Negative Pell and arithmetic statistics

Peter Stevenhagen
Universiteit Leiden

ALGANT Alumni in China, December 27, 2025

Founding father of ALGANT

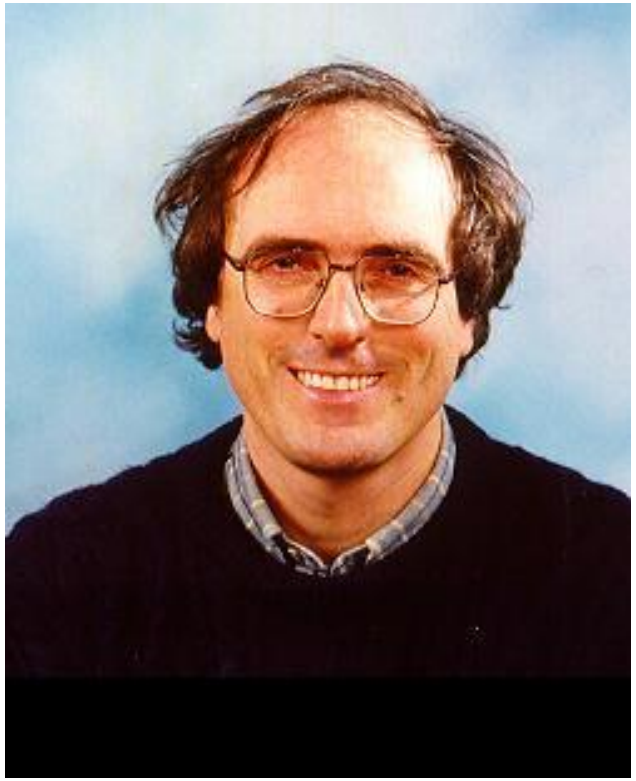
Founding father of ALGANT (Bordeaux)

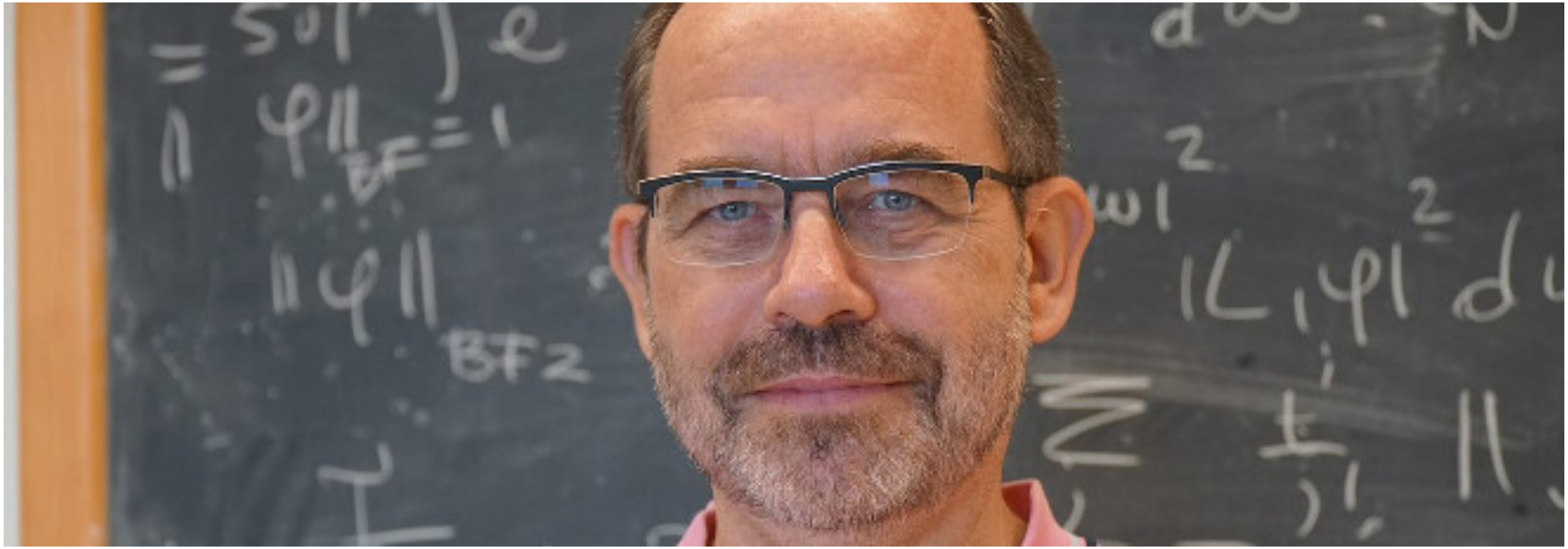
Boas Erez (Algant director 2004-2014)

Other founding fathers of ALGANT (Leiden)

Bas Edixhoven (1962-2022)

Other founding fathers of ALGANT (Padova)





Marco Garuti (1968-2021)

Some personal recollections of ALGANT-math

$\geq$1980's: algorithms & computations in number theory

- factoring integers: quadratic sieve, elliptic curves
- point counting on elliptic curves over finite fields
- computation of units and class groups
- determining rational points on curves of genus

Public key cryptography stimulated this development.

$\geq$1990’s: computer algebra systems:

GP-Pari, Maple, Mathematica, GAP, Magma, SAGE, …

Collection of data:

curves with many points, exotic class groups, …

Public data bases: LMFDB

Conjectures more often based on *numerical experimentation.*

Example: Cohen-Lenstra heuristics (1983)

Earliest *large* class group computations: quadratic fields.

Oldest example: Gauss (*Disquisitiones Arithmeticae*).

For $D \in \mathbf{Z}, \;\; D \equiv 0{,}1 \bmod 4$ not a square:

$$\begin{aligned} G = G_D &= \text{(form) class group of discriminant } D \\ &= \mathrm{SL}_2(\mathbf{Z}) \backslash \mathscr{F}_D \end{aligned}$$

with $\mathscr{F}_D =$ set of primitive integral binary quadratic forms $aX^2 + bXY + cY^2$ of discriminant $D = b^2 - 4ac$.

G is actually the (narrow) class group of the order

$$\mathcal{O}_D = \mathbf{Z}[(D+\sqrt{D})/2].$$

Behaviour for $D > 0$ and $D < 0$ is quite different.

Today: take D *fundamental*, i.e., $D = \mathrm{disc}(\mathbf{Q}(\sqrt{D}))$.

Numerical observations:

- the *odd* part of G is rarely non-cyclic
- If $D < 0$ then 3 divides $\#G$ for 43% of all discriminants
- G vanishes for 76% of (positive) prime discriminants $p \equiv 1 \bmod 4$.

These observations are **still** unproved!

Cohen-Lenstra's heuristic `explanation'

for $D < 0$, the **odd** part of G is a `random abelian group' of odd order, which occurs with weight $1/\#\mathrm{Aut}(G)$.

Example: we have $\#\mathrm{GL}_2(\mathbf{F}_p) = (p^2 - 1) \cdot \#(\mathbf{Z}/p^2\mathbf{Z})^*$, so the group $\mathbf{Z}/p^2\mathbf{Z}$ is $p^2 - 1$ times more likely than $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

For $D > 0$, the odd part of G is a `random abelian group of odd order modulo a random cyclic subgroup'.

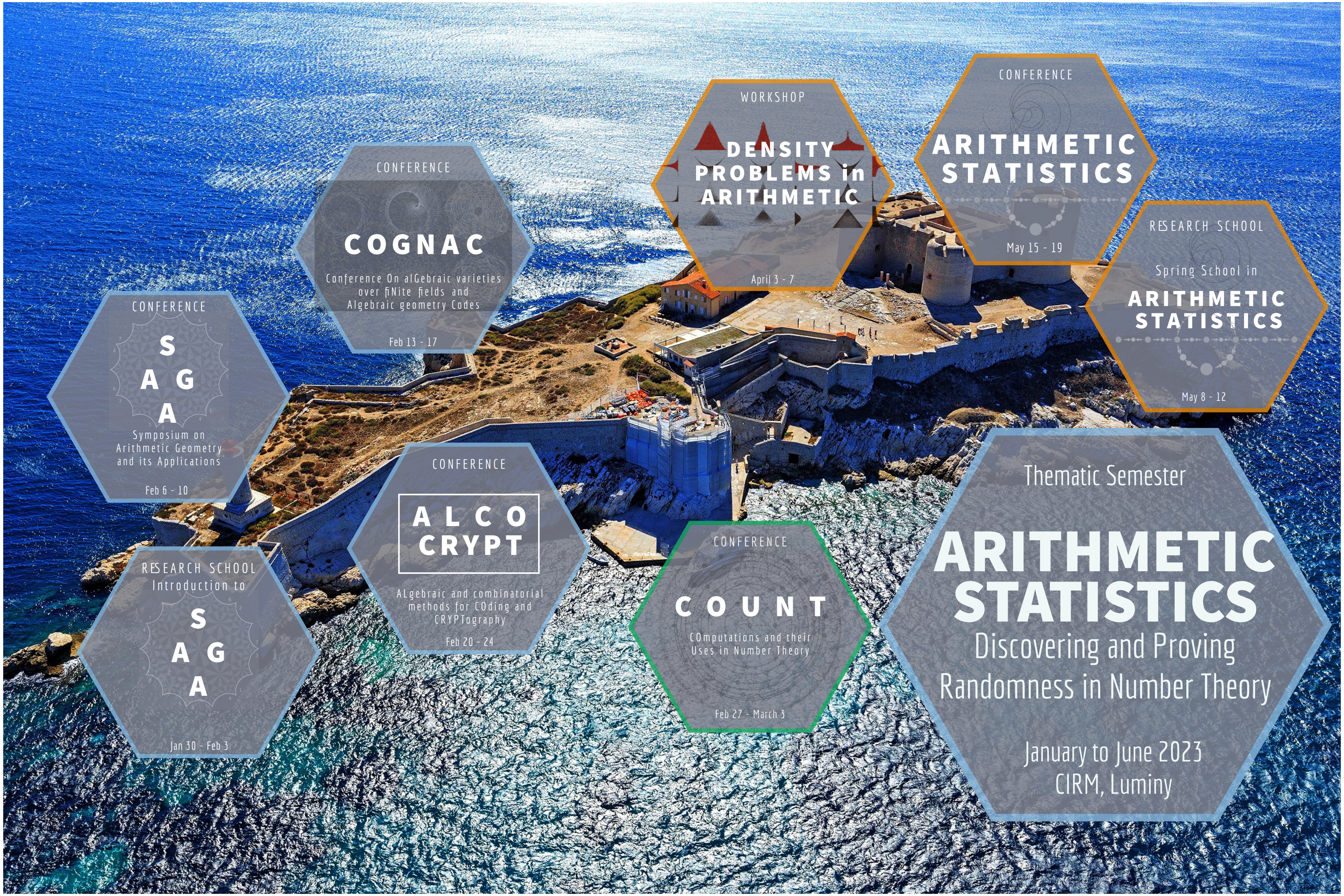
This simple framework yields very precise predictions.

Arithmetic Statistics

With the advent of computer power, we can “compute” arithmetical objects in large numbers, and access them via data bases.

Answers to natural questions about *average behaviour* can be found empirically, explained heuristically, and in some cases be *proved*.

Philosophy: objects are *randomly* distributed while obeying all *rules* that our theorems force upon them.



Thematic Semester

ARITHMETIC STATISTICS

Discovering and Proving Randomness in Number Theory

January to June 2023
CIRM, Luminy

RESEARCH SCHOOL
Introduction to
SAGA
Jan 30 - Feb 3

CONFERENCE
SAGA
Symposium on Arithmetic Geometry and its Applications
Feb 6 - 10

CONFERENCE
COGNAC
Conference On alGebraic varieties over fiNite fields and Algebraic geometry Codes
Feb 13 - 17

CONFERENCE
ALCO CRYPT
ALgebraic and combinatorial methods for COding and CRYPTography
Feb 20 - 24

CONFERENCE
COUNT
COmputations and their Uses in Number Theory
Feb 27 - March 3

WORKSHOP
DENSITY PROBLEMS in ARITHMETIC
April 3 - 7

RESEARCH SCHOOL
Spring School in
ARITHMETIC STATISTICS
May 8 - 12

CONFERENCE
ARITHMETIC STATISTICS
May 15 - 19

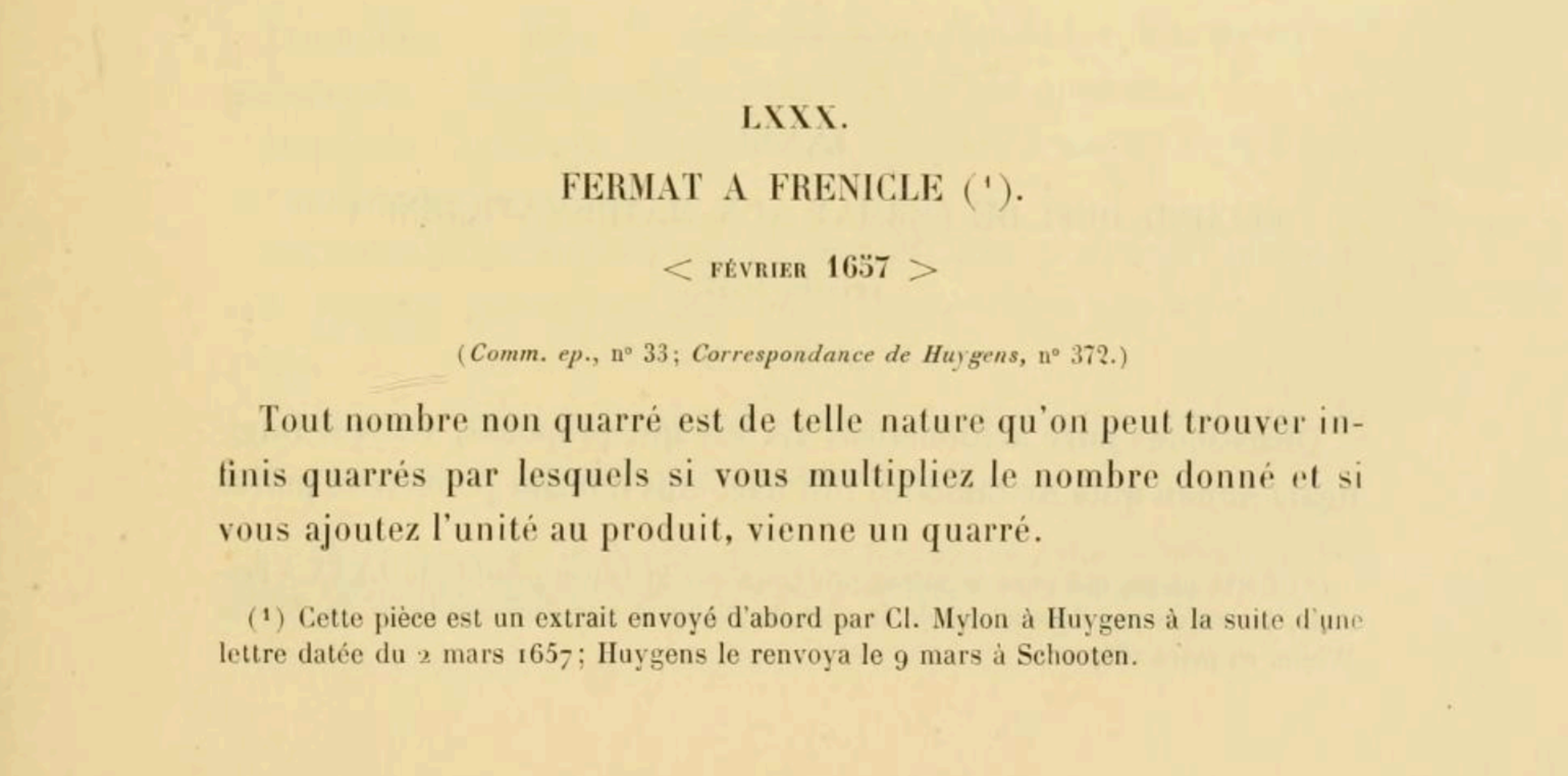
The Pell equation

For a positive non-square integer d, the equation

$$x^2 - dy^2 = 1$$

has no clear relation to John Pell (1611-1685), who was involved in in the 1668 English edition of the Swiss mathematician Johann Rahn’s *Teutsche Algebra (1659).*

Its popularity is partly due to Fermat (1607–1665), who asked for integer solutions $x, y \in \mathbf{Z}_{>0}$ in 1657.



LXXX.

FERMAT A FRENICLE [1].

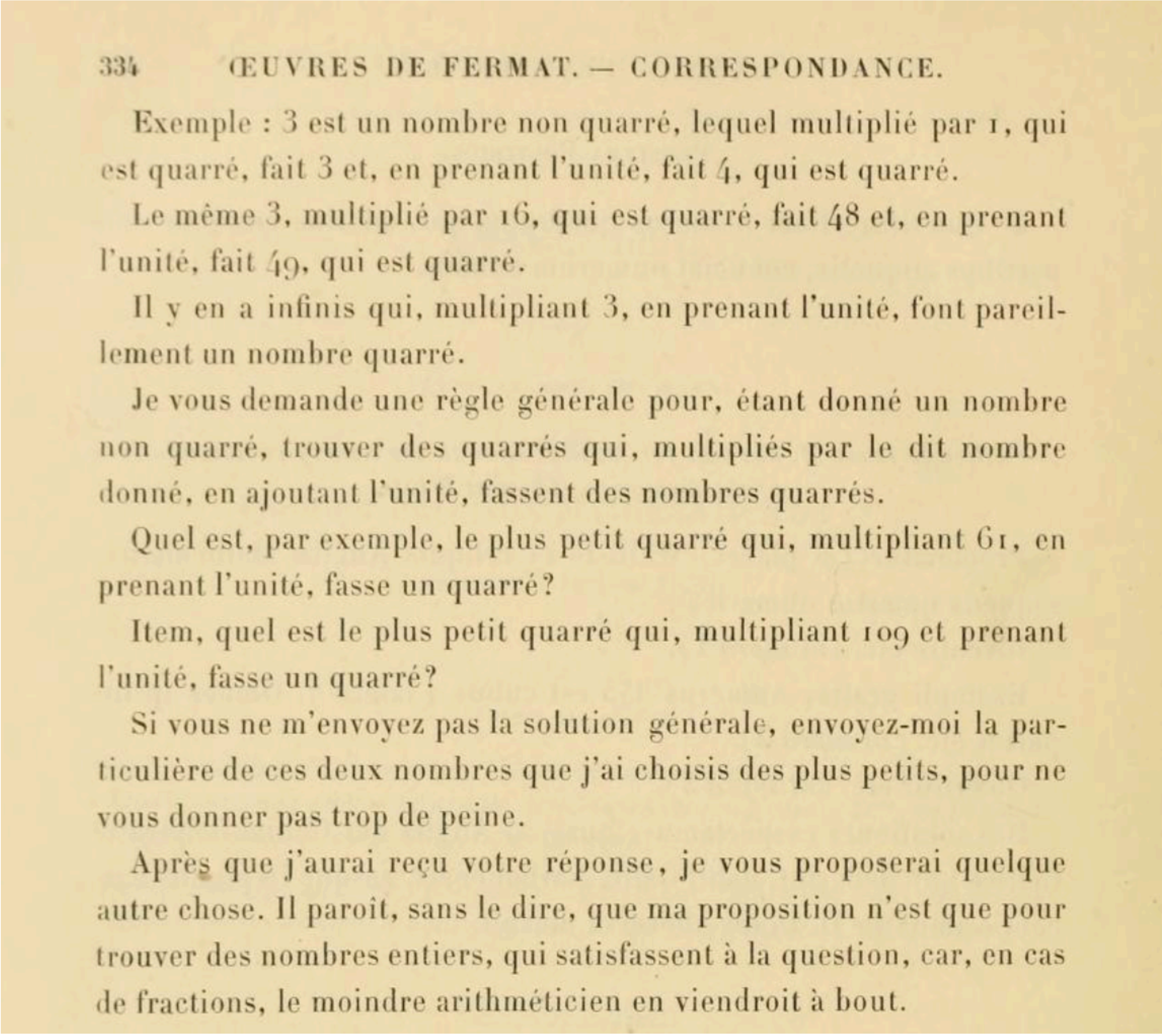
< FÉVRIER 1657 >

(*Comm. ep.*, n° 33; *Correspondance de Huygens*, n° 372.)

Tout nombre non quarré est de telle nature qu'on peut trouver infinis quarrés par lesquels si vous multipliez le nombre donné et si vous ajoutez l'unité au produit, vienne un quarré.

[1] Cette pièce est un extrait envoyé d'abord par Cl. Mylon à Huygens à la suite d'une lettre datée du 2 mars 1657; Huygens le renvoya le 9 mars à Schooten.

$$d \in \mathbf{Z}_{>0},\ d \neq \square \implies d \cdot \square + 1 = \square$$



334 ŒUVRES DE FERMAT. — CORRESPONDANCE.

Exemple : 3 est un nombre non quarré, lequel multiplié par 1, qui est quarré, fait 3 et, en prenant l'unité, fait 4, qui est quarré.

Le même 3, multiplié par 16, qui est quarré, fait 48 et, en prenant l'unité, fait 49, qui est quarré.

Il y en a infinis qui, multipliant 3, en prenant l'unité, font pareillement un nombre quarré.

Je vous demande une règle générale pour, étant donné un nombre non quarré, trouver des quarrés qui, multipliés par le dit nombre donné, en ajoutant l'unité, fassent des nombres quarrés.

Quel est, par exemple, le plus petit quarré qui, multipliant 61, en prenant l'unité, fasse un quarré?

Item, quel est le plus petit quarré qui, multipliant 109 et prenant l'unité, fasse un quarré?

Si vous ne m'envoyez pas la solution générale, envoyez-moi la particulière de ces deux nombres que j'ai choisis des plus petits, pour ne vous donner pas trop de peine.

Après que j'aurai reçu votre réponse, je vous proposerai quelque autre chose. Il paroît, sans le dire, que ma proposition n'est que pour trouver des nombres entiers, qui satisfassent à la question, car, en cas de fractions, le moindre arithméticien en viendroit à bout.

$$3 \cdot 1^2 + 1 = 2^2$$

$$3 \cdot 4^2 + 1 = 7^2$$

$$3y^2 + 1 = x^2$$

$$61y^2 + 1 = x^2 \ ?$$

$$109y^2 + 1 = x^2 \ ?$$

Integral versus rational solutions

The Pell equation

$$x^2 - dy^2 = 1$$

describes a conic in the plane passing through the point (1,0). Intersecting the hyperbola with the line

$$y = \lambda(x - 1)$$

with *rational* slope λ yields a quadratic equation in x having roots

$$x = 1 \quad \text{and} \quad x = (d\lambda^2 + 1)/(d\lambda^2 - 1).$$

We can parametrize ***all*** rational solutions as

$$(x, y) = \left(\frac{d\lambda^2 + 1}{d\lambda^2 - 1}, \frac{2\lambda}{d\lambda^2 - 1} \right), \quad \lambda \in \mathbf{Q}.$$

Pour ne pas vous donner trop de peine….

The smallest solutions Fermat asks for are

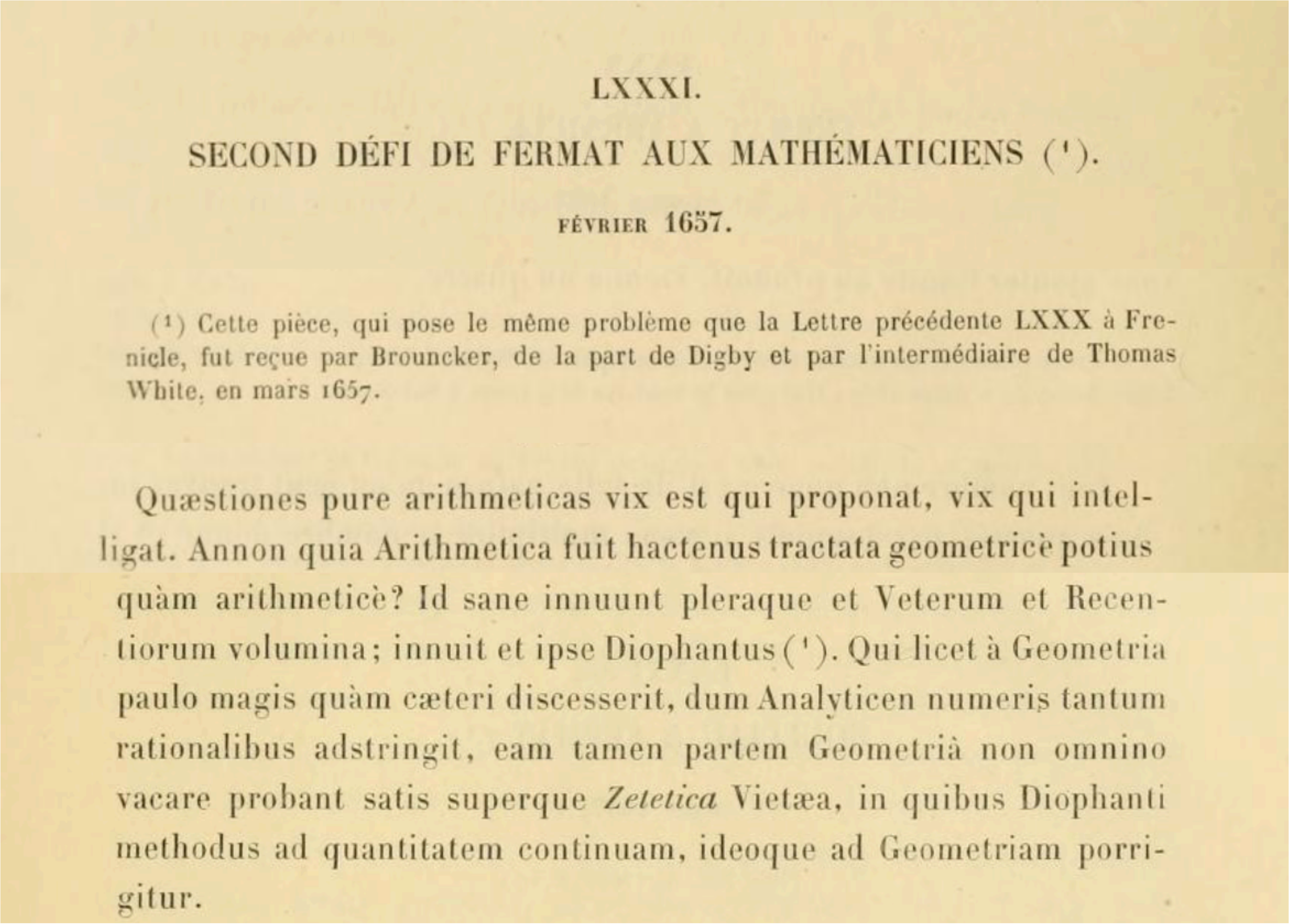
$$d = 61: \quad x = 1766\,319049,\ y = 226\,153980$$

$$d = 109: \ x = 158\,070671\,986249,\ y = 15\,140424\,455100.$$

The size of the smallest solution does not grow regularly with d :

$$d = 110: \ x = 21,\ y = 2.$$

How to communicate this to your English colleagues?



LXXXI.

SECOND DÉFI DE FERMAT AUX MATHÉMATICIENS [1].

FÉVRIER 1657.

Quæstiones pure arithmeticas vix est qui proponat, vix qui intelligat. Annon quia Arithmetica fuit hactenus tractata geometricè potius quàm arithmeticè? Id sane innuunt pleraque et Veterum et Recentiorum volumina; innuit et ipse Diophantus [1]. Qui licet à Geometria paulo magis quàm cæteri discesserit, dum Analyticen numeris tantum rationalibus adstringit, eam tamen partem Geometrià non omnino vacare probant satis superque *Zetetica* Vietæa, in quibus Diophanti methodus ad quantitatem continuam, ideoque ad Geometriam porrigitur.

[1] Cette pièce, qui pose le même problème que la Lettre précédente LXXX à Frenicle, fut reçue par Brouncker, de la part de Digby et par l'intermédiaire de Thomas White, en mars 1657.

Doctrinam itaque de numeris integris tanquam peculiare sibi vendicat Arithmetica patrimonium; eam, apud Euclidem leviter duntaxat in *Elementis* adumbratam, ab iis autem qui secuti sunt non satis excultam (nisi forte in iis Diophanti libris, quos injuria temporis abstulit, delitescat), aut promovere studeant 'Αριθμητικῶν παῖδες aut renovare.

Quibus, ut præviam lucem præferamus, theorema seu problema sequens aut demonstrandum aut construendum proponimus; hoc autem si invenerint, fatebuntur hujusmodi quæstiones nec subtilitate, nec difficultate, nec ratione demonstrandi, celebrioribus ex Geometria esse inferiores :

Dato quovis numero non quadrato, dantur infiniti quadrati qui, in datum numerum ducti, adscitâ unitate conficiant quadratum.

Exemplum. — Datur 3, numerus non quadratus; ille, ductus in quadratum 1, adscitâ unitate conficit 4, qui est quadratus.

Item idem 3, ductus in quadratum 16, adscitâ unitate facit 49 qui est quadratus.

Et, loco 1 et 16, possunt infiniti quadrati idem præstantes inveniri; sed canonem generalem, *dato quovis numero non quadrato*, inquirimus.

Quæratur, verbi gratia, quadratus qui, ductus in 149, aut 109, aut 433, etc., adscitâ unitate conficiat quadratum.

Many people solved special cases of the equation.

Big solutions yield good rational approximations $x/y \approx \sqrt{d}$.

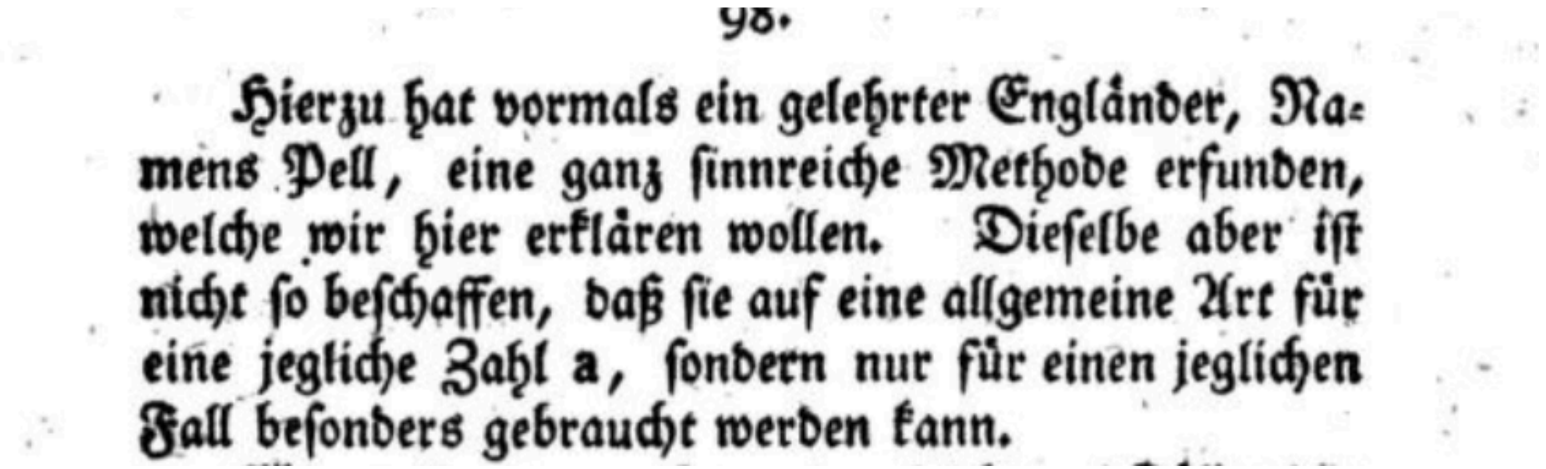
- $d = 2, 3$: ancient sources — Indians, Pythagoreans, …
- Diophantus (250 AD) solved various quadratic equations
- Brahmagupta (628 AD) *composed* solutions
- $d = 61$: solved by Bhaskara II (1114–1185)
- 17th century: Fermat, Brouncker, Wallis, …
- Euler (1765) gave a lucid exposition of what is now called the *continued fraction method* to solve the equation.
- Lagrange (1773) was the first to publish a proof that the method always finds a solution for non-square $d \in \mathbf{Z}_{>0}$.

Why Pell?

Euler (1707–1783) wrote a very influential textbook on Algebra.

It set the standard for much of our modern notation.

Euler spends a chapter (13 pages) in the book on solving the Pell equation, more than a century after Fermat's challenge.



98.

Hierzu hat vormals ein gelehrter Engländer, Namens Pell, eine ganz ſinnreiche Methode erfunden, welche wir hier erklären wollen. Dieſelbe aber iſt nicht ſo beſchaffen, daß ſie auf eine allgemeine Art für eine jegliche Zahl **a**, ſondern nur für einen jeglichen Fall beſonders gebraucht werden kann.

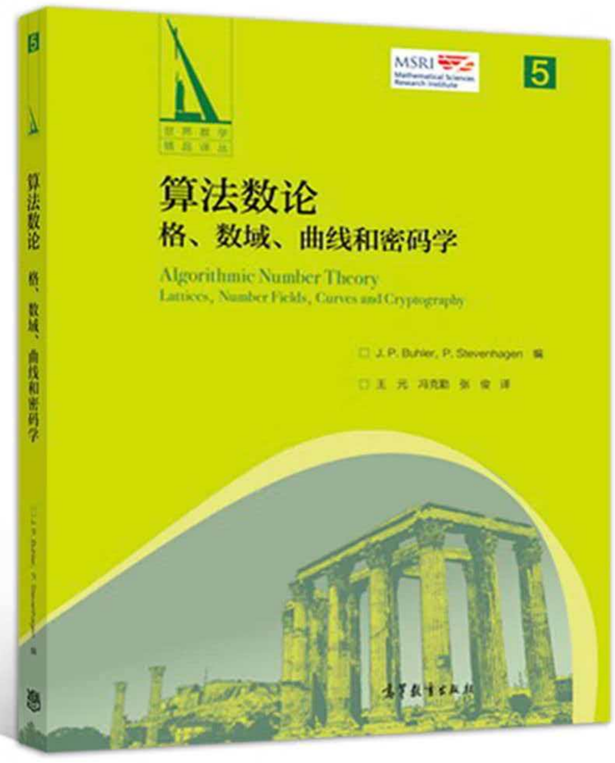
Problema bovinum (cattle problem)

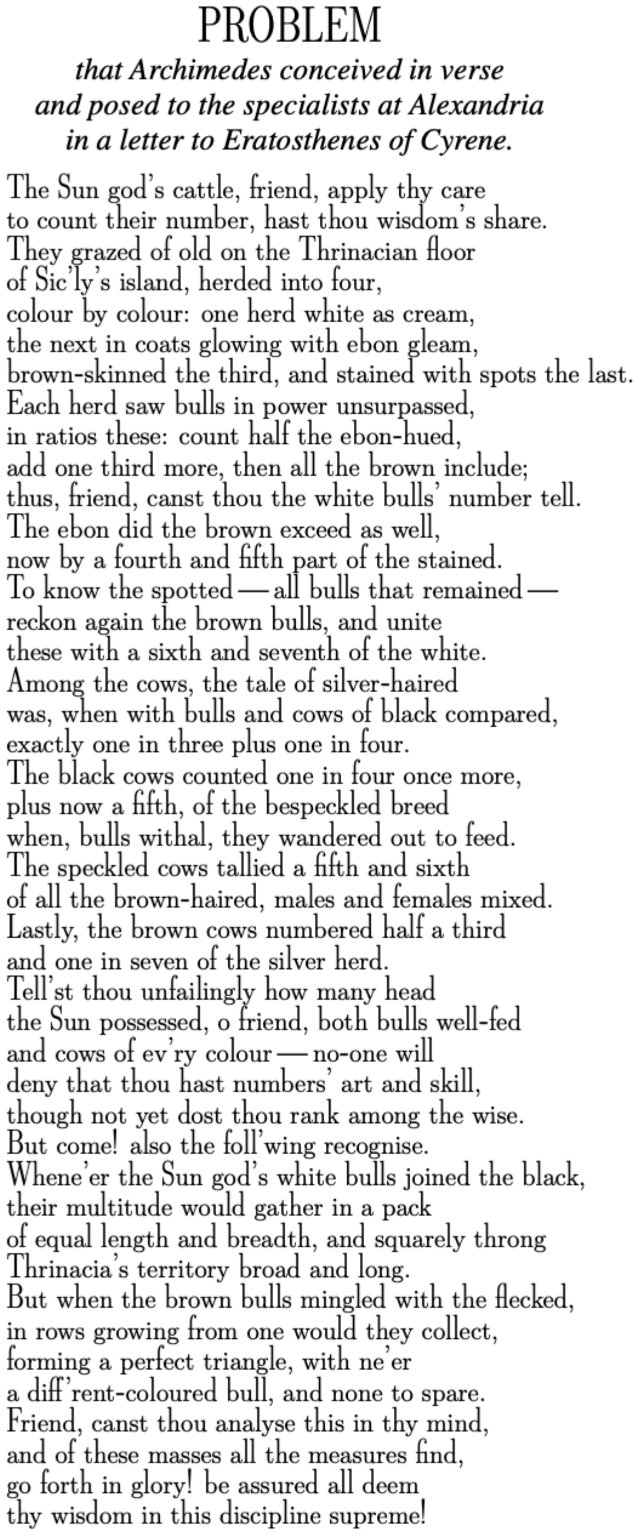
Discovered by Lessing in 1773.

Credited to Archimedes.

Leads to the Pell equation for

$d = 410\,286423\,278424$


MSRI Mathematical Sciences Research Institute
5
世界数学精品译丛
算法数论
格、数域、曲线和密码学
Algorithmic Number Theory
Lattices, Number Fields, Curves and Cryptography
J. P. Buhler, P. Stevenhagen 编
王 元 冯克勤 张 俊 译



PROBLEM

that Archimedes conceived in verse
and posed to the specialists at Alexandria
in a letter to Eratosthenes of Cyrene.

The Sun god's cattle, friend, apply thy care
to count their number, hast thou wisdom's share.
They grazed of old on the Thrinacian floor
of Sic'ly's island, herded into four,
colour by colour: one herd white as cream,
the next in coats glowing with ebon gleam,
brown-skinned the third, and stained with spots the last.
Each herd saw bulls in power unsurpassed,
in ratios these: count half the ebon-hued,
add one third more, then all the brown include;
thus, friend, canst thou the white bulls' number tell.
The ebon did the brown exceed as well,
now by a fourth and fifth part of the stained.
To know the spotted — all bulls that remained —
reckon again the brown bulls, and unite
these with a sixth and seventh of the white.
Among the cows, the tale of silver-haired
was, when with bulls and cows of black compared,
exactly one in three plus one in four.
The black cows counted one in four once more,
plus now a fifth, of the bespeckled breed
when, bulls withal, they wandered out to feed.
The speckled cows tallied a fifth and sixth
of all the brown-haired, males and females mixed.
Lastly, the brown cows numbered half a third
and one in seven of the silver herd.
Tell'st thou unfailingly how many head
the Sun possessed, o friend, both bulls well-fed
and cows of ev'ry colour — no-one will
deny that thou hast numbers' art and skill,
though not yet dost thou rank among the wise.
But come! also the foll'wing recognise.
Whene'er the Sun god's white bulls joined the black,
their multitude would gather in a pack
of equal length and breadth, and squarely throng
Thrinacia's territory broad and long.
But when the brown bulls mingled with the flecked,
in rows growing from one would they collect,
forming a perfect triangle, with ne'er
a diff'rent-coloured bull, and none to spare.
Friend, canst thou analyse this in thy mind,
and of these masses all the measures find,
go forth in glory! be assured all deem
thy wisdom in this discipline supreme!

Continued fraction method $(d = 14)$

$$\sqrt{14} = 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \sqrt{14}}}}}$$

$$3 + \sqrt{14} = \overline{[6,1,2,1]}$$

$$3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\cfrac{1}{1}}}} = \frac{15}{4} \quad \approx \sqrt{14}$$

$$15^2 - 14 \cdot 4^2 = 1$$

$$x = 15,\ y = 4$$

Algebraic number theory

$$x^2 - dy^2 = 1 \quad \Longleftrightarrow \quad (x + y\sqrt{d})(x - y\sqrt{d}) = 1$$

We recognise the norm map $\quad N : \mathbf{Z}[\sqrt{d}] \to \mathbf{Z}$

on the quadratic order $\mathbf{Z}[\sqrt{d}]$, which maps *units* to $\mathbf{Z}^* = \{\pm 1\}$.

The units $x + y\sqrt{d} \in \mathbf{Z}[\sqrt{d}]^*$ correspond to the solutions of

$$x^2 - dy^2 = \pm 1$$

Dirichlet unit theorem: $\quad \mathbf{Z}[\sqrt{d}]^* = \{\pm 1\} \times \langle x + y\sqrt{d} \rangle$

All units in the order $\mathbf{Z}[\sqrt{d}]$ are — up to sign — powers of a single *fundamental unit* $x + y\sqrt{d}$: we have $x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n$.

The order $\mathbf{Z}[\sqrt{d}]$ may not be the maximal order $\mathcal{O}_d$ in $\mathbf{Q}(\sqrt{d})$.

For $p \equiv 1 \bmod 4$ prime we have $\mathcal{O}_p = \mathbf{Z}[(1+\sqrt{p})/2]$ with fundamental unit of norm -1:

$$\left(\frac{39+5\sqrt{61}}{2}\right)^6 = 1766\,319049 + 226\,153980\sqrt{61}$$

$$\left(\frac{261+25\sqrt{109}}{2}\right)^6 = 158\,070671\,986249 + 15\,140424\,455100\sqrt{109}$$

This is not the cause of the `exponential size’ of the solutions as a function of the input parameter d.

Arithmetic statistics question (still open…)_

Fermat found primes $p = 61,\ 109,\ 149,\ \ldots$ for which it takes large positive y to make $1 + py^2$ into a square.

For primes $p \equiv 1 \bmod 4$, the fundamental unit $\varepsilon_p \in \mathcal{O}_p = \mathbf{Z}[(1+\sqrt{p})/2]$ has norm -1, as does $\varepsilon_{4p} \in \mathcal{O}_{4p} = \mathbf{Z}[\sqrt{p}]$.

The fundamental solution to $x^2 - py^2 = 1$ equals

$$x + y\sqrt{p} = \begin{cases} \varepsilon_p^2 & \text{when } \varepsilon_p \in \mathcal{O}_{4p} \\ \varepsilon_p^6 & \text{else.} \end{cases}$$

For which fraction of $p \equiv 1 \bmod 4$ are we in Fermat's "second case"?

Negative Pell question

For how many non-squares $d > 0$ is the *negative Pell equation*

$$x^2 - dy^2 = -1$$

solvable?

The continued fraction method does give a criterion: this happens if and only if the continued fraction for $\sqrt{d}$ has *odd* period length.

But how often will that happen?

For primes $p \mid d$, the congruence $x^2 \equiv -1 \bmod p$ results.

Necessary condition: no prime $p \equiv 3 \bmod 4$ divides d.

Solvability of negative Pell is rare

$$\mathbf{D} = \{d \in \mathbf{Z}_{>0} : \text{no } p \equiv 3 \bmod 4 \text{ divides } d\}$$

$$d \in \mathbf{D} \iff x^2 - dy^2 = -1 \text{ is solvable in } \textit{rational } x \text{ and } y$$

Integers $d \in \mathbf{Z}_{>0}$ not divisible by primes $p \equiv 3 \bmod 4$ form a *thin* subset of all integers.

$$\#\{d \in \mathbf{D} : d \leq X\} \sim c \cdot \frac{X}{\sqrt{\log X}}$$

with the explicit value

$$c = \frac{3}{2\pi} \prod_{p \equiv 1 \bmod 4} (1 - p^{-2})^{1/2}.$$

But how often will there be *integral* solutions?

A Fermat-like proof

$x^2 - py^2 = -1$ is solvable for all primes $p \equiv 1 \bmod 4$

Proof. Suppose $x^2 - py^2 = 1$ is the fundamental solution.
As x is odd and y is even, we can write

$$\frac{x+1}{2} \cdot \frac{x-1}{2} = p\left(\frac{y}{2}\right)^2.$$

Two positive coprime integers at distance 1 with product $p \cdot \square$ are of the form a^2 and pb^2, so $a^2 - pb^2 = -1$.

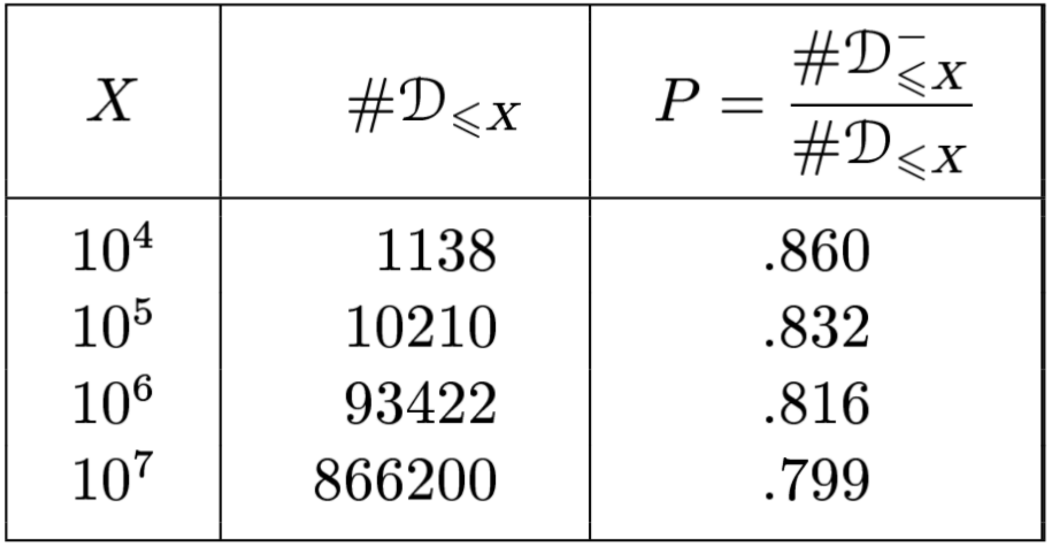
So at least negative Pell is solvable for infinitely many d…

For now: restrict to *squarefree* $d \in \mathbf{Z}_{>0}$.

$$\mathscr{D}^- = \{d \in \mathbf{Z}_{>0} : d \text{ squarefree, } x^2 - dy^2 = -1 \text{ is solvable}\}$$

$$\mathscr{D} = \{d \in \mathbf{Z}_{>0} : d \text{ squarefree, no } p \,|\, d \text{ prime is } 3 \bmod 4\}$$

Question: what is the *probability* for `random' $d \in \mathscr{D}$ to be in $\mathscr{D}^-$?



X	$\#\mathcal{D}_{\leqslant X}$	$P = \dfrac{\#\mathcal{D}^-_{\leqslant X}}{\#\mathcal{D}_{\leqslant X}}$
10^4	1138	.860
10^5	10210	.832
10^6	93422	.816
10^7	866200	.799

Any guesses for a limit value for $X \to \infty$?

Stevenhagen’s conjecture (1992)

The limit value exists and is equal to

$$S = \lim_{X\to\infty} \frac{\#\mathscr{D}^{-}_{\leq X}}{\#\mathscr{D}_{\leq X}} = 1 - \prod_{j\geq 1 \text{ odd}} (1 - 2^{-j}) \approx .580577\,5582$$

This has now been proved by Koymans and Pagano.

It cannot be directly `observed’ from tabulated numerical data.

- Why this number?
- Why doesn’t it show from the data?
- What goes into proving this?

Solvability of negative Pell

Units are intimately related to class groups.

The sign of the norm of the fundamental unit in $\mathcal{O} = \mathbf{Z}[\sqrt{d}]$ determines the difference between the *ordinary* and the *narrow* class group of $\mathcal{O}$:

$$1 \to \langle[(\sqrt{d})]\rangle \to \mathrm{Cl}^+(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}) \to 1.$$

The ideal class $F_\infty = F_{\infty,d} = [(\sqrt{d})]$ in $\mathrm{Cl}^+(\mathcal{O})$ has order 1 or 2.

It “is” the *Frobenius at infinity* for the narrow ring class field of $\mathcal{O}$.

Negative Pell is solvable for $d \iff F_\infty = 1$

F_∞ lives in the 2-part of $\mathrm{Cl}^+(\mathcal{O})$, which is not exactly `random’.

Genus theory

For $d = p_1 p_2 p_3 \cdots p_t$ a product of t primes not congruent to $3 \bmod 4$

$$\mathrm{Cl}^+(\mathcal{O})[2] \cong (\mathbf{Z}/2\mathbf{Z})^{t-1}$$

Given $\epsilon \in \mathbf{R}_{>0}$, *almost all* integers $n > 0$ have the property that its number $\omega(n)$ of distinct prime divisors satisfies

$$(1-\epsilon)\log\log n < \omega(n) < (1+\epsilon)\log\log n.$$

So with *increasing* d, we would expect $F_\infty = 1$ to happen with *decreasing* probability if $F_\infty \in \mathrm{Cl}^+(\mathcal{O})[2]$ were a random element.

Apparently it is not a random element….

The 4-rank of $\mathrm{Cl}^+(\mathcal{O})$

[László Rédei (1900–1980)]

For our $d \in \mathcal{D}$, the Frobenius at infinity F_∞ is always contained in the kernel of the natural map

$$\mathrm{Cl}^+(\mathcal{O})[2] \longrightarrow \mathrm{Cl}^+(\mathcal{O})/\mathrm{Cl}^+(\mathcal{O})^2.$$

This kernel is an $\mathbf{F}_2$-vector space of dimension equal to the 4-rank $e_4(\mathrm{Cl}^+(\mathcal{O}))$ of the narrow class group $\mathrm{Cl}^+(\mathcal{O})$.

For $d = p_1 p_2 p_3 \cdots p_t$,

- $\mathrm{Cl}^+(\mathcal{O})[2]$ has t canonical generators (with 1 relation)
- $\mathrm{Cl}^+(\mathcal{O})/\mathrm{Cl}^+(\mathcal{O})^2$ is a subgroup of index 2 in Gal$(G/\mathbf{Q}) \cong \mathbf{F}_2^t$.

So our map can be described in terms of a $t \times t$-matrix over $\mathbf{F}_2$.

The Rédei matrix

$$R_4 : \mathbf{F}_2^t \twoheadrightarrow \mathrm{Cl}^+(\mathcal{O})[2] \longrightarrow \mathrm{Cl}^+(\mathcal{O})/\mathrm{Cl}^+(\mathcal{O})^2 \subset \mathbf{F}_2^t$$

Rédei's theorem (1934):

$$e_4(\mathrm{Cl}^+(\mathcal{O})) = \dim_{\mathbf{F}_2} \ker R_4 - 1 = t - 1 - \dim_{\mathbf{F}_2} \operatorname{im} R_4.$$

For $u = (1)_{i=1}^t \in \mathbf{F}_2^t$ we have $u \mapsto [(\sqrt{d})] = F_\infty \in \mathrm{Cl}^+(\mathcal{O})[2]$.

Remember:

Negative Pell is solvable for $d \iff F_\infty = 1$

"Negative Pell is solvable" now translates as

$\ker R_4 \twoheadrightarrow \mathrm{Cl}^+(\mathcal{O})[2] \cap \mathrm{Cl}^+(\mathcal{O})^2$ has kernel $\mathbf{F}_2 \cdot u$.

A random $w \neq 0$ in $\ker R_4$ generates the kernel with probability $2^{e_4+1} - 1$.

Heuristic underlying the conjecture

If $\mathcal{O} = \mathbf{Z}[\sqrt{d}]$ has narrow class group $\mathrm{Cl}^+(\mathcal{O})$ of 4-rank e, then we expect Negative Pell for d to be solvable with probability $(2^{e+1} - 1)^{-1}$.

The 4-rank e is determined by the corank of the Rédei matrix for $\mathcal{O}$.

For $d \in \mathcal{D}$, this is essentially a symmetric $(t-1) \times (t-1)$ matrix over $\mathbf{F}_2$.

Fixing $t = \omega(d)$, the Rédei matrix “is” random symmetric.

It has corank e with some probability $p_{e,t} \in \mathbf{Q}$. Put $S_t = \displaystyle\sum_{e=0}^{t-1} \frac{p_{e,t}}{2^{e+1} - 1}$.

Conjectural constant: $S = \displaystyle\lim_{t\to\infty} S_t = 1 - \prod_{j \geq 1 \text{ odd}} (1 - 2^{-j})$.

Three decades towards a proof

Rédei matrices of maximal rank $t-1=\omega(d)-1$ are frequent.

For $t\to\infty$ they make up a fraction $\prod_{j\geq 1 \text{ odd}}(1-2^{-j})$ of all matrices.

In this case $(e=0)$ our heuristic is a well known theorem. It yields lower bounds on $\#\mathscr{D}_t^-(X)$ for *fixed* t (**Cremona-Odoni**, 1989).

Fouvry & Klüners (2010)

$$\lim_{t\to\infty}\lim_{X\to\infty}\frac{\mathscr{D}_t^-(X)}{\mathscr{D}_t(X)}=\lim_{X\to\infty}\frac{\mathscr{D}^-(X)}{\mathscr{D}(X)}$$

Alexander Smith (2017—..) proved Cohen—Lenstra for the 2-Sylow part of imaginary quadratic class groups.

On Stevenhagen's conjecture

Peter Koymans*[1] and Carlo Pagano†[2]

[1]University of Michigan
[2]University of Glasgow

February 1, 2022

Abstract

We generalize a classical reciprocity law due to Rédei [39] using our recently developed description of the 2-torsion of class groups of multiquadratic fields [28]. This result is then used to prove a variety of new reflection principles for class groups, one of which involves a symbol similar to the spin symbol as defined in work of Friedlander, Iwaniec, Mazur and Rubin [20]. We combine these reflection principles with Smith's techniques [42] to prove Stevenhagen's conjecture [43] on the solubility of the negative Pell equation.

1 Introduction

Integral points on conics are a classical topic of study going back to at least the ancient Greeks. For fixed squarefree $d > 0$, the equation

$$x^2 - dy^2 = 1 \text{ to be solved in } x, y \in \mathbb{Z}$$

What’s next?

The “easier” case of fixed $t = \omega(d)$ has remained open.

For primes $p, q \equiv 1 \bmod 4$ the equation

$$x^2 - pqy^2 = -1$$

should be solvable for a fraction 2/3 of all $d = pq$.

What about the non-squarefree case? Can we also determine

$$\lim_{X \to \infty} \frac{\mathbf{D}^-(X)}{\mathbf{D}(X)}$$

for $\mathbf{D} = \{d \in \mathbf{Z}_{>0}$: no $p \equiv 3 \bmod 4$ divides $d\}$?

Recall:

$$\#\{d \in \mathbf{D} : d \leq X\} \sim \frac{3}{2\pi} \prod_{p \equiv 1 \bmod 4} (1 - p^{-2})^{1/2} \cdot \frac{X}{\sqrt{\log X}}$$

The subset $\mathbf{D}^- \subset \mathbf{D}$ of those d for which $x^2 - dy^2 = -1$ is solvable should also have a density!

Conjecture (JTNB 7, 1995)

$$\lim_{X \to \infty} \frac{\mathbf{D}^-(X)}{\mathbf{D}(X)} = S \cdot \prod_{p \equiv 1 \bmod 4} (1 + \frac{\psi(p)}{p^2 - 1})(1 - \frac{1}{p^2}) \approx .57339$$

with

$$\psi(p) = \frac{2 + (1 + 2^{1 - \mathrm{ord}_2(p-1)})p}{2(p+1)}.$$

Thank you!

$$\sum_{f\geq 1}\frac{\psi(f)}{f^2} = \prod_{p \text{ prime}}(1+\frac{\psi(p)}{p^2}+\frac{\psi(p)}{p^4}+\frac{\psi(p)}{p^6}+\dots)$$

$$= \prod_{\substack{p \text{ prime} \\ p\equiv 1 \bmod 4}}(1+\frac{\psi(p)}{p^2-1}).$$