Outline of the presentation

1. Fermat, Legendre and the equation \( p = x^2 + y^2 \)
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.*

$$p = X^2 + Y^2 \iff p \equiv 1 \mod 4$$
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

\[ x_1^2 + x_2^2 \pmod{s_0} = x_0^2 + 1 \pmod{s_0} = 0 \Rightarrow x_1^2 + x_2^2 = s_0s_1 \]

with \(s_1 < \frac{s_0}{2}\). Multiplying \(s_0p\) by \(s_0s_1\), and using an identity already known to Diophantus, we obtain the equation

\[ s_0^2s_1p = (x_1^2 + x_2^2)(x_0^2 + 1) = (x_0x_2 - x_1)^2 + (x_0 \ x_1 + x_2)^2 \]
Euler’s proof (cont.)

- Since \( x_0x_2 = x_1 \pmod{s_0} \) by definition of \( x_1 \) e \( x_2 \), we have \( m \mid (x_0x_2 - x_1) \), thus dividing by \( s_0^2 \)

- \( s_1p = \left( \frac{x_0x_2-x_1}{s_0} \right)^2 + \left( \frac{x_0\, x_1+x_2}{s_0} \right)^2 \)

  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

\[
(x, y, z) \rightarrow (x, z, y) \quad \text{and fixes} \quad (x, y, y)
\]

2. The second involution has a more complex definition

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

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

\[
x = \frac{(2k)!}{2(k!)^2} \mod p \quad , \quad y = \frac{(2k!)^2}{2(k!)^2} \mod p
\]

the second is based on quadratic forms of discriminant \(-4\)

\[
p \rightarrow pX^2 + 2b_1 XY + \frac{b_1^2 + 1}{p} Y^2 \rightarrow x^2 + y^2
\]

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

$$X = p_{\frac{\tau-1}{2}}^2 - Nq_{\frac{\tau-1}{2}}^2, \quad Y = \sqrt{N - X^2}.$$  

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

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

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


... 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 immédiatement 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 manière directe et sans aucun tâtonnement.
Consider $N = 149$, the period of the continued fraction of $\sqrt{149}$ is 9,

<table>
<thead>
<tr>
<th>$j$</th>
<th>$\Delta_j$</th>
<th>$\Omega_j$</th>
<th>$\sqrt{149 - \Delta_j^2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>1</td>
<td>-12</td>
<td>$2\sqrt{37}$</td>
</tr>
<tr>
<td>0</td>
<td>-5</td>
<td>12</td>
<td>$2\sqrt{31}$</td>
</tr>
<tr>
<td>1</td>
<td>17</td>
<td>-8</td>
<td>$2I\sqrt{35}$</td>
</tr>
<tr>
<td>2</td>
<td>-4</td>
<td>9</td>
<td>$\sqrt{133}$</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>-11</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>-7</td>
<td><strong>10</strong></td>
<td><strong>10</strong></td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>-11</td>
<td>$\sqrt{133}$</td>
</tr>
<tr>
<td>6</td>
<td>-17</td>
<td>9</td>
<td>$2I\sqrt{35}$</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>-8</td>
<td>$2\sqrt{31}$</td>
</tr>
<tr>
<td>8</td>
<td>-1</td>
<td>12</td>
<td>$2\sqrt{37}$</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>-12</td>
<td>$2\sqrt{31}$</td>
</tr>
</tbody>
</table>

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 \((a_0 \geq 0, \ a_i \in \mathbb{N} \ \forall i > 0)\)

\[
a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}} , \quad (2)
\]

Periodic continued fractions are compactly written in the form

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

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.

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

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

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

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

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

$$\frac{5 + \sqrt{89}}{8} = [1, 1, 4, 9, 4, 1, 1] \quad \tau = 7.$$
A quadratic irrational $\alpha$ is said to be **reduced** if $\alpha > 1$ and its conjugate $\alpha'$ 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 $\alpha$ is purely periodic if and only if $\alpha$ is reduced. In this case for the conjugate $\alpha'$ of

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

we have

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

(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 \( \alpha \) 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

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

\[
\alpha = \frac{5 + \sqrt{89}}{8} \Rightarrow [[\ ], [1, 1, 4, 9, 4, 1, 1]] \Leftarrow -\frac{1}{\alpha'}
\]
Consider $\sqrt{N} = [a_0, a_1, a_2, \ldots, a_{\tau-1}, a_{\tau}]$, the \( m \)-convergent is the fraction obtained considering only the first \( m \) terms.

The sequence of convergents is

\[
\frac{p_0}{q_0} = a_0, \quad \frac{p_1}{q_1} = \frac{a_0a_1 + 1}{a_1}, \quad \ldots, \quad \frac{p_j}{q_j} = \frac{a_jp_{j-1} + p_{j-2}}{a_jq_{j-1} + q_{j-2}}, \quad \ldots
\]

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

\[
\begin{align*}
\Delta_j &= p_j^2 - Nq_j^2 \\
\Omega_j &= p_jp_{j-1} - Nq_jq_{j-1} \quad j = 1, 2, \ldots
\end{align*}
\]

The properties of two sequences $c_n$ and $r_n$ defined as

\[
c_n = |\Omega_{n-1}|, \quad r_n = |\Delta_{n-1}|
\]

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

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

$$
\begin{align*}
a_{n+1} &= \left\lfloor \frac{a_0 + c_n}{r_n} \right\rfloor \\
c_{n+1} &= a_{n+1}r_n - c_n \\
r_{n+1} &= \frac{N - c_{n+1}^2}{r_n}.
\end{align*}
$$

These equations allow us to compute the sequence $\{a_n\}_{n \geq 1}$ using only rational arithmetical operations.
Periodicity of $\Delta$ and $\Omega$

**Theorem**

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

The sequence $\Delta = \{\Delta_1, \Delta_2, \cdots, \Delta_{\tau-1}, \Delta_{\tau}, \cdots\}$ is periodic with period $\tau$, or $2\tau$ if $\tau$ 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 $\Omega = \{\Omega_1, \Omega_2, \cdots, \Omega_{\tau-1}, \Omega_{\tau}, \cdots\}$ is periodic with period $\tau$, or $2\tau$ if $\tau$ 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

$$c_{\tau-1} = A_{\tau-1} + B_{\tau-1}\sqrt{N}$$

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

The quadratic forms

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

have discriminant 4N.

In each period (of length \(\tau\) or 2\(\tau\)) the correspondence \(m \leftrightarrow f_m\) is one-to-one.
Example

even $\tau = 10$

$$\sqrt{543} = [23, [3, 3, 3, 1, 14, 1, 3, 3, 3, 46]]$$

$$\Delta = [13, -11, 34, -3, 34, -11, 13, -14, 1, -14]$$

$$\Omega = [-19, 20, -13, 21, -21, 13, -20, 19, -23, 23]$$

odd $\tau = 11$

$$\sqrt{6437} = [80, [4, 3, 39, 1, 4, 4, 1, 39, 3, 4, 160]]$$

$$\Delta = [49, -4, 127, -31, 31, -127, 4, -49, 37, -1, 37]$$

$$\Omega = [-68, 79, -77, 50, -74, 50, -77, 79, -68, 80, -80]$$
\( \tau \) odd

Observed that \( \tau - \left(\frac{\tau-1}{2}\right) - 2 = \frac{\tau-3}{2} \), the symmetry in each period of the sequence \( \Delta \) 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

\[
p = \Delta \frac{\tau-1}{2}^2 + \Omega \frac{\tau-1}{2}^2 \quad (7)
\]

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

\[
a_j : \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8, \quad 9, \quad 10, \quad 11, \ldots
\]

\[
\Delta : \quad 17, \quad -5, \quad 24, \quad -15, \quad 23, \quad -8, \quad 15, \quad -16, \quad 3, \quad -3, \quad 16, \ldots
\]

\[
\Omega : \quad -16, \quad 18, \quad -17, \quad 7, \quad -8, \quad 15, \quad -17, \quad 13, \quad -19, \quad 20, \quad -19, \ldots
\]

\[
409 = 3^2 + 20^2
\]
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 $\epsilon_0$ (or $\epsilon_0^3$) 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 $\Delta$. 

τ even  -  Main theorem  (I)
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

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

which has characteristic polynomial \( Z^2 - 1 \), i.e. eigenvalues \( \pm 1 \). It can be proved that holds the relation

\[
\begin{bmatrix}
A_{\tau-j-2} \\
B_{\tau-j-2}
\end{bmatrix} = (-1)^j M_{\tau-1} \begin{bmatrix}
A_j \\
B_j
\end{bmatrix} .
\] (8)
When $\tau - \ell - 2 = \ell$, i.e. $\ell = \frac{\tau - 2}{2}$, we have two possibilities depending whether $\ell$ is even or odd

\[
A_{\tau - \ell - 2} = A\ell = A \quad \text{e} \quad B_{\tau - \ell - 2} = B\ell = B \quad \text{even } \ell
\]

\[
A_{\tau - \ell - 2} = -A\ell = -A \quad \text{e} \quad B_{\tau - \ell - 2} = -B\ell = -B \quad \text{odd } \ell
\]

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

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

thus, from the chain of equalities

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

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,

<table>
<thead>
<tr>
<th>( j )</th>
<th>( \Delta_j )</th>
<th>( \Omega_j )</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>1</td>
<td>-148</td>
</tr>
<tr>
<td>0</td>
<td>-41</td>
<td>148</td>
</tr>
<tr>
<td>1</td>
<td>64</td>
<td>-139</td>
</tr>
<tr>
<td>2</td>
<td>-129</td>
<td>117</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td>-141</td>
</tr>
<tr>
<td>4</td>
<td>-21</td>
<td>147</td>
</tr>
<tr>
<td>5</td>
<td>16</td>
<td>-147</td>
</tr>
<tr>
<td>6</td>
<td>-129</td>
<td>141</td>
</tr>
<tr>
<td>7</td>
<td>64</td>
<td>-117</td>
</tr>
<tr>
<td>8</td>
<td>-41</td>
<td>139</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>-148</td>
</tr>
<tr>
<td>10</td>
<td>-41</td>
<td>148</td>
</tr>
</tbody>
</table>

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 \( N = p \cdot q \) is the product of two prime numbers, these conditions are known, and are reported in the following slides without proof, which is based on properties 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 $\tau$ is even, and

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

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 $N = pq$

<table>
<thead>
<tr>
<th>$p \mod 8$</th>
<th>$q \mod 8$</th>
<th>Split?</th>
<th>$(p \mid q)$</th>
<th>$\Delta_{\tau/2-1}$</th>
<th>$T \mod 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3</td>
<td>Yes</td>
<td>±1</td>
<td>$-(p \mid q)p$</td>
<td>$1 + (p \mid q)$</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>Yes</td>
<td>±1</td>
<td>$-(p \mid q)p$</td>
<td>$1 + (p \mid q)$</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>Yes</td>
<td>±1</td>
<td>$-(p \mid q)p$</td>
<td>$1 + (p \mid q)$</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>Yes</td>
<td>±1</td>
<td>$-(p \mid q)p$</td>
<td>$1 + (p \mid q)$</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>Yes</td>
<td>1</td>
<td>$p$</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>Yes</td>
<td>1</td>
<td>$-p$</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>Yes</td>
<td>−1</td>
<td>$2p$</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>Yes</td>
<td>−1</td>
<td>$-2p$</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>Yes</td>
<td>1</td>
<td>$p$</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>Yes</td>
<td>1</td>
<td>$-p$</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>Yes</td>
<td>−1</td>
<td>$-2p$</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>Yes</td>
<td>−1</td>
<td>$2p$</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>No</td>
<td>−1</td>
<td>−2</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>Yes</td>
<td>1</td>
<td>$p$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>No/Yes</td>
<td>1</td>
<td>$-2, -2p$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>No</td>
<td>−1</td>
<td>−2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>1</td>
<td>$2p$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>No/Yes</td>
<td>1</td>
<td>$-2, -p$</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**Table:** $p < q$
Factorability of $N = pq$

<table>
<thead>
<tr>
<th>$7$</th>
<th>$1$</th>
<th>No</th>
<th>$-1$</th>
<th>$2$</th>
<th>$0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7$</td>
<td>$1$</td>
<td>No</td>
<td>$1$</td>
<td>$2$</td>
<td>$0$</td>
</tr>
<tr>
<td>$7$</td>
<td>$1$</td>
<td>Yes</td>
<td>$1$</td>
<td>$-p, -2p$</td>
<td>$2$</td>
</tr>
<tr>
<td>$1$</td>
<td>$7$</td>
<td>No</td>
<td>$-1$</td>
<td>$2$</td>
<td>$0$</td>
</tr>
<tr>
<td>$1$</td>
<td>$7$</td>
<td>No/Yes</td>
<td>$1$</td>
<td>$2, p, 2p$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$5$</th>
<th>$1$</th>
<th>No</th>
<th>$-1$</th>
<th>$p$</th>
<th>$1, 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5$</td>
<td>$1$</td>
<td>No</td>
<td>$1$</td>
<td>$p$</td>
<td>$1, 3$</td>
</tr>
<tr>
<td>$5$</td>
<td>$1$</td>
<td>Yes</td>
<td>$1$</td>
<td>$-p$</td>
<td>$2$</td>
</tr>
<tr>
<td>$5$</td>
<td>$1$</td>
<td>Yes</td>
<td>$1$</td>
<td>$p$</td>
<td>$0$</td>
</tr>
<tr>
<td>$1$</td>
<td>$5$</td>
<td>No</td>
<td>$-1$</td>
<td>$1, 3$</td>
<td>$1, 3$</td>
</tr>
<tr>
<td>$1$</td>
<td>$5$</td>
<td>No</td>
<td>$1$</td>
<td>$1, 3$</td>
<td>$1, 3$</td>
</tr>
<tr>
<td>$1$</td>
<td>$5$</td>
<td>Yes</td>
<td>$1$</td>
<td>$-p$</td>
<td>$2$</td>
</tr>
<tr>
<td>$1$</td>
<td>$5$</td>
<td>Yes</td>
<td>$1$</td>
<td>$p$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$5$</th>
<th>$5$</th>
<th>No</th>
<th>$-1$</th>
<th>$1, 3$</th>
<th>$1, 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5$</td>
<td>$5$</td>
<td>No</td>
<td>$1$</td>
<td>$1, 3$</td>
<td>$1, 3$</td>
</tr>
<tr>
<td>$5$</td>
<td>$5$</td>
<td>Yes</td>
<td>$1$</td>
<td>$1, 3$</td>
<td>$1, 3$</td>
</tr>
<tr>
<td>$5$</td>
<td>$5$</td>
<td>Yes</td>
<td>$1$</td>
<td>$1, 3$</td>
<td>$1, 3$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$1$</th>
<th>$1$</th>
<th>No</th>
<th>$-1$</th>
<th>$1, 3$</th>
<th>$1, 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>$1$</td>
<td>No</td>
<td>$1$</td>
<td>$1, 3$</td>
<td>$1, 3$</td>
</tr>
<tr>
<td>$1$</td>
<td>$1$</td>
<td>Yes</td>
<td>$1$</td>
<td>$-p$</td>
<td>$2$</td>
</tr>
<tr>
<td>$1$</td>
<td>$1$</td>
<td>Yes</td>
<td>$1$</td>
<td>$p$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

Table: $p < q$
The computational problem

Assuming that a factor of $N$ is in position $\frac{\tau - 2}{2} + j_0 \tau$, for some $j_0$, the problem is:

How to get rapidly the position $\frac{\tau - 2}{2} + j_0 \tau$ in the infinite sequence

$$\Delta = \Delta_1, \Delta_2, \ldots, \Delta_m, \ldots$$

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 $\Delta$, and adopting as stopping rule

$$\frac{2N}{|\Delta_i|} \in N.$$
**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 \(\rho\) is defined as

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

where \(\alpha\) is selected to satisfy the inequality

\[
|a + 2b\alpha + c\alpha^2| < |c|.
\]
Let $N$ be not a square integer, and $[a_0, a_1, a_2, \ldots, a_{\tau-1}, a_{\tau}]$ be the continued fraction expansion of $\sqrt{N}$ having even period.

Let $\epsilon_0$ be the positive fundamental unit of $K = \mathbb{Q}(\sqrt{N})$.

The natural logarithm $R_K = \ln \epsilon_0$ is called regulator of $K$.

Consider the infinite sequence $\Upsilon$ of reduced quadratic forms

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

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

Every quadratic form in $\Upsilon$ has discriminant $4N$, and a period contains every reduced form of the principal class.
Between pairs of elements in $\mathcal{Y}$ it is possible to define an operation, denoted with "•", for which $\mathcal{Y}$ is closed:

**Definition**

Let $f_m, f_n \in \mathcal{Y}$ 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 $\mathcal{Y}$. 
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

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

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

\[ d = ua_1 + va_2 + w(b_1 + b_2). \]
In the sequence $\mathcal{Y}$ it is possible to introduce a metric, compatible with the composition $\bullet$, defining a distance between two contiguous quadratic forms

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

The distance between two quadratic forms $f_m(x, y)$ and $f_n(x, y)$, with $m > n$, is defined to be the sum

$$d(f_m, f_n) = \sum_{j=n}^{m-1} d(f_{j+1}, f_j).$$ (9)
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 $\epsilon_0$ 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).
It is also possible to move forward or backward from a quadratic form \( f_m(x, y) = [\Delta_m, 2\Omega_m, \Delta_{m-1}] \) to the contiguous forms \( f_{m+1}(x, y) \) or \( f_{m-1}(x, y) \) respectively:

Moving forward

\[
\begin{align*}
f_{m+1}(x, y) &= \rho^+(f_m(x, y)) = \left[ \frac{b_1^2 - N}{\Delta_m}, 2b_1, \Delta_m \right],
\end{align*}
\]

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

Moving backward

\[
\begin{align*}
f_{m-1}(x, y) &= \rho^-(f_m(x, y)) = \left[ \Delta_{m-1}, 2b_1, \frac{b_1^2 - N}{\Delta_{m-1}} \right],
\end{align*}
\]

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

1. The sign of $\Delta_{m-1}$ is the same of $\Omega_m$, which is opposite to that of $\Delta_m$, thus in the sequence $\Upsilon$ the two triplets of signs $(-, +, +)$ and $(+, -, -)$ alternate.

2. The distance of $f_m(x, y)$ from the beginning of $\Upsilon$ is defined by referring to a hypothetical quadratic form $f_0(x, y)$ properly defined, i.e.

$$f_0(x, y) = f_\tau(x, y) = \Delta_0 x^2 + 2\sqrt{N} + \Delta_0 xy + y^2,$$

which is located before $f_1(x, y)$, that is

$$d(f_m, f_0) = \sum_{j=0}^{m-1} d(f_{j+1}, f_j) \text{ if } m \leq \tau, \quad (10)$$

and by $d(f_m, f_0) = d(f_{m \mod \tau}, f_0) + kR_{\mathbb{F}}$ if $k\tau \leq m < (k+1)\tau$. 
Remark

1. Shanks observed that, within the first period, the composition law ° 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 $\mathcal{Y}$ the distance is nearly maintained by the giant-steps, and is rigorously maintained by the baby-steps.

Theorem

The distance $d(f_\tau, f_0)$ is exactly equal to $\ln c_{\tau-1}$, i.e. this distance $d(f_\tau, f_0)$ is either the regulator $R_K$ or $3R_K$.

The distance $d(f_{\tau \frac{\pi}{2}}, f_0)$ is exactly equal to $\frac{1}{2} \ln c_{\tau-1}$,
Example of giant and baby steps

\[ a_1 \quad a_2 \quad \ldots \quad a_m \quad \ldots \quad a_n \quad \ldots \quad a_{\ell(m,n)} \quad \ldots \quad a_\tau \quad \ldots \]

\[ \Delta_1 \quad \Delta_2 \quad \ldots \quad \Delta_m \quad \ldots \quad \Delta_n \quad \ldots \quad \Delta_{\ell(m,n)} \quad \ldots \quad \Delta_\tau \quad \ldots \]

\[ f_1 \quad f_2 \quad \ldots \quad f_m \quad \ldots \quad f_n \quad \ldots \quad f_{\ell(m,n)} \quad \ldots \quad f_\tau \quad \ldots \]

\[ d_1 \quad d_2 \quad \ldots \quad d_m \quad \ldots \quad d_n \quad \ldots \quad d_m + d_n \quad \ldots \quad \ln(c_{\tau-1}) \quad \ldots \]

\[ f_m \bullet f_n = f_{\ell(m,n)} \iff d_{\ell(m,n)} \approx d_m + d_n \]

\[ \ldots \quad a_{m-1} \quad a_m \quad a_{m+1} \quad \ldots \]

\[ \ldots \quad \Delta_{m-1} \quad \Delta_m \quad \Delta_{m+1} \quad \ldots \]

\[ \ldots \quad f_{m-1} \quad f_m \quad f_{m+1} \quad \ldots \]

\[ \ldots \quad d_{m-1} \quad d_m \quad d_{m+1} \quad \ldots \]

\[ f_{m+1} = \rho^+(f_m) \iff d_{m+1} = d_m + \frac{1}{2} \ln \frac{\sqrt{N} + (-1)^m \Omega_m}{\sqrt{N} - (-1)^m \Omega_m} \]
Factoring

Let $N$ be a composite integer which is not a square. Assume that the continued fraction of $\sqrt{N}$ has even period. Let $h_K$ be the class number of $K = \mathbb{Q}(\sqrt{N})$ with fundamental positive unit $\epsilon_0$, and regulator $R_K = \ln \epsilon_0$. The main result is formulated as a theorem.

**Theorem**

*If the fundamental unit $\epsilon_0$ (or $\epsilon_0^3$) of $K$ splits $N$, the computational complexity for obtaining a non-trivial factor is not greater than the complexity for computing the product $h_K R_K$.***
A celebrated Dirichlet’s formula establishes the equality

\[ h_K R_K = \frac{\sqrt{N}}{2} L(1, \chi_N) \]

where

- \( \chi \) 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 $c_{τ−1}$ (in particular $N = pq$, with $p = q = 3 \mod 4$) is not greater than the complexity for evaluating the series*

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

*with an approximation of the order $O((\ln N)^a)$, $a > 0$.**
The direct computation of \( L(1, \chi_N) \) is impractical when \( N \) is large. Using the functional equation, the following expression was derived

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

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 $h_K R_K$ is computable with a good approximation, i.e. $O((\ln N)^\kappa)$, then it is possible to factorize with the same complexity.
Bibliography


