Continued Fractions and Factoring

Michele Elia - Politecnico di Torino

De Cyfris Augustae Taurinorum

Torino, December 6th, 2019

Outline of the presentation

1. Fermat, the equation $p = x^2 + y^2$, and Legendre
2. Properties of continued fractions
3. Convergents, quadratic forms
   Periodicity and Symmetry
4. Units in real quadratic fields and Factoring
5. Shanks and Dirichlet
6. Conclusions

Fermat (1607-1665)

In a letter to **Pierre de Carcavi**, August 14^{th}, 1659, **Pierre de Fermat** reported several propositions, in particular

Teorema (Fermat)

Every prime p of the form $4k+1$ is uniquely expressible as a sum of two squares, i.e.

$$p = X^2 + Y^2 \quad \Leftrightarrow \quad p \equiv 1 \bmod 4 \tag{1}$$

Computation of X and Y in equation (1)

Two challenges were implicit in Fermat's problem

1. Prove Fermat statement
2. For all primes $p \equiv 1 \bmod 4$, compute explicitly the positive integers X and Y such that

$$p = X^2 + Y^2 \quad .$$

When a solution exists, it is obtained checking every possibility, using a O($\sqrt{p}$) arithmetical operations:

Write $Y = \sqrt{p - X^2}$ and check every integer $X < \sqrt{p}$ until Y is found.

When $N = 1 + n^2$, only one chack is needed, for example $N = 152415222070337 =$

Computation of X and Y in equation (1)

Two challenges were implicit in Fermat's problem

1. Prove Fermat statement
2. For all primes $p \equiv 1 \bmod 4$, compute explicitly the positive integers X and Y such that

$$p = X^2 + Y^2 \quad .$$

When a solution exists, it is obtained checking every possibility, using a $\mathbf{O}(\sqrt{p})$ arithmetical operations:

Write $Y = \sqrt{p - X^2}$ and check every integer $X < \sqrt{p}$ until Y is found.

When $N = 1 + n^2$, only one chack is needed, for example $N = 152415222070337 = 1 + 12345656^2$

Proof of Theorem (fermat) - **Euler (1707-1783)** (**constructive proof**)

Probably the first proof of Fermat proposition is due to Euler (1749), and uses Fermat's *infinite descent*.

- The equation $X^2 + Y^2 = p$ implies the modular equation $x^2 + 1 = 0 \pmod p$, which has a solution $|x_0| < \frac{p}{2}$ by the little Fermat's theorem,
  i.e. $x^{p-1} = 1 \pmod p$, and $p = 4k + 1$.
- $x_0^2 + 1 = s_0\, p$ with $s_0 < \frac{p}{2}$
- Setting $x_1 = x_0 \pmod{s_0}$ and $x_2 = 1 \pmod{s_0}$, we have

$$x_1^2 + x_2^2 \pmod{s_0} = x_0^2 + 1 \pmod{s_0} = 0 \Rightarrow x_1^2 + x_2^2 = s_0 s_1$$

with $s_1 < \frac{s_0}{2}$.

Proof (cont.)

- Multiplying $s_0 p$ by $s_0 s_1$, and using an identity already known to Diophantus, we have

$$s_0^2 s_1 p = (x_1^2 + x_2^2)(x_0^2 + 1) = (x_0 x_2 - x_1)^2 + (x_0\ x_1 + x_2)^2 \quad (2)$$

- Since $x_0 x_2 = x_1 \pmod{s_0}$ by definition of x_1 e x_2, we have $s_0 | (x_0 x_2 - x_1)$, thus dividing (2) by s_0^2
- $$s_1 p = \left(\frac{x_0 x_2 - x_1}{s_0}\right)^2 + \left(\frac{x_0\ x_1 + x_2}{s_0}\right)^2$$
  the rightest term is necessarily an integer.
  The first step of the *infinite descent* is complete.
- Iterating, the process a sequence of positive decreasing terms is produced

$$s_0 > s_1 > s_2 \cdots > 1$$

which necessarily ends with 1.

One sentence proof (Zagier's proof) (non constructive)

Consider a prime $p = 4k + 1$, and define the finite set of triples $\mathcal{T} = \{(x, y, z) \in \mathbb{Z}_+^3 : x^2 + 4yz = p\}$ which has two involutions

1. The first involution is

$$(x, y, z) \to (x, z, y) \quad \text{and fixes } (x, y, y)) \quad .$$

2. The second involution has a more complex definition

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z) & \text{if} \quad x < y - z \\ (2y - x, y, x - y + z) & \text{if} \quad y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if} \quad x > 2y \end{cases} ,$$

and has the unique fixed point $(1, 1, k) \in \mathcal{T}$.
Since involutions on the same finite set must have a number of fixed points with the same parity, if follows that $(x, y, y) \in \mathcal{T}$, i.e. $x^2 + (2y)^2 = p$ necessarily has a solution.

Constructive proofs

The problem of effectively computing a solution to $X^2 + Y^2 = p$ $(p = 4k + 1)$ was considered by many authors in different times.

1. Gauss (1825) gave two ways, the first is direct

$$x = \frac{(2k)!}{2(k!)^2} \bmod p \quad , \quad y = \frac{((2k)!)^2}{2(k!)^2} \bmod p \quad .$$

   the second is based on quadratic forms of discriminant -4

$$p \to pX^2 + 2b_1XY + \frac{b_1^2+1}{p}Y^2 \to x^2 + y^2$$

   where b_1 is a root of $z^2 + 1$ modulo p.

2. Jacobsthal (1906) solution is based on the sum

$$S(a) = \sum_{n=1}^{p-1} \left(\frac{n(n^2-a)}{p} \right) \Rightarrow x = \frac{1}{2}S(QR) \quad , \quad y = \frac{1}{2}S(QN)$$

   where $QR, QN \in \mathbb{Z}_p$ such that $(QR \mid p) = 1$ and $(QS \mid p) = -1$.

Constructive proofs (cont.)

1. Legendre (1808) (pages 59-60 of *Essai sur la Théorie des Nombres*) showed, using the continued fraction expansion of $\sqrt{p}$, that the convergent $\frac{p_m}{q_m}$ with $m = \frac{\tau-1}{2}$ yields

$$X = p_m^2 - N q_m^2 \quad (= \Delta_m) \qquad , \qquad Y = \sqrt{N - X^2}$$

   It is noted that Y may also be computed from the convergents as

$$Y = p_m p_{m-1} - N q_m q_{m-1} \quad (= \Omega_m).$$

2. The Legendre finding is a consequence of the palindromic character of the quotient sequence $a_1, \ldots, a_{\tau-1}$

Legendre own words

... Donc tous le fois que l'équation $x^2 - Ay^2 = -1$ *est résoluble (ce qui ha lieu entre autre cas lorsque* A *est un numbre premier* $4n+1$*) le nombre* A *peut toujours être decomposé en deux quarrés; et cette décomposition est donnée immediatement par lo quotient-complet* $\frac{\sqrt{A}+I}{D}$ *qui répond au second des quotients moyens compris dans la première période du développement de* $\sqrt{A}$*; le nombres* I *et* D *étant ainsi connu, on aura*
$A = D^2 + I^2$*.*

Cette conclusion ranferme un des plus beaux théorèmes de la science des nombres, savoir, *que tout nombre premier* $4n+1$ *est la somme de deux quarrés;* elle donne en même temps le moyen de faire cette décomposition d'une manière directe et sans aucun **tâtonnement**.

Example

Consider $N = 149$, the period of the continued fraction of $\sqrt{149}$ is 9,

j	Δ_j	Ω_j
0	-5	8
1	17	-8
2	-4	9
3	7	-11
4	**-7**	**10**
5	4	-11
6	-17	9
7	5	-8
8	-1	12
9	5	-12
10	-7	11

In position 4 we find $\mathbf{-7}$ and **10**, i.e. $7^2 + 10^2 = 149$.

The Problem

A question is naturally suggested by the tricky property that Legendre discovered when the continued fraction expansion of $\sqrt{N}$ has **odd** period:

What happens when the continued fraction expansion of $\sqrt{N}$ has even period?

Continued Fractions

Simple continued fractions ($a_i > 0$, $i > 0$, $a_i \in \mathbb{N}$) are expressions of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \quad , \tag{3}$$

where the a_is are called quotients. The (simple) continued fractions may be finite or infinite. Infinite continued fraction are periodic when a finite pattern of quotients repeats indefinitely. Periodic continued fractions are compactly written in the form

$$\alpha = [b_0, \ldots, b_k, \overline{a_1, a_2, \ldots, a_{\tau-1}, a_\tau}] \quad , \tag{4}$$

where the period of length τ is over-lined, and the pre-period is evidenced in red.

Continued Fractions - Lagrange (1736-1813)

If N is a positive non-square integer, we have

$$\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]$$

where the first $\tau - 1$ terms of the period are a palindrome.

Theorem (Nouv. Mem. Acad. R. Berlin 1769/70)

A number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ is a quadratic irrational (i.e. $\alpha = \frac{a+b\sqrt{N}}{c}$) if and only if its continued fraction expansion is periodic.

Examples

Let τ denote the period.

$$\sqrt{91} = [9, \overline{1, 1, 5, 1, 5, 1, 1, 18}\,] \qquad \tau = 8$$

A continued fraction is said **purely periodic** if the pre-period is missing.

$$\frac{5+\sqrt{91}}{8} = [\,\overline{1, 1, 4, 2, 10, 2, 4, 1, 1, 1, 1, 3, 4, 1, 4, 3, 1, 1}\,] \quad \tau = 18$$

$$\sqrt{89} = [9, \overline{2, 3, 3, 2, 18}\,] \qquad \tau = 5$$

$$\frac{9+\sqrt{89}}{8} = [\,\overline{2, 3, 3, 2, 18}\,] \qquad \tau = 5$$

$$\frac{5+\sqrt{89}}{8} = [\,\overline{1, 1, 4, 9, 4, 1, 1}\,] \qquad \tau = 7 \quad .$$

Galois (1811-1832)

A quadratic irrational α is said to be **reduced** if $\alpha > 1$ and its conjugate α' lies in the interval $-1 < \alpha' < 0$. (Steuding p.75-78).

Theorem (Annals de Gergonne,1829)

The continued fraction expansion of a quadratic irrational number α is purely periodic if and only if α is reduced. In this case for the conjugate α' of

$$\alpha = [\overline{a_0, a_1, a_2, \ldots, a_{\tau-2}, a_{\tau-1}}]$$

we have

$$-\frac{1}{\alpha'} = [\overline{a_{\tau-1}, a_{\tau-2}, \ldots, a_1, a_0}] \tag{5}$$

(cont.) A Corollary

Given $p = 1 \bmod 4$ prime, then $p = Q_m^2 + P_m^2$, $Q_m < P_m$. Consider $\alpha = \frac{Q_m + \sqrt{p}}{P_m} \in \mathbb{Q}(\sqrt{p})$, we have $\alpha > 1$ and $\alpha' = \frac{Q_m - \sqrt{p}}{P_m} \in]-1,\ 0[$, thus by the theorem of Galois the continued fraction expansion of α is purely periodic

Since $\alpha\alpha' = -1$, the period turns out to be palindromic.

Example. Consider $N = 89 = 5^2 + 8^2$, we have

$$\sqrt{89} \Rightarrow [[9], [2, 3, 3, 2, 18]]$$

$$\alpha = \frac{5 + \sqrt{89}}{8} \Rightarrow [\overline{1, 1, 4, 9, 4, 1, 1}] \Leftarrow -\frac{1}{\alpha'}$$

The continued fraction of $\sqrt{N}$

Let $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_{\tau-1}, a_\tau}]$, the m-convergent is the fraction obtained considering only the first m terms.
The sequence of convergents is

$$\frac{p_0}{q_0} = \frac{a_0}{1} \ , \ \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1} \ , \ \cdots \ , \ \frac{p_j}{q_j} = \frac{a_j p_{j-1} + p_{j-2}}{a_j q_{j-1} + q_{j-2}} \ , \ \cdots$$

Two sequences $\mathbf{\Delta} = \{\Delta_j\}_{j=1}^{\infty}$ and $\mathbf{\Omega} = \{\Omega_j\}_{j=1}^{\infty}$ are defined as

$$\begin{cases} \Delta_j = p_j^2 - N q_j^2 \\ \Omega_j = p_j p_{j-1} - N q_j q_{j-1} \\ \\ \Omega_j^2 - \Delta_j \Delta_{j-1} = N \end{cases} \qquad j = 1, 2, \ldots$$

$$\Delta_{\tau-1} = (-1)^{\tau}$$

(cont.)

1. Let c_n and r_n be the elements of two sequences of positive integers defined by the relation

$$\frac{\sqrt{N}+c_n}{r_n} = a_{n+1} + \frac{r_{n+1}}{\sqrt{N}+c_{n+1}}$$

with $c_0 = \left\lfloor \sqrt{N} \right\rfloor$, and $r_0 = N - a_0^2$; the elements of the sequence $a_1, a_2, \ldots, a_n \ldots$ are thus obtained as the integer parts of the left-side fraction

$$a_{n+1} = \left\lfloor \frac{\sqrt{N}+c_n}{r_n} \right\rfloor = \left\lfloor \frac{c_0+c_n}{r_n} \right\rfloor \quad . \tag{6}$$

(cont.)

1. Let $a_0 = \lfloor \sqrt{N} \rfloor$, the sequences $\{c_n\}_{n\geq 0}$ and $\{r_n\}_{n\geq 0}$ are produced by the recursions

$$\begin{aligned} a_{m+1} &= \left\lfloor \frac{a_0 + c_m}{r_m} \right\rfloor \\ c_{m+1} &= a_{m+1} r_m - c_m \\ r_{m+1} &= \frac{N - c_{m+1}^2}{r_m} \quad . \end{aligned} \tag{7}$$

   These recursive equations allow us to compute the sequence $\{a_m\}_{m\geq 1}$ using only rational arithmetical operations

2. $$c_{m+1} = |\Omega_m| \quad , \quad r_{m+1} = |\Delta_m| \quad .$$

(cont.) Periodic sequences

Theorem

Let $N \in \mathbb{Z}^+$ be square-free, then:

The sequence $\mathbf{\Delta} = \{\Delta_1, \Delta_2, \cdots, \Delta_{\tau-1}, \Delta_\tau, \cdots\}$ *is periodic with period* τ*, or* 2τ *if* τ *is odd. The first* $\tau - 3$ *terms of a period satisfy the condition of symmetry* $\Delta_m = (-1)^\tau \Delta_{\tau-m-2}$.

The sequence $\mathbf{\Omega} = \{\Omega_1, \Omega_2, \cdots, \Omega_{\tau-1}, \Omega_\tau, \cdots\}$ *is periodic with period* τ*, or* 2τ *if* τ *is odd. The first* $\tau - 2$ *terms of a period satisfy the condition of symmetry* $\Omega_m = -(-1)^\tau \Omega_{\tau-1-m}$.

(cont.)

Theorem

The quadratic forms

$$f_m(X,Y) = \Delta_m X^2 + 2\Omega_m XY + \Delta_{m-1} Y^2 \Leftrightarrow [\Delta_m, 2\Omega_m, \Delta_{m-1}]$$

have discriminant $4N$.

In every period (of length τ *or* 2τ*) the correspondence* $\mathbf{m} \leftrightarrow \mathbf{f_m}$ *is one-to-one.*

Example

$\tau = 10$ even

$$\begin{array}{lcl}
\sqrt{543} & = & [[23],[\,3,\ 3,\ 3,\ 1,14,\ 1,\ 3,\ 3,\ 3,46]] \\
\Delta & & \quad [13,-11,34,-\mathbf{3},34,-11,13,-14,1,-14] \\
\Omega & & \quad [-19,20,-13,21,-21,13,-20,19,-23,23]
\end{array}$$

In position 4 of the period of Δ we find $-\mathbf{3}$, a factor of 543

$\tau = 11$ odd

$$\begin{array}{lcl}
\sqrt{6437} & = & [[80],[4,3,39,1,4,4,1,39,3,4,160]] \\
\Delta & & \quad [49,-4,127,-31,\ \mathbf{31},-127,4,-49,37,-1,37] \\
\Omega & & \quad [-68,79,-77,50,-\mathbf{74},50,-77,79,-68,80,-80]
\end{array}$$

In position 5 of the period we find $\mathbf{31}^2 + (-\mathbf{74})^2 = 6437$

τ odd (a proof of Legendre's yheorem)

Set $m = \frac{\tau-1}{2}$, then $\tau - m - 2 = \frac{\tau-3}{2}$. The symmetry in every period of the sequence $\mathbf{\Delta}$ implies $\Delta_{\frac{\tau-3}{2}} = -\Delta_{\frac{\tau-1}{2}}$, thus the computation of the discriminant of the quadratic form $f_{\frac{\tau-1}{2}}$ lets us to conclude

$$p = \Delta^2_{\frac{\tau-1}{2}} + \Omega^2_{\frac{\tau-1}{2}} \tag{8}$$

What is the complexity for computing $\Delta_{\frac{\tau-1}{2}}$ and $\Omega_{\frac{\tau-1}{2}}$?

τ even - Main theorem (I)

Theorem

Let N be an odd square-free composite integer such that the continued fraction for $\sqrt{N}$ has even period, then

1. *The fundamental unit $\mathfrak{u}$ (or $\mathfrak{u}^3$) in $\mathbb{Q}(\sqrt{N})$ factors $2N$,*
2. *One of the factors of $2N$ can be found in the positions $\frac{\tau-2}{2} + j\tau$, $j = 0, 1, \ldots$ of the infinite periodic sequence $\boldsymbol{\Delta}$.*

Outline of the proof

Consider the j-convergent $\frac{A_j}{B_j}$, and define the column vector $[A_j, B_j]^T$. Since $A_{\tau-1} + B_{\tau-1}\sqrt{N}$ is a unit in $\mathbb{Q}(\sqrt{N})$, the matrix

$$M_{\tau-1} = \begin{bmatrix} -A_{\tau-1} & NB_{\tau-1} \\ -B_{\tau-1} & A_{\tau-1} \end{bmatrix} ,$$

is **involutory**, and has characteristic polynomial $Z^2 - 1$, i.e. eigenvalues ± 1, since the trace is 0 and the determinant $-A_{\tau-1}^2 + NB_{\tau-1}^2 = (-1)^{\tau-1}$, is -1.

With a rather long argument, it can be proved that

$$\begin{bmatrix} A_{\tau-j-2} \\ B_{\tau-j-2} \end{bmatrix} = (-1)^j M_{\tau-1} \begin{bmatrix} A_j \\ B_j \end{bmatrix} . \tag{9}$$

proof (cont.)

When $\tau - \ell - 2 = \ell$, i.e. $\ell = \frac{\tau-2}{2}$, we have two possibilities depending whether ℓ is even or odd

$$A_{\tau-\ell-2} = A_\ell = A \;\text{ e }\; B_{\tau-\ell-2} = B_\ell = B \qquad \text{even } \ell$$

$$A_{\tau-\ell-2} = -A_\ell = -A \;\text{ and }\; B_{\tau-\ell-2} = -B_\ell = -B \qquad \text{odd } \ell$$

Therefore $[A, B]^T$ turns out to be an eigenvector of the matrix $M_{\tau-1}$ with eigenvalue $(-1)^{\frac{\tau-2}{2}}$.

proof (cont.)

Thus, we have that any eigenvector of the matrix $M_{\tau-1}$ is a scalar multiple of $\frac{1}{d}[A_{\tau-1} - (-1)^{\frac{\tau-2}{2}}, B_{\tau-1}]$, where $d = \gcd\{A_{\tau-1} - (-1)^{\frac{\tau-2}{2}}, B_{\tau-1}\}$. Since $\gcd\{A, B\} = 1$, from the identification $[A, B] = \frac{1}{d}[A_{\tau-1} - (-1)^{\frac{\tau-2}{2}}, B_{\tau-1}]$, it follows that

$$A = \frac{A_{\tau-1} - (-1)^{\frac{\tau-2}{2}}}{d} \quad , \quad B = \frac{B_{\tau-1}}{d} \quad ;$$

thus, from the chain of equalities

$$\Delta_{\frac{\tau-2}{2}} = A^2 - NB^2 = 2\frac{-(-1)^{\frac{\tau-2}{2}} A_{\tau-1} + 1}{d^2} = 2(-1)^{\frac{\tau}{2}} \frac{A}{d}$$

it follows that $2\frac{A}{d}$ **divides** $2N$, that is $\Delta_{\frac{\tau-2}{2}}$ is a divisor of $2N$.

Example

Consider $N = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 = 21945$; the period of the continued fraction of $\sqrt{21945}$ is found to be 10,

j	Δ_j	Ω_j
0	-41	148
1	64	-139
2	-129	117
3	16	-141
4	**-21**	147
5	16	-147
6	-129	141
7	64	-117
8	-41	139
9	1	-148
10	-41	148
11	64	-139

In position $j = \frac{\tau-2}{2} = 4$ we find $\mathbf{-21}$, a factor of N.

Open problem

$\Delta_{\frac{\tau-2}{2}}$ is a divisor of $2N$, but depending on the factors of N, it may be equal 2, a trivial factor.

Find the conditions on N for having $\Delta_{\frac{\tau-2}{2}} \neq 2$.

When $N = p\, q$ is the product of two prime numbers, the conditions are known.

Main theorem (II)

Theorem

Let N be a product of two primes p, q congruent 3 modulo 4, then period τ is even and

$$\Delta_{\frac{\tau-2}{2}} = \left(\frac{p}{q}\right) p \quad \textit{with} \quad p < q \quad .$$

What is the complexity for computing $\Delta_{\frac{\tau-2}{2}}$?

Factorizability of $N = pq$

$p \bmod 8$	$q \bmod 8$	Split?	$(p \mid q)$	$\Delta_{\tau/2-1}$	$T \bmod 4$
3	3	Yes	± 1	$-(p \mid q)\, p$	$1 + (p \mid q)$
3	7	Yes	± 1	$-(p \mid q)\, p$	$1 + (p \mid q)$
7	3	Yes	± 1	$-(p \mid q)\, p$	$1 + (p \mid q)$
7	7	Yes	± 1	$-(p \mid q)\, p$	$1 + (p \mid q)$
5	3	Yes	1	p	0
3	5	Yes	1	$-p$	2
5	3	Yes	-1	$2p$	0
3	5	Yes	-1	$-2p$	2
5	7	Yes	1	p	0
7	5	Yes	1	$-p$	2
5	7	Yes	-1	$-2p$	2
7	5	Yes	-1	$2p$	0
1	3	No	-1	-2	2
1	3	Yes	1	p	AND 0
1	3	No/Yes	1	$-2, -2p$	2
3	1	No	-1		2
3	1	Yes	1	$2p$	AND 0
3	1	No/Yes	1	$-2, -p$	2

Table : $p < q$

Factorizability of $N = pq$

7	1	No	-1	2	0
7	1	No	1	2	AND 0
7	1	Yes	1	$-p, -2p$	2
1	7	No	-1	2	0
1	7	No/Yes	1	$2, p, 2p$	0
5	1	No	-1		$1, 3$
5	1	No	1		AND $1, 3$
5	1	Yes	1	$-p$	AND 2
5	1	Yes	1	p	AND 0
1	5	No	-1		$1, 3$
1	5	No	1		AND $1, 3$
1	5	Yes	1	$-p$	AND 2
1	5	Yes	1	p	AND 0
5	5	No	-1		$1, 3$
5	5	No	1		AND $1, 3$
5	5	Yes	1	$-p$	AND 2
5	5	Yes	1	p	AND 0
1	1	No	-1		$1, 3$
1	1	No	1		AND $1, 3$
1	1	Yes	1	$-p$	AND 2
1	1	Yes	1	p	AND 0

The computational problem

Assuming that
i) a factor of N is in position $\frac{\tau-2}{2}+j\tau$, for some j,
ii) τ is unknown
the problem is:
How to get an unknown position $\frac{\tau-2}{2}+j\tau$ in the infinite sequence

$$\boldsymbol{\Delta} = \Delta_1, \Delta_2, \ldots, \Delta_m, \ldots \quad ?$$

A way is offered by the
a) **Shanks's infrastructural algorithm**
(based on **quadratic forms**) that allows us to move quickly through the sequence $\boldsymbol{\Delta}$ with big and little jumps
b) Adopting as stopping rule the condition

$$\Delta_i \text{ divides } N$$

Quadratic forms

A binary quadratic form $f(x, y) = ax^2 + 2bxy + cy^2$ is identified by the triplet of coefficients

$$[a, 2b, c]$$

Definition

A real quadratic form $[a, 2b, c]$ of discriminant $4N$ is said to be reduced if b is the integer (unique in absolute value) such that $\sqrt{N} - |b| < \kappa < \sqrt{N}$, where $\kappa = \min\{|a|, |c|\}$.

We are interested in the class of reduced principal forms of discriminant $4N$: *when a quadratic form is not reduced it can be reduced by an algorithm of Gauss'*.
Reduction is a linear transformation on the variable x and y, that does not change the class of a quadratic form.

Gauss reduction

Algorithm basic principle (p. 75-76, G.B. Mathews, *Theory of Numbers*, Chelsea)

Suppose that $[a, 2b, c]$ *is a primitive quadratic form which is not reduced and has discriminant* $4N$, *with* $|a| > |c|$.
A reduction function ρ *is defined as*

$$\rho([a, 2b, c]) = [c, 2(b + c\alpha), a + 2b\alpha + c\alpha^2] \quad ,$$

where α *is an integer selected to satisfy the inequality*

$$\left\lceil \sqrt{N} \right\rceil - |c| \leq b + c\alpha \leq \left\lfloor \sqrt{N} \right\rfloor \quad .$$

If

$$|a + 2b\alpha + c\alpha^2| < |c| \quad .$$

the application of ρ *is iterated.*

Shanks' Infrastructure within a class

Let N be a non-square integer, and $[a_0, \overline{a_1, a_2, \ldots, a_{\tau-1}, a_\tau}]$ be the continued fraction expansion of $\sqrt{N}$ having even period.

Let ϵ_0 denote the positive fundamental unit of $\mathbb{K} = \mathbb{Q}(\sqrt{N})$.
The natural logarithm $R_{\mathbb{K}} = \ln \epsilon_0$ is called *regulator* of $\mathbb{K}$.
Consider the infinite sequence $\boldsymbol{\Upsilon}$ of reduced quadratic forms

$$\mathbf{f}_m(X, Y) = \Delta_m X^2 + 2\Omega_m XY + \Delta_{m-1} Y^2 \Leftrightarrow [\Delta_m, 2\Omega_m, \Delta_{m-1}],\ m = 1, 2, \ldots,$$

with $\Delta_0 = \Omega_0^2 - N$ and $\Omega_0 = \Omega_\tau$.

Every quadratic form in $\boldsymbol{\Upsilon}$ has discriminant $4N$.

Infrastructure - Giant step (cont.)

Theorem

The correspondence $m \leftrightarrow \mathbf{f}_m(x,y)$ *for* $1+\ell\tau \leq m \leq \tau+\ell\tau$, $\ell = 0,1,\ldots,$ *is one-to-one, that is, in a period all quadratic forms* $\mathbf{f}_m(x,y)$ *are distinct.*

Between pairs of elements in $\boldsymbol{\Upsilon}$ it is possible to define an operation, denoted with "$\bullet$", for which $\boldsymbol{\Upsilon}$ is closed:

Definition

Let $\mathbf{f}_m, \mathbf{f}_n \in \boldsymbol{\Upsilon}$ *be two quadratic forms, the operation* $\mathbf{f}_m \bullet \mathbf{f}_n$ *is defined as the Gauss's composition of two forms followed by the reduction to the closest quadratic form in* $\boldsymbol{\Upsilon}$ *(that is, the reduction* ρ *is applied the minimum number of times).*

Infrastructure (cont.)

Definition (Gauss composition)

The composition $f_3 = f_1 \circ f_2$ of two forms $f_1 = [a_1, 2b_1, c_1]$ and $f_2 = [a_2, 2b_2, c_2]$, having the same discriminant, is defined to be

$$f_3 = \left[d_0 \frac{a_1 a_2}{d^2}, b_2 + \frac{2a_2}{d}(vn - wc_2), \frac{b_3^2 - N}{a_3} \right] \quad ,$$

where:

$n = b_1 - b_2$, $d = \gcd\{a_1, a_2, b_1 + b_2\}$, $d_0 = \gcd\{d, c_1, c_2, n\}$, *and* v, w *are obtained using the extended Euclidean algorithm to satisfy the condition*

$$d = ua_1 + va_2 + w(b_1 + b_2).$$

Infrastructure (cont.)

It is possible to introduce a metric, compatible with the composition $\bullet$ by defining a distance between two contiguous quadratic forms in the sequence $\boldsymbol{\Upsilon}$

$$d(f_m, f_{m+1}) = \frac{1}{2}\left|\ln \frac{\sqrt{N} + (-1)^m \Omega_m}{\sqrt{N} - (-1)^m \Omega_m}\right| \quad .$$

The distance between two quadratic forms $\mathbf{f}_m(x, y)$ and $\mathbf{f}_n(x, y)$, with $m > n$, is defined to be the sum

$$d(\mathbf{f}_m, \mathbf{f}_n) = \sum_{j=n}^{m-1} d(\mathbf{f}_{j+1}, \mathbf{f}_j) \quad . \tag{10}$$

Infrastructure (cont.)

Assuming $f_0 = f_\tau$, it is possible to prove that

$$d(f_0, f_\tau) = \ln \epsilon_0 \qquad (\text{or } 3 \ln \epsilon_0)$$

where ϵ_0 is the fundamental unit of $\mathbb{K}$.

Shanks observed that, for the composition $\bullet$ of quadratic forms, with a good approximation we have

$$d(f_0, f_m \bullet f_n) \approx d(f_0, f_m) + d(f_0, f_n)$$

The approximation error is of polynomial order $O((\ln N)^\kappa)$ (Schoof).

Infrastructure - Baby step (cont.)

It is also possible to move forward or backward from a quadratic form $\mathbf{f}_m = [\Delta_m, 2\Omega_m, \Delta_{m-1}]$ to the contiguous forms $\mathbf{f}_{m+1}$ or $\mathbf{f}_{m-1}$ respectively:

Moving forward

$$\mathbf{f}_{m+1} = \rho^{+}(\mathbf{f}_m) = \left[\frac{b_1^2 - N}{\Delta_m}, 2b_1, \Delta_m\right] \quad ,$$

where b_1 is computed as $2b_1 = [2\Omega_m \bmod (2\Delta_m)] + 2k\Delta_m$ with k chosen in such a way that $-|\Delta_m| < b_1 < |\Delta_m|$.

Moving backward

$$\mathbf{f}_{m-1} = \rho^{-}((\mathbf{f}_m) = \left[\Delta_{m-1}, 2b_1, \frac{b_1^2 - N}{\Delta_{m-1}}\right] \quad ,$$

where b_1 is computed as $2b_1 = [-2\Omega_m \bmod (2\Delta_{m-1})] + 2k\Delta_{m-1}$ with k chosen in such a way that $-|\Delta_{m-1}| < b_1 < |\Delta_{m-1}|$.

Remark

1. The sign of Δ_{m-1} is the same of Ω_m, which is opposite to that of Δ_m, thus in the sequence Υ the two triples of signs $(-,+,+)$ and $(+,-,-)$ alternate.
2. The distance of $\mathbf{f}_m(x,y)$ from the beginning of $\boldsymbol{\Upsilon}$ is defined by referring to a hypothetical quadratic form $\mathbf{f}_0(x,y)$ properly defined, i.e. $\mathbf{f}_0(x,y) = \mathbf{f}_\tau(x,y) = \Delta_0 x^2 + 2\sqrt{N+\Delta_0}xy + y^2$, which is located before $\mathbf{f}_1(x,y)$, that is

$$d(\mathbf{f}_m, \mathbf{f}_0) = \sum_{j=0}^{m-1} d(\mathbf{f}_{j+1}, \mathbf{f}_j) \quad \text{if } m \leq \tau \ , \tag{11}$$

and by $d(\mathbf{f}_m, \mathbf{f}_0) = d(\mathbf{f}_{m \bmod \tau}, \mathbf{f}_0) + kR_{\mathbb{F}}$ if $k\tau \leq m < (k+1)\tau$.

Remark

1. Shanks observed that, within the first period, the composition law "$\bullet$" induces a structure similar to a cyclic group for the addition of distances modulo the regulator, (or three times the regulator).
2. Between the elements of Υ the distance is nearly maintained by the giant-steps, and is rigorously maintained by the baby-steps.

Theorem

The distance $d(\mathbf{f}_\tau, \mathbf{f}_0)$ is exactly equal to $\ln \mathfrak{c}_{\tau-1}$, i.e. this distance $d(\mathbf{f}_\tau, \mathbf{f}_0)$ is either the regulator $R_{\mathbb{K}}$ or $3R_{\mathbb{K}}$.
The distance $d(\mathbf{f}_{\frac{\tau}{2}}, \mathbf{f}_0)$ is exactly equal to $\frac{1}{2} \ln \mathfrak{c}_{\tau-1}$,

Example of giant and baby steps

$$
\begin{array}{cccccccccccc}
a_1 & a_2 & \dots & a_m & \dots & a_n & \dots & a_{\ell(m,n)} & \dots & a_\tau & \dots \\
\Delta_1 & \Delta_2 & \dots & \Delta_m & \dots & \Delta_n & \dots & \Delta_{\ell(m,n)} & \dots & \Delta_\tau & \dots \\
f_1 & f_2 & \dots & f_m & \dots & f_n & \dots & f_{\ell(m,n)} & \dots & f_\tau & \dots \\
d_1 & d_2 & \dots & d_m & \dots & d_n & \dots & d_m + d_n & \dots & \ln(\mathfrak{c}_{\tau-1}) & \dots
\end{array}
$$

$$
f_m \bullet f_n = f_{\ell(m,n)} \qquad \Leftrightarrow \qquad d_{\ell(m,n)} \approx d_m + d_n
$$

$$
\begin{array}{ccccc}
\dots & a_{m-1} & a_m & a_{m+1} & \dots \\
\dots & \Delta_{m-1} & \Delta_m & \Delta_{m+1} & \dots \\
\dots & f_{m-1} & f_m & f_{m+1} & \dots \\
\dots & d_{m-1} & d_m & d_{m+1} & \dots
\end{array}
$$

$$
f_{m+1} = \rho^+(f_m) \qquad \Leftrightarrow \qquad d_{m+1} = d_m + \frac{1}{2} \ln \frac{\sqrt{N} + (-1)^m \Omega_m}{\sqrt{N} - (-1)^m \Omega_m}
$$

Factoring

Let N be a composite non-square integer, and let N' be the product of all primes in N. Assume that the continued fraction of $\sqrt{N'}$ has even period.

Let $h_{\mathbb{K}}$ be the class number of $\mathbb{K} = \mathbb{Q}(\sqrt{N'})$ with fundamental positive unit ϵ_0, and regulator $R_{\mathbb{K}} = \ln \epsilon_0$.

Since $\mathfrak{c}_{\tau-1}$ is either equal to the positive fundamental unit of $\mathbb{K}$ or equal to its cube, the regulator of $\mathfrak{O}_{\mathbb{K}}$ is either $R_{\mathbb{K}} = \ln \mathfrak{c}_{\tau-1}$, or $R_{\mathbb{K}} = \frac{1}{3} \ln \mathfrak{c}_{\tau-1}$.

Theorem

If the fundamental unit $\mathbf{u}$ *(or* $\mathbf{u}^3$*) of* $\mathbb{K}$ *splits* N*, the computational complexity for obtaining a non-trivial factor is not greater than the complexity for computing the product* $h_{\mathbb{K}} R_{\mathbb{K}}$.

Dirichlet

A celebrated Dirichlet's formula establishes the equality

$$h_{\mathbb{K}} R_{\mathbb{K}} = \frac{\sqrt{N}}{2} L(1, \chi_N)$$

where

- χ is a Kronecker character that, in this case, is given by the Jacobi symbol $\left(\frac{N}{\cdot}\right)$.
- $L(1, \chi_N)$ is a L-function of Dirichlet defined by the series

$$\sum_{n=1}^{\infty} \left(\frac{N}{n}\right) \frac{1}{n}$$

A conditional theorem

Dirichlet's result lets us to formulate a conditional theorem

Theorem

The factoring complexity of a composite N which is split by the unit $\mathfrak{c}_{\tau-1}$ (in particular $N = pq$, with $p = q = 3 \bmod 4$) is not greater than the complexity for evaluating the series

$$\sqrt{N}\sum_{n=1}^{\infty}\left(\frac{N}{n}\right)\frac{1}{n}$$

with an approximation of the order $O((\ln N)^a)$, $a > 0$.

$\mathbf{L}(1, \chi_N)$ (cont.)

The direct computation of $L(1, \chi_N)$ is impractical when N is large. Using the functional equation, the following expression was derived

$$L(1, \chi_N) = \sum_{x \geq 1} \left(\frac{N}{x} \right) \left(\frac{1}{x} \mathrm{erfc}(x\sqrt{\frac{\pi}{N}}) + \frac{1}{\sqrt{N}} E_1(\frac{\pi x^2}{N}) \right) \quad ,$$

where $\mathrm{erfc}(x)$ is the error complementary function computable as ([Abramowitz, p.297-299])

$$\mathrm{erfc}(z) = \frac{2}{\sqrt{\pi}} \int_z^\infty e^{t^2} dt = 1 - \mathrm{erf}(z) = 1 - \frac{2}{\sqrt{\pi}} \sum_{n=0}^\infty \frac{(-1)^n z^{2n+1}}{n!(2n+1)}$$

e $E_1(x)$ is the integral exponential function computable as

$$E_1(z) = \int_1^\infty \frac{e^{-tz}}{t} dt = -\gamma - ln(z) - \sum_{n=1}^\infty \frac{(-1)^n z^n}{n \cdot n!}$$

Conclusions

1. The factorization of an integer N can be obtained from the continued fraction expansion of $\sqrt{N}$, when the period is even.
2. If the product $h_{\mathbb{K}} R_{\mathbb{K}}$ is computable with a good approximation, i.e. $O((\ln N)^{\kappa})$, then it is possible to factorize with the same complexity.
3. These properties have a significant impact in **Number theory** and **Cryptography** .

Bibliography

1. Buell D.A., *Binary Quadratic Forms*, Springer, New York, 1989.
2. Davenport H., *The Higher Arithmetic*, Dover, New York, 1960.
3. Legendre A-M., *Essai sur la Théorie des Nombres*, Chez Courcier, Paris, 1808, reissued by Cambridge University Press, 2009.
4. Perron O., *Die Lehre von den Kettenbrüchen*, Band I, Springer, Wiesbaden, 1977.
5. Scharlau W., Opolka H., *From Fermat to Minkowski*, Springer, New York, 1985.
6. Sierpinski W., *Elementary Theory of Numbers*, North Holland, New York, 1988.