On the Work of Hendrik W. Lenstra, Jr.¹

Marius van der Put

Department of Mathematics, University of Groningen
P.O.Box 800, 9700 AV Groningen, The Netherlands
email: mvdp@math.rug.nl

The Johann Bernoulli Foundation of Mathematics has given me the pleasant opportunity to introduce Professor Hendrik Willem Lenstra, Jr., our speaker for the 1994–1995 Johann Bernoulli Lecture.

Let me start with some information about his Curriculum Vitae. Hendrik was born in 1949 (Zaandam, The Netherlands) in a family where mathematics had a special place. His father was a mathematician. He was among other things teacher in Mathematics and rector at the Heymans-Lyceum in Groningen and Hendrik grew up in Groningen. There are more mathematicians bearing the name Lenstra. Two of them are Arjen K. Lenstra and Jan Karel Lenstra, both brothers of Hendrik and both well known mathematicians. It seems inevitable that mathematics was a common subject of conversation in the Lenstra family. In an interview printed in the newspaper Trouw (19-10-1988), Hendrik has stated that he cannot recollect not to know what prime numbers are. At present he is a leading authority on prime numbers and number theory.

Hendrik studied mathematics at the University of Amsterdam. It seems unnecessary to say that he was an extraordinary student. He solved a problem on finite fields. His first great feat is the solution of a problem of Emmy Noether. A seminar given by Frans Oort (later his thesis adviser) stimulated this research on Emmy Noether’s problem. The subject of the seminar was a “counterexample” by R.G. Swan, dating from 1969. Hendrik solved the question of Emmy Noether for any abelian group and any base field.

Lenstra’s theorem was the subject of the Séminaire Bourbaki talk by M. Kervaire: “Fractions rationnelles invariantes d’après H.W. Lenstra.” Lenstra’s paper on the subject appeared in the prestigious journal Inventiones mathematicae. No small feat for a student!

We continue with his professional career. In 1977 Hendrik wrote his thesis “Euclidische getallenlichamen” under the supervision of Prof. Frans Oort. At

the age of 28 he was appointed full professor at the University of Amsterdam. In
1987 he left The Netherlands in order to become full professor at the University
of California, Berkeley. From January–June 1994, he was Miller professor at
the University of California, Berkeley.
The full account of the data of his active career would take several pages. We
just mention a few items:

- An invited lecture at Séminaire Bourbaki, June 1981.
- Member of the Koninklijke Nederlandse Akademie van Wetenschappen
  (Royal Dutch Academy of Science) since 1984.
- Fullerson Prize winner 1985.
- Plenary lecture, international Congress of Mathematicians, Berkeley, Au-
  gust 1986.
- Honorary doctor, Université de Franche-Comté, Besançon, 1995.
- Kloosterman-lecturer at the University of Leiden, 1995.

It is difficult not to compare this with Johann Bernoulli. In 1695, Johann
Bernoulli was appointed professor at the University of Groningen. He was 28
at the time. More mathematicians with the name Bernoulli are known. There
is an elder brother Jacob Bernoulli. Another famous Bernoulli is Daniel. He
was the son of Johann, born in Groningen in 1700. Johann and Jacob worked
together at the development of the differential and integral calculus. This
cooporation did not last. Johann had, in the words of Jan van Maanen, his
"dark sides". The quarrels of Johann with his brother Jacob, his son Daniel
and many others scientists are well known. We will see later that in the Lenstra
family there is also scientific cooperation. However, the dark sides of Johann
have no counterpart in the Lenstra family.

In the sequel we give a kaleidoscopic impression of Hendrik's scientific work.
The aim is not to give a full scientific report but to interest a general mathema-
tical public.

1. THE EMMY NOETHER PROBLEM
As usual $\mathbb{Q}$ denotes the field of rational numbers. Let $x_1, \ldots, x_n$ be variables.
The field $K := \mathbb{Q}(x_1, \ldots, x_n)$ of rational functions in $x_1, \ldots, x_n$ consists of all
fractions $R(x_1, \ldots, x_n) = \frac{f}{g}$ with $g \neq 0$ and $f, g$ polynomials in $x_1, \ldots, x_n$ with
coefficients in $\mathbb{Q}$. Let $L$ consist of the elements of $K$ which are invariant under
cyclic permutation of the variables. An expression $R(x_1, x_2, \ldots, x_{n-1}, x_n) \in K$
belongs to $L$ precisely when

$$R(x_2, x_3, \ldots, x_n, x_1) = R(x_1, x_2, \ldots, x_{n-1}, x_n)$$

holds.

A very special case of Emmy Noether's problem is:

Are there invariants $y_1, \ldots, y_n$ (i.e. elements in $L$) such that every invari-
ant is a rational expression in $y_1, \ldots, y_n$ (i.e. such that $L = \mathbb{Q}(y_1, \ldots, y_n)$)?
For \( n = 2 \) the answer is positive. Indeed, \( y_1 = x_1 + x_2; y_2 = x_1x_2 \) have the required properties. The first negative answer was found by R.G. Swan in 1969 for \( n = 47 \). For the formulation of Lenstra’s solution we have to introduce some notation. Let \( m > 2 \) be an integer. Write \( \mathbb{Z}_m \) for \( \mathbb{Z}[\zeta_m] = \mathbb{Z}[e^{2\pi i/m}] \). By \( \mathbb{Z}[\zeta_m] \) we mean the subset of \( \mathbb{C} \) consisting of the expressions \( \alpha = a_0 + a_1\zeta_m + \ldots + a_\ell \zeta_m^\ell \), where \( \ell \) and \( a_0, \ldots, a_\ell \) are integers. The conjugates of \( \alpha \) are the expressions \( a_0 + a_1\zeta_m + \ldots + a_\ell \zeta_m^\ell \) where \( \ell \) is an integer with \( 1 \leq \ell < m \) and \( \gcd(c, m) = 1 \). The norm \( N(\alpha) \) of \( \alpha \) is the product of all the conjugates of \( \alpha \). This norm is a non-negative integer. Further \( N(\alpha) = 0 \) if and only if \( \alpha = 0 \). For \( m = 4 \) the set \( \mathbb{Z}[\zeta_4] \) consists of the expressions \( a + bi \) with \( a, b \) integers. The norm of \( a + bi \) is the integer \( a^2 + b^2 \). The solution given by Lenstra can be formulated as follows.

**Invariants** \( y_1, \ldots, y_n \) such that every invariant is a rational expression in \( y_1, \ldots, y_n \), exist if and only if the following two conditions are satisfied:

1. the integer \( n \) is not divisible by 8.
2. for every divisor \( q \) of \( n \) of the form \( q = p^s \), with \( p \) an odd prime and \( s \) a positive integer, there is an element in \( \mathbb{Z}[\zeta_{p^s}] \) with norm \( p \). Here \( \phi(q) = p^{s-1}(p-1) \).

Algebraic number theory is used to decide whether an integer \( n \) satisfies condition (2). The first integer for which the problem has a negative answer turns out to be \( n = 8 \).

We briefly discuss the general problem. Let \( k \) be a field and let \( x_1, \ldots, x_n \) denote variables. The group \( S_n \) permutes \( \{x_1, \ldots, x_n\} \) and acts on the field \( K = k(x_1, \ldots, x_n) \). For a subgroup \( G \) of \( S_n \) one can consider the field \( K^G \) of all elements which are invariant under \( G \). In connection with the inverse problem of Galois theory, Emmy Noether raised the question whether \( K^G \) is again a purely transcendental extension of \( k \) (i.e. \( K^G = k(y_1, \ldots, y_n) \) for algebraically independent \( y_1, \ldots, y_n \)).

For the group \( G = S_n \) the answer is positive; for the \( y_1, \ldots, y_n \) one can take the elementary symmetric functions in the \( x_1, \ldots, x_n \). An old result of E. Fischer gives a positive answer for an abelian group over a base field \( k \) which has sufficiently many roots of unity. Hendrik solved the question of Emmy Noether for any abelian group and any base field \( k \). (See [1]).

2. **Norm-Euclidean rings**

A number field \( K \) is a subfield of the field of complex numbers of the form \( \mathbb{Q}(\alpha) \) where \( \alpha \) is some algebraic number. The degree \( n \) of \( \alpha \) (and of \( K \)) is the degree of the irreducible polynomial which has \( \alpha \) as zero. The field \( \mathbb{Q}(\alpha) \) consists of all expressions \( a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \) with \( a_0, \ldots, a_{n-1} \in \mathbb{Q} \). For an element \( \rho \) of \( K \) one defines the norm \( N(\rho) \) as the absolute value of the product of all conjugates of \( \rho \). The field \( K \) can be considered as a vector space over \( \mathbb{Q} \) of dimension \( n \). An element \( \rho \) of \( K \) is called integral if there is a relation of the form

\[ \rho^n + b_2\rho^{n-1} + \ldots + b_1\rho + b_0 = 0 \]

with all \( b_i \in \mathbb{Z} \).
The integral elements form a subring $R$ of $K$. The set $R$ can be seen as a lattice in the $n$-dimensional vector space $K$ over $\mathbb{Q}$. The norm of an element $\beta$ of $R$ is always an integer. The ring $R$ (and the field $K$) is said to be \textit{norm-Euclidean} if for every pair of elements $\beta$ and $\gamma$ of $R$, with $\gamma \neq 0$, it is possible to find a quotient $\kappa$ and a remainder $\rho$, both belonging to $R$, so that

$$\beta = \kappa\gamma + \rho \quad \text{and} \quad N(\rho) < N(\gamma).$$

The problem is to find number fields which are norm-Euclidean. It turns out that $R$ is norm-Euclidean if and only if for every $\xi \in K$ we can find a $\kappa$ in $R$ such that $N(\xi - \kappa) < 1$. One can use this to give a geometric formulation of the problem. Let $V$ denote the subset of $K$ consisting of the elements of norm less than one. Then $K$ is norm-Euclidean if and only if $K = \cup_{\kappa \in R}(\kappa + V)$. See Figure 1.

\begin{figure}
\includegraphics[width=\textwidth]{figure1}
\caption{This illustration shows a portion of the ring $R = \{a + b\theta$ and $b$ integers $\}$ with $\theta^2 - \theta - 1 = 0$, embedded in $\mathbb{R} \times \mathbb{R}$ by mapping $a + b\theta$ to $((a+b(1+\sqrt{5})/2, a+b(1-\sqrt{5})/2).$ The hyperbolas bound the region $V$ consisting of points of norm less than one. The elements of $R$ lying on the hyperbolas are units of the ring. The shaded region is a parallelepiped. The small part of this parallelepiped not contained in $V$ is easily seen to be contained in $1 + V$. It follows from this that the ring $R$ is norm-euclidean.

With this criterion Lenstra found many norm-Euclidean number fields. In particular, he discovered norm-Euclidean number fields of large degree (See [3]). For more details we refer to the excellent surveys [6,8].}
3. ARTIN'S CONJECTURE AND EUCLIDEAN RINGS

Let \( t \) be an integer with \( |t| > 1 \) and let \( p \) be a prime number. Then \( t \) is called a primitive root modulo \( p \) if every integer \( a \) with \( 1 \leq a \leq p - 1 \) is congruent, modulo \( p \), to a number of the shape \( t^j \), with \( j \) an integer, \( j \geq 0 \). Artin conjectured that the limit

\[
\lim_{x \to \infty} \frac{\text{number of primes } < x \text{ which have } t \text{ as a primitive root}}{\text{number of primes } < x}
\]

exists. Lenstra extended this conjecture to number fields and gave a proof of this extended version under assumptions which are called generalized Riemann hypotheses.

Lenstra applied the extended version of the Artin conjecture to classify Euclidean "number rings". We will briefly explain this and we refer to [5] and [9] for more details.

Again \( K \) is a number field and \( R \) is its subring of integral elements. In order to formulate the classification we have to introduce the set of prime divisors of \( K \). An archimedean prime divisor of \( K \) is an absolute value on \( K \) obtained by an embedding of \( K \) into \( \mathbb{R} \) or \( \mathbb{C} \). The (finite) set of archimedean prime divisors is denoted by \( S_\infty \). A non-archimedean prime divisor \( \text{ord}_p \) is associated with a maximal ideal \( p \) of \( R \). One first defines \( \text{ord}_p \) as a map from \( R \setminus \{0\} \to \mathbb{Z} \). The value \( n = \text{ord}_p(x) \) is the largest integer such that \( x \in p^n \). Then one extends \( \text{ord}_p \) to \( K \setminus \{0\} \) by \( \text{ord}_p(f/g) = \text{ord}_p(f) - \text{ord}_p(g) \). Finally, one extends \( \text{ord}_p \) to \( K \) by putting \( \text{ord}_p(0) = \infty \). For the field of rational numbers, \( S_\infty \) consists of one element corresponding to the inclusion \( \mathbb{Q} \subseteq \mathbb{R} \). The set of non-archimedean prime divisors of \( \mathbb{Q} \) can be identified with the set of prime numbers.

A number ring will be a ring of the type \( R_S \) where \( S \) is a set of prime divisors of \( K \) containing \( S_\infty \) and where

\[
R_S = \{ x \in K | \text{ord}_p(x) \geq 0 \text{ for all } p \notin S \}.
\]

A number ring \( R_S \) is called Euclidean if there is a map \( \psi : R_S \setminus \{0\} \to \mathbb{Z}_{\geq 0} \) such that for all \( b, c \in R_S \), \( c \neq 0 \), there exist \( q, r \in R_S \) with

\[
b = qc + r, \text{ with } r = 0 \text{ or } \psi(r) < \psi(c).
\]

A main tool is the following: if \( R_S \) is Euclidean then there is a smallest Euclidean algorithm \( \psi \). (See Figure 2). We note that a Euclidean ring is a unique factorization ring. Lenstra's classification (see [5]) of the Euclidean number rings is the following:

The Euclidean number rings \( R_S \) with \( \#S = 1 \) are:

\[
\mathbb{Z}; \mathbb{Z}(1 + \sqrt{-3})/2; \mathbb{Z}(\sqrt{-1}); \mathbb{Z}(1 + \sqrt{-7})/2; \mathbb{Z}(\sqrt{-2}); \mathbb{Z}(1 + \sqrt{-11})/2
\]

If \( R_S \) has unique factorization and \( \#S \geq 2 \) then (under some generalized Riemann hypotheses) \( R_S \) is Euclidean.
Figure 2. The smallest division algorithm on the ring $\mathbb{Z}[\rho] = \{a + b\rho : a \text{ and } b \text{ are integers}\}$, where $\rho = (-1 + \sqrt{-3})/2$ is a primitive cube root of unity. The ring is a triangular lattice in the complex plane, and the points of the lattice are the centers of a regular hexagonal tiling of the plane. The black hexagons in the picture correspond to the elements $\alpha$ of $\mathbb{Z}[\rho]$ for which $\alpha = 0$ or $\psi(\alpha) = 1$, 3 or 5.

4. The LLL Algorithm
A lattice $L$ in the Euclidean space $\mathbb{R}^n$ is a subset of the shape
\[ \{m_1b_1 + \ldots + m_nb_n \mid m_1, \ldots, m_n \in \mathbb{Z}\} \] where $b_1, \ldots, b_n$ is a basis of $\mathbb{R}^n$.

The set $\{b_1, \ldots, b_n\}$ is called a $Z$ basis of $L$. Among all the $Z$ bases of $L$, some are better than others. The ones whose elements are the shortest are called reduced. A reduced basis is not far from being orthogonal. In connection with “integer programming”, H.W. Lenstra introduced basis reduction of a lattice. An improvement of basis reduction was given by L. Lovász. The well known paper [14], by A.K. Lenstra, H.W. Lenstra and L. Lovász, gives the new definition of reduced basis and a reduction algorithm which is deterministic and works in polynomial time. This algorithm is now called LLL-reduction. The application of basis reduction to the construction of a polynomial-time algorithm for factoring polynomials with rational coefficients is due to A.K. Lenstra. The LLL-reduction has nowadays a wide range of applications.
5. INTEGER PROGRAMMING
The problem can be formulated as follows. Let n and m be positive integers
and let real n-vectors \(a_i\) and real numbers \(b_i\) be given for \(i = 1, 2, \ldots, m\). The
problem is to decide whether or not there exists an n-vector \(x\) with integral
coordinates satisfying the inequalities
\[ a_i x \leq b_i \text{ for } i = 1, 2, \ldots, m. \]
One assumes (without loss of generality) that the \(b_i\) and the coordinates of
the \(a_i\) are integers. The problem is formulated as a decision problem. As a
variation of the problem one may ask for an actual solution \(x\) (if such a solution
exists). This does not change the complexity of the problem. It is not likely
that a polynomial time algorithm for the problem exists since the problem is
known to be NP-complete.
It is rather surprising that Lenstra came up with an algorithm for integer pro-
gramming which is for any fixed n polynomial time. That special cryptosystems
can be broken with the use of Lenstra’s algorithm was noticed by A. Shamir.
There is also a link with the LLL-reduction. We refer to [15,18] for a more
complete discussion of the geometry behind the algorithm and for the confusion
caused by Lenstra’s algorithm.

6. ELLIPTIC CURVES
Lenstra has developed a wide variety of methods for producing large prime
numbers, for testing whether certain numbers are prime and for factoring large
integers. The elliptic curve method or ECM, invented by Lenstra in 1985 (see [21]), is one of the three leading methods for factoring integers. (The other
two are the quadratic sieve and the number field sieve). Lenstra’s student R.
Schoof inspired the use of elliptic curves for factoring integers.
Roughly speaking, an elliptic curve is the zero set of an equation of the form
\[ y^2 = x^3 + ax + b. \]
The points of an elliptic curve \(E\) over any ring or field form a group. The group structure is derived from the geometry of the curve. The
next picture describes the situation for the real points of an elliptic curve.
The idea of ECM is the following.

Let \(N\) be the number that we want to factor. We suppose that \(N\) has no
small prime divisors and that \(N\) is composite. An “elliptic curve” \(E\) over \(\mathbb{Z}/N\mathbb{Z}\)
is a pair of elements \(a, b \in \mathbb{Z}/N\mathbb{Z}\) such that \(4a^3 + 27b^2\) is invertible modulo \(N\).
As a projective curve over \(\mathbb{Z}/N\mathbb{Z}\) one defines \(E\) by the homogeneous equation
\[ Y^2T = X^3 + aXT^2 + bT^3. \]
The set of points \(E(\mathbb{Z}/N\mathbb{Z})\) of \(E\) with coordinates
in \(\mathbb{Z}/N\mathbb{Z}\), consists of the equivalence classes of the triples \((x : y : t)\) with
\(\gcd(x, y, t, N) = 1\) and \(y^2t = x^3 + axt^2 + bt^3\). This set is a union
\[ E(\mathbb{Z}/N\mathbb{Z}) = E^{\text{Aff}} \cup \{(0 : 1 : 0)\} \cup E^s, \]
where \(E^{\text{Aff}}\) denotes the elements with \(t\) invertible mod \(N\) and where \(E^s\) denote the
triples where \(t\) is not invertible mod \(N\) and is not 0 mod \(N\).
Of course \(E^s\) is empty if \(N\) were prime. The geometry of \(E\) defines for any \(N\)
a group law on \(E(\mathbb{Z}/N\mathbb{Z})\). Starting with elements in \(E^{\text{Aff}}\) one hopes to find
an addition with answer in $E^*$. If this is successful then a decomposition of $N$ is found.

For a point $Q \in E^{\text{Aff}}$ we will write $[k]Q$ for the sum $Q \oplus Q \oplus \ldots \oplus Q$ ($k$ times) on $E$. Let $p$ be a prime divisor of $N$. There is a natural map $E(\mathbb{Z}/N\mathbb{Z}) \to E(\mathbb{Z}/p\mathbb{Z})$. If $m$ is a multiple of the order of $E(\mathbb{Z}/p\mathbb{Z})$ then the image of $[m]Q = (x : y : t)$ is $(0 : 1 : 0) \in E(\mathbb{Z}/p\mathbb{Z})$. This means that $t$ is not invertible mod $N$ and that $\gcd(t, N)$ gives a divisor of $N$ if $t \neq 0 \mod N$. If the order of $E(\mathbb{Z}/p\mathbb{Z})$ has small divisors $d$ then one might hope that $[d]Q$ already lies in $E^*$. If one specifies the size of the prime divisors $p$ of $N$ that one wants to find, then the Hasse inequality and the group structure of $E(\mathbb{Z}/p\mathbb{Z})$ lead to a certain bound $B$. For some $m$, such that every prime power $q$ with $q|m$ satisfies $q \leq B$, one expects to find a $[m]Q \in E^*$. This leads to computing $[\text{lcm}(1, 2, \ldots, c)]Q$ for increasing $1 < c \leq B$ and to try (from time to time) whether $[\text{lcm}(1, 2, \ldots, c)]Q \in E^*$. If after a reasonable time no solution is found then one continues with another elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ with an affine point.
on it.

On the basis of work of S. Goldwasser and J. Kilian, a powerful "elliptic curve test" was developed by Lenstra. For an integer $N$, which is suspected to be prime, elliptic curves $E$ over $\mathbb{Z}/N\mathbb{Z}$ are used to give a proof of primality. In 1987, A.K. LENSTRA en H.W. LENSTRA described a practical way, due to R. Schoof, to calculate the order of $E(\mathbb{Z}/N\mathbb{Z})$ for prime numbers $N$. This is an important ingredient of the "elliptic curve test".

7. The number field sieve
Recent work of Arjen Lenstra and Hendrik Lenstra concerns the number field sieve. ([28,29]). The word sieve denotes a method which finds in a given set of (say) numbers the special elements (say prime numbers) that one wants to obtain. The goal is to factor an integer $n$, which is suspected to be composite. The method is very well explained in [30]. In what follows we have borrowed from that paper.

Suppose that one has found integers $x,y$ giving a non trivial solution of the equation $x^2 \equiv y^2 \mod n$. Then one obtains a factorization of $n$ by finding the greatest common divisor of $x-y$ and $n$. The number field sieve tries to find such solutions by producing:

1. A monic irreducible polynomial $f \in \mathbb{Z}[X]$ of degree $d > 1$. One writes $\alpha$ for a complex root of $f$. Then $\mathbb{Z}[\alpha] \subset \mathbb{C}$ is the same thing as the ring $\mathbb{Z}[X]/f\mathbb{Z}[X]$.

2. An integer $m$ with $f(m) \equiv 0 \mod n$.

3. A non-empty set $S$ of pairs $(a, b)$ of relatively prime integers with the following properties:

\[ \prod_{(a,b) \in S} (a + bm) \text{ is a square in } \mathbb{Z}, \]

\[ \prod_{(a,b) \in S} (a + ba) \text{ is a square in } \mathbb{Z}[\alpha]. \]

4. An element $\beta$ in (the integral closure of $\alpha$) $\mathbb{Z}[\alpha]$ with $\beta^2 = \prod_{(a,b) \in S} (a + ba)$

The ring $\mathbb{Z}[\alpha]$ is mapped to $\mathbb{Z}/n\mathbb{Z}$ by

\[ \sum_i a_i \alpha^i \mapsto \phi(\sum_i a_i \alpha^i) := \sum_i a_i m^i \mod n. \]

Let $x \in \mathbb{Z}$ satisfy $x^2 = \prod_{(a,b) \in S} (a + bm)$ and let $y \in \mathbb{Z}$ be such that $\phi(\beta) \equiv y \mod n$. Then the pair $(x, y)$ is a candidate for a non trivial solution of $x^2 \equiv y^2 \mod n$.

The algorithm for finding $f$ and $m$ is quite simple. One fixes an integer $d > 1$ such that $n > 2^d$. Set $m = [n^{1/d}]$, and write $n$ to the basis $m$:
Figure 4. This picture, designed by Hendrik Lenstra, illustrates the number field sieve. The schemes $\text{Spec}(\mathbb{Z})$ and $\text{Spec}(\mathbb{Z}[\alpha])$ are embedded in the affine plane $\text{Spec}(\mathbb{Z}[x])$. Their intersection is the scheme $\text{Spec}(\mathbb{Z}/n\mathbb{Z})$. The positive integer $n$ is supposed to be the product of the primes $p$ and $q$ and so $\text{Spec}(\mathbb{Z}/n\mathbb{Z})$ consists of two points. For a suitable choice of $\alpha$, one tries to remove one of the points of intersection. If this is successful then the decomposition $n = pq$ is found.

$$n = c_d m^d + c_{d-1} m^{d-1} + \ldots + c_0$$

where the digits $c_i$ satisfy, as usual, the inequality $0 \leq c_i < m$. It is easily seen that $c_d = 1$. Let $f = X^d + c_{d-1} X^{d-1} + \ldots + c_1 X + c_0$. If $f$ happens to be reducible then a factorization of $n$ is found. If $f$ is irreducible then $f$ and $m$ satisfy the requirement $f(m) \equiv 0 \pmod{n}$.

Finding a set $S$ with the prescribed properties is the heart of the number field sieve. The set $S$ is indeed found by sieving in a large class of coprime pairs $(a, b)$. Finding the square root $\beta$ of an element of (the integral closure of) $\mathbb{Z}[\alpha]$ is another non-trivial part of the algorithm. See Figure 4.

A.K. Lenstra and M.S. Manasse (see [31]) successfully applied the number field sieve for the factorization of the ninth Fermat number $F_9 := 2^{2^9} + 1 = 2^{512} + 1 = 1340780994259709957402499820584612747846882059293377723561443$

$721764030073546976801874298166903427690031858186486050585375388281$

$19465994643364900060804097$

The three prime factors have respectively 7, 49 and 99 digits. The 7-digit factor was of course already known.
8. Wiles, Taylor and Fermat
A major issue in the proof of Wiles and Taylor-Wiles of Fermat’s last theorem is to establish that a morphism between a universal deformation ring \( R \) and a certain Hecke ring \( T \) is in fact an isomorphism. Wiles has given a criterion which allows one to draw this conclusion. Lenstra’s contribution ([33]) has been to analyze the relation between complete intersections and Gorenstein rings. This led to an important simplification in the proof that \( T \) is a complete intersection. Another input for Wiles’ proof of Fermat’s last theorem is Lenstra’s joint paper [24].

9. Abelian varieties
Lenstra has written several papers on Abelian varieties. A well known paper is the joint work [19], written with F. Oort. The formulation of the main result requires some specialized algebraic geometry. Nevertheless we give here the main result.

Let \( A \) be an Abelian variety of dimension \( g \) over a field \( K \). Let \( v \) be a discrete valuation on \( K \). Suppose that \( A \) has purely additive reduction at \( v \). For every prime \( l \), different from the residue characteristic, one defines \( b(l) \) by \( \sup_{N \geq 0} \# A[N]^{\times}(K) = l^{b(l)} \). Then every \( b(l) \) is finite and \( \sum(l - 1)b(l) \leq 2g \).

For elliptic curves, i.e. \( g = 1 \), this result was already known from the classification of elliptic curves. The proof of the main result does not use specific classification, but relies on monodromy arguments.

A selected list of publications of H.W. Lenstra, Jr.
Ser. 56, 1982.
15. Integer programming with a fixed number of variables, Mat. Oper. Res. 8, 538–548, 1983.