107$.

La plej ĝena parto de ĉi tiu procedo estas la forstrekado de la trovitaj neeblaj nombroj el la sinsekvo de l' entjeroj, kaj kiam temas pri grandegaj nombroj, la plej facila metodo plenumi ĝin estas per papero dividita en kvadratajn ĉelojn kaj kartonslipoj en kiuj estas tranĉitaj fenestretoj. Unue oni nombras, komencante per 1, la ĉelojn de la papero, sed kompreneble ne necesas enskribi la nombrojn — tion oni povas sufiĉe indiki laŭrande laŭ horizontalaj kaj vertikalaj vicoj. Tiam oni prenas kartonslipon, longan ekzemple 7 ĉelojn, kaj eltranĉas fenestretojn respondantajn al la trovitaj malpermesitaj pozicioj laŭ modulo 7. Nun oni trapaŝas per ĝi la kolonaron, tramarkante per krajono ĉiujn tiujn ĉelojn kiuj aperas sub la eltranĉitaj fenestretoj. Poste oni ripetas la procedon kun diversaj aliaj slipoj laŭ aliaj (prefere primaj) moduloj ĝis ĉiuj ĉeloj, escepte de nur unu aŭ du, estas markitaj; tiam la valorojn respondantajn al tiuj blankaj ĉeloj oni provu en la ekvacio, substituante ilin por x.

Ĉi tiu metodo (kun iuj pluaj kondiĉoj kiujn ni poste pritraktos) estas eble la plej potenca konata metodo por la disfaktorigo de grandaj nombroj, sed eĉ ĝi postulas pezegan laboron kiam oni faras atakon kontraŭ vere grandegaj nombroj. Pro tio *D. H. Lehmer* elpensis mirindan, tamen simplan maŝinon, la E l e k t r a n K r i b r i l o n, kiu kapablas esplori en unu minuto 300 000 valorojn por x laŭ 30 moduloj samtempe; li taksis, ke ĝi povas fari en 20 minutoj laboron kiu okupus kalkuliston dum tuta jaro. Ĝi konsistas el 30 dentradoj diversgrandaj (unu por ĉiu modulo) paralele muntitaj unu flanke de la alia, sed (pro ilia diversgrandeco) ne sur la sama akso. Ili tamen havas komunan tangenton kaj ili ĉiuj estas turnataj samtempe de longa denthava cilindro kiu agas sur ilin laŭ la komuna tangento. La denthava cilindro estas rapide turnata de elektra motoro tiel ke proksimume 300 000 dentoj preterpasas en unu minuto; ĉiu preterpasanta dento respondas al unu provvaloro por x, komencante per 1, kaj registrilo montras kiom da dentoj pasis je ajna momento. La plej malgranda el la 30 radoj havas 67 dentojn kaj la plej granda 128 kaj ĉiu respondas al unu el la primoj inter 3 kaj 127 inkluzive. Plue, ĉe la bazo de ĉiu dento de la turnataj radoj troviĝas malgranda tratruo; ĉiuj truoj en ĉiuj radoj estas je sama distanco de la cirkonferenco, tiel ke en certaj pozicioj estas eble ĵeti lumradion tute tra la radaro tra 30 kunordigitaj truoj. Kiam tio okazas la lumradio trafas sur fotoĉelon kaj tuj haltigas la maŝinon.

La rado kun 67 truoj respondas al la primo 67, do estas kvazaŭ slipo senfenestra laŭ modulo 67; kiam oni estas uzonta la maŝinon, oni

ŝtopas la truojn respondantajn al la neeblaj valoroj, laŭ tio kion oni konstatis el la kongruaĵo laŭ modulo 67. La rado kun 68 ($\equiv 4\times17$) dentoj respondas al la primo 17, sed ĝi estas kvazaŭ 4 sinsekvaj slipoj. Do oni devas trairi kvar fojojn la neeblajn valorojn laŭ modulo 17 laŭ la rando de tiu ĉi rado. Kiam oni jam ŝtopis la ĝustajn truojn de ĉiuj 30 radoj, oni ekfunkciigas la maŝinon kaj foriras. Kiam oni revenas, la maŝino jam haltis se ĝi trovis valoron de x kiu plenumas samtempe ĉiujn 30 kongruaĵojn. Oni legas x sur la registrilo kaj provas, ĉu ĝi donas faktoron de N; se ne, oni denove funkciigas la maŝinon kaj atendas ĝis ĝi trovis alian eblan valoron.

Kiel ajn simpla laŭ principo estas ĉi tiu maŝino, ni kredeble ne rajtas supozi, ke *Fermat* posedis ion ajn tian, eĉ en pli kruda formo. Verdire neniu el la rimedoj kiujn ni jam priskribis kaj kiujn siatempe li povis uzi, estus efika, sen tro granda laboro, kontraŭ tiu granda nombro kiun li ricevis.

Ni reiru tamen iomete al la fundamenta ekvacio

$$N \equiv pq \equiv (A+x)^2 - b^2 \equiv (a+b)(a-b).$$

Ni montris, ke ju pli granda la diferenco inter p kaj q, des pli granda devas esti x, la nombro de etapoj. La simpla artifiko obligi N tamen povas helpi, se la diferenco estas tro granda por esti facile traktebla; ekzemple, se N estus $341 \equiv 11\times31$, kaj ni triobligus N, ni ricevus 33×31, kiu multe pli facile cedus ol N mem. De la ekvacio ni konstatas, ke $(p+q) \equiv 2a$ kaj $(p-q) \equiv 2b$, do, kaj la sumo, kaj la diferenco de la faktoroj devas esti paraj por ke nia metodo efiku. Kutime, kompreneble, kaj p kaj q estas neparaj kaj la metodo sukcesas. Se tamen ni suspektus, ke eble unu faktoro estas proksimume la duoblo de la alia, kaj tial volus duobligi N, ni ricevus unu paran kaj unu neparan faktoron, kaj la metodo ne povus efiki, ĉar ankaŭ $(p+q)$ estus nepara. Se ni kvarobligus N ni gajnus nenion, ĉar ni nur duobligus ambaŭ faktorojn. Efektive $8N$ estas la plej malgranda oblo kiu permesas, ke ni esploru la konsekvencojn de duobligo de unu el la faktoroj, ĉar tiuokaze $8N \equiv 4p\times2q$. Ĝenerale ni povas diri, ke estas sendaĝere obligi N per ajna nepara nombro (ekz. 3, supre); por kvarobligi ni bezonas $16N$, por sesobligi $24N$, por okobligi $32N$ ktp.

Ni rajtas supozi, ke kaj la metodo, kaj ĉi tiuj simplaj faktoj, estis konataj al *Fermat;* do, supozante ke li faris nesukcesajn provojn esprimi N mem kiel la diferencon inter du kvadratoj, la sekvanta logika paŝo estus fari provojn kun $8N$. Ni faru simile:

$N \equiv 100\,895\,598\,169$; $8N \equiv 807\,164\,785\,352$. A, la unua entjero super la kvadratradiko de $8N$, estas 898 424, kies kvadrato estas 807 165 683 776. Do ni havas:

$$8N \equiv 898\,424^2 - 898\,424 \quad (!)$$

Tial $N \equiv (898\,424/8)(898\,423) \equiv 112\,303\times898\,423$.

Jes, *Fermat* certe estis bonŝanca!

MIRINDA KURACILO 615.779.932

de T. L. C. BLUETT (Anglujo).

Dum la milito, kiu finiĝis antaŭ tri jaroj ni aŭdis multon pri la sukcesoj de la scienco; tamen tiaj sukcesoj ne estis ĝojigaj, sed tendencis eksciti dubon, ĉu la scienco efektive estas profito aŭ malprofito por la homaro. La scienco estas obeema servisto, kiu senkritike plenumas la dezirojn de sia mastro, ĉu ili estas virtaj aŭ malvirtaj, saĝaj aŭ malsaĝaj, gravaj aŭ negravaj, dignaj aŭ frivolaj. La potenco, kiun la scienco donis al la homoj, tiom pligrandiĝis, ke ĝi fariĝis danĝera; se ĝi falus en la manojn de malvirtaj frenezuloj, eble pereus la gajnoj de la civilizacio de miloj da jaroj. Tamen plejmulte la homoj estas bonkoraj, kaj eĉ la malvirtaj deziras la bonon pli ofte ol la malbonon, kaj ne tute mankas al ili la racio, do oni povas esperi. Plue apenaŭ ekzistas limoj al tio, kion ni povas esperi akiri per la scienco, se ni saĝe uzos la potencon, kiun ĝi donas. Ankaŭ eĉ la plej teruraj armiloj, kiujn oni iam elpensis, ne kaŭzis dum cent jaroj tiom da suferado, kiom forigis la eltrovintoj de la kloroformo, la etero kaj aliaj anesteziloj. La kavaliro James Simpson, en Britujo, Morton en Usono kaj aliaj igis la ĥirurgiajn operaciojn nedolorigaj; poste la lordo Lister k.c. igis ilin sendanĝeraj. Lastatempe oni multe plibonigis la anestezilojn; en la lasta okazo, kiam mi mem subiris operacion, oni ne metis maskon sur mian buŝon, kiel antaŭe, kaj mi ne devis enspiri gason aŭ vaporon, kaj senti kvazaŭ mi sufokiĝus, sed oni uzis novan specon de anestezilo, — mi kredas, ke ĝi estis tiu, kiu nomiĝas „*pentothal*" — mi konsciis pri nenio krom piketo de la injektilo je la kubuto, kaj poste mi vekiĝis en mia lito en la ĉambrego de la hospitalo, ne nur ne sentante ian doloron, sed eĉ ne sentante ian naŭzon tian, kian estigas la kutimaj anesteziloj. Mi ne konsciis eĉ pri perdo de konscio.

Estas vere, ke la scienco igis la militon multe pli terura kaj universala; apenaŭ ekzistas ie en la mondo homo kiu tute ne sentis ian efikon de la milito. Tamen unu el la efikoj, kiu ĉiam akompanis la militon, ĝi grandmezure forigis. Dum antaŭaj militoj la nombro de la soldatoj, kiuj mortis de malsanoj, preskaŭ egalis la nombron de tiuj, kiuj falis en batalo. Eĉ dum la milito en Suda Afriko de 1898 ĝis 1902 tiom da soldatoj pereis de intesta febro, kiom pereis per la armiloj de la malamikoj.

Sed dum la du mondmilitoj tio ne okazis; la plimulto da mortoj rezul-