Continued Fractions and Factoring

Michele Elia - Politecnico di Torino

De Cifris Athesis Seminars

Trento, October 30th, 2019

Outline of the presentation

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

Fermat (1607-1665)

In a letter to **Pierre de Carcavi**, August 14, 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 (of positive numbers), i.e.

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

Euler (1707-1783) - First known proof (constructive)

Euler proof (1749) uses Fermat's *infinite descent.*

$$X^2 + Y^2 = p \Rightarrow x^2 + 1 = 0 \pmod{p}$$

A solution $|x_0| < \frac{p}{2}$ of the modular equation certainly exists by the little Fermat's theorem, then $x_0^2 + 1 = s_0\ p$ with $s_0 < \frac{p}{2}$. Setting $x_1 = x_0 \pmod{s_0}$ and $x_2 = 1$, 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 $s_1 < \frac{s_0}{2}$. Multiplying $s_0 p$ by $s_0 s_1$, and using an identity already known to Diophantus, we obtain the equation

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

Euler's proof (cont.)

- Since $x_0 x_2 = x_1 \pmod{s_0}$ by definition of x_1 e x_2, we have $m|(x_0x_2 - x_1)$, thus dividing by s_0^2
- $$s_1 p = \left(\frac{x_0x_2 - x_1}{s_0}\right)^2 + \left(\frac{x_0 \; x_1 + x_2}{s_0}\right)^2$$
  the rightest term is necessarily an integer.
  The first step of the *infinite descent* is complete.
- Iterating the process, a sequence of positive decreasing integers 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 triplets $\mathcal{T} = \{(x, y, z) \in \mathbb{Z}_+^3 : x^2 + 4yz = p\}$ 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

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

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

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

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

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 $\frac{p_{\frac{\tau-1}{2}}}{q_{\frac{\tau-1}{2}}}$ yields

$$X = p^2_{\frac{\tau-1}{2}} - Nq^2_{\frac{\tau-1}{2}} \quad , \quad Y = \sqrt{N - X^2} \quad .$$

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

$$Y = p_{\frac{\tau-1}{2}} p_{\frac{\tau-1}{2}-1} - Nq_{\frac{\tau-1}{2}} q_{\frac{\tau-1}{2}-1} \quad .$$

2. This property is a consequence of the palindromic features of sequences connected with the continued fraction expansion of $\sqrt{N}$.

Legendre own words

... Donc tous le fois que $x^2 - Ay^2 = -1$ *est résoluble (ce qui ha lieu entre autre cas lorsque* A *est un nombre premier* $4n+1$*) le nombre* A *peut toujours être décomposé en deux quarrées; et cette décomposition est donnée immediatement par le 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, 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 quarrées; elle donne en même temps le moyen de faire cette décomposition d'une maniére 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	$\sqrt{149 - \Delta_j^2}$
-1	1	-12	$2\sqrt{37}$
0	-5	12	$2\sqrt{31}$
1	17	-8	$2I\sqrt{35}$
2	-4	9	$\sqrt{133}$
3	7	-11	10
4	**-7**	**10**	10
5	4	-11	$\sqrt{133}$
6	-17	9	$2I\sqrt{35}$
7	5	-8	$2\sqrt{31}$
8	-1	12	$2\sqrt{37}$
9	5	-12	$2\sqrt{31}$

In position $J = 4$ we find $X = -7$ and $Y = 10$.

The Problem

The tricky property discovered by Legendre when the Pell equation $x^2 - Ny^2 = -1$ has a solution, i.e. the continued fraction expansion of $\sqrt{N}$ has odd period, naturally rises a question

What happens when the period of the continued fraction expansion of $\sqrt{N}$ is even, i.e. the Pell equation $x^2 - Ny^2 = -1$ has not a solution ?

Note: the Pell equation $x^2 - Ny^2 = 1$ always has a solution. .

Continued Fractions

Regular continued fractions ($a_0 \geq 0$, $a_i \in \mathbb{N} \quad \forall i > 0$)

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \quad , \tag{2}$$

Periodic continued fractions are compactly written in the form

$$\alpha = [b_0, \ldots, b_k, \overline{a_1, a_2, \ldots, a_{\tau-1}, a_\tau}] \quad , \tag{3}$$

where the period is over-lined, and the pre-period is red.
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.

Lagrange (1736-1813)

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.

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

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

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

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

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

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

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 (Annales 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

$$-\frac{1}{\alpha'} = [\overline{a_{\tau-1}, a_{\tau-2}, \ldots, a_1, a_0}] \tag{4}$$

A Corollary (cont.)

Given a prime $p = Q^2 + P^2$, with $Q < P$, then $\alpha = \frac{Q+\sqrt{p}}{P}$ is greater than 1, and belongs to $\mathbb{Q}(\sqrt{p})$. Thus $\alpha' = \frac{Q-\sqrt{p}}{P} \in [-1,\ 0]$, and by the Galois' theorem the continued fraction expansion of α is purely periodic

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

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

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

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

Periodic continued fraction of $\sqrt{N}$

Consider $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_{\tau-1}, a_\tau}]$, 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

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

The properties of two sequences c_n and r_n defined as

$$c_n = |\Omega_{n-1}| \quad , \quad r_n = |\Delta_{n-1}| \ .$$

are summarized in the next two slides

Carr's list of properties

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

$$\frac{\sqrt{N}+c_n}{r_n} = a_{n+1} + \frac{r_{n+1}}{\sqrt{N}+c_{n+1}} \quad n = 0, 1, \ldots$$

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

$$a_{n+1} = \left\lfloor \frac{\sqrt{N}+c_n}{r_n} \right\rfloor = \left\lfloor \frac{c_0+c_n}{r_n} \right\rfloor \quad . \tag{5}$$

(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

$$\begin{aligned} a_{n+1} &= \left\lfloor \tfrac{a_0+c_n}{r_n} \right\rfloor \\ c_{n+1} &= a_{n+1}r_n - c_n \\ r_{n+1} &= \tfrac{N-c_{n+1}^2}{r_n} \quad . \end{aligned} \tag{6}$$

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

Periodicity of $\boldsymbol{\Delta}$ and $\boldsymbol{\Omega}$

Theorem

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

The sequence $\boldsymbol{\Delta} = \{\Delta_1, \Delta_2, \cdots, \Delta_{\tau-1}, \Delta_\tau, \cdots\}$ 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 $\boldsymbol{\Omega} = \{\Omega_1, \Omega_2, \cdots, \Omega_{\tau-1}, \Omega_\tau, \cdots\}$ is periodic with period τ, or 2τ if τ is odd. The first $\tau - 2$ terms of a period satisfy the condition of symmetry $\Omega_m = -(-1)^\tau \Omega_{\tau-m-1}$.

Remark: It is known that $\Delta_{\tau-1} = (-1)^\tau$, that is

$$\mathfrak{c}_{\tau-1} = A_{\tau-1} + B_{\tau-1}\sqrt{N}$$

is a unit in the quadratic field $\mathbb{Q}(\sqrt{N})$: it is the positive fundamental unit if $\{1, \sqrt{N}\}$ is integral basis.

Quadratic forms

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

Example

even $\tau = 10$

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

odd $\tau = 11$

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

τ odd

Observed that $\tau - (\frac{\tau-1}{2}) - 2 = \frac{\tau-3}{2}$, the symmetry in each 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

$$f_{\frac{\tau-1}{2}}(x,y) = \Delta_{\frac{\tau-1}{2}} x^2 + 2\Omega_{\frac{\tau-1}{2}} xy + \Delta_{\frac{\tau-3}{2}} y^2$$

lets us to conclude

$$p = \Delta^2_{\frac{\tau-1}{2}} + \Omega^2_{\frac{\tau-1}{2}} \tag{7}$$

Example Consider $p = 409$, $\tau = 21$, $\frac{\tau-1}{2} = 10$

	1,	2,	3,	,4,	5,	6,	7,	8,	9,	10,	11, ...
a_j :	4,	2,	7,	1,	1,	1,	4,	2,	2,	13,	13, ...
$\mathbf{\Delta}$:	17,	−5,	24,	−15,	23,	−8,	15,	−16,	3,	−3,	16, ...
$\mathbf{\Omega}$:	−16,	18,	−17,	7,	−8,	15,	−17,	13,	−19,	20,	−19, ...

$$409 = 3^2 + 20^2$$

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 ϵ_0 (or ϵ_0^3) 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 $\mathbf{\Delta}$.*

Outline of the proof

Consider the j-convergent $\frac{A_j}{B_j}$, define the column vector $[A_j, B_j]^T$, and consider the involutory matrix

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

which has characteristic polynomial $Z^2 - 1$, i.e. eigenvalues ± 1. It can be proved that holds the relation

$$\begin{bmatrix} A_{\tau-j-2} \\ B_{\tau-j-2} \end{bmatrix} = (-1)^j M_{\tau-1} \begin{bmatrix} A_j \\ B_j \end{bmatrix} \quad . \tag{8}$$

Outline of the 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

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

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

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

Outline of the proof (cont.)

From the matrix $M_{\tau-1}$ we have that any eigenvector is of the form $\frac{1}{d}[A_{\tau-1} - (-1)^{\frac{\tau-2}{2}}, B_{\tau-1}]$, 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 10,

j	Δ_j	Ω_j
-1	1	-148
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

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

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 $\Delta_{\frac{\tau-2}{2}} \neq 2$.

When $\mathbf{N = p\ q}$ is the product of two prime numbers, these conditions are known, and are reported in the following slides without proof, which is based on propertis of the quadratic field extension of $\mathbb{Q}$.

Main theorem (II)

Theorem

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

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

This theorem is a corollary of Theorem 5, p.381 in the paper *"Relative Densities of Ramified Primes in $\mathbb{Q}(\sqrt{pq})$, International Mathematical Forum, 3, 2008, no. 8, 375 - 384"*.

Factorability of $N = pq$

p mod 8	q mod 8	Split?	$(p \mid q)$	$\Delta_{\tau/2-1}$	T mod 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	2
3	1	Yes	1	$2p$	AND 0
3	1	No/Yes	1	$-2, -p$	2

Table : $p < q$

Factorability 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

Table : $p < q$

The computational problem

Assuming that a factor of N is in position $\frac{\tau-2}{2}+j\tau$, for some j_o, the problem is:
How to get rapidly the position $\frac{\tau-2}{2}+j_o\tau$ *in the infinite sequence*

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

A way is offered by

Shanks's infrastructural algorithm

based on the class quadratic forms $f_m(X,Y)$ that allows us to move fast through $\boldsymbol{\Delta}$, and adopting as stopping rule

$$\frac{\mathbf{2N}}{|\boldsymbol{\Delta}_\mathbf{i}|} \in N.$$

Shanks' Infrastructure: Quadratic forms

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* $\kappa = \min\{|a|, |c|\}$.

Definition (Gauss reduction)

Let $[a, 2b, c]$ *be a primitive quadratic form, 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 selected to satisfy the inequality*

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

Shanks' Infrastructure (cont.)

Let N be not a 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 be 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

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

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

Every quadratic form in $\boldsymbol{\Upsilon}$ has discriminant $4N$, and a period contains every reduced form of the principal class.

Infrastructure - Giant step (cont.)

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 $f_m, f_n \in \boldsymbol{\Upsilon}$ be to quadratic forms, the operation $f_m \bullet f_n$ is defined as the Gauss's composition of two forms followed by the reduction to the closest quadratic form in $\boldsymbol{\Upsilon}$.

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 as*

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

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.)

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

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

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

$$d(\mathbf{f}_m, \mathbf{f}_n) = \sum_{j=n}^{m-1} d(\mathbf{f}_{j+1}, \mathbf{f}_j) \quad . \tag{9}$$

Infrastructure (cont.)

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

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

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 $\mathbf{f}_m(x,y) = [\Delta_m, 2\Omega_m, \Delta_{m-1}]$ to the contiguous forms $\mathbf{f}_{m+1}(x,y)$ or $\mathbf{f}_{m-1}(x,y)$ respectively:
Moving forward

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

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

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

where b_1 is $2b_1 = [-2\Omega_m \bmod (2\Delta_{m-1})] + 2k\Delta_{m-1}$ 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 triplets 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

$$d(\mathbf{f}_m, \mathbf{f}_0) = \sum_{j=0}^{m-1} d(\mathbf{f}_{j+1}, \mathbf{f}_j) \quad \text{if } m \leq \tau \ , \tag{10}$$

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 $\boldsymbol{\Upsilon}$ 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

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

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

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

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

Factoring

Let N be a composite integer which is not a square. 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 $R_{\mathbb{K}} = \ln \epsilon_0$. The main result is formulated as a theorem.

Theorem

If the fundamental unit ϵ_0 (or ϵ_0^3) 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 $\left(\dfrac{N}{\cdot}\right)$.
- $L(1, \chi_N)$ 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.

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.