EULER'S FAMOUS PRIME GENERATING POLYNOMIAL AND THE CLASS NUMBER OF IMAGINARY QUADRATIC FIELDS

Autor(en): **Ribenboim, Paulo**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **34 (1988)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-56587

L'Enseignement Mathématique, t. 34 (1988), p. 23-42

EULER'S FAMOUS PRIME GENERATING POLYNOMIAL AND THE CLASS NUMBER OF IMAGINARY QUADRATIC FIELDS

by Paulo RIBENBOIM

This is the text of a lecture at the University of Rome, on May 8, 1986. The original notes disappeared when my luggage was stolen in Toronto (!); however, I had given a copy to my friend Paolo Maroscia, who did not have his luggage stolen in Rome (!) and was very kind to let me consult his copy. It is good to have friends.

INTRODUCTION

Can a non-constant polynomial, with integral coefficients, assume only prime values?

No! because of the following

THEOREM. *If* $f(X) \in \mathbf{Z}[X]$, $\deg(f) > 0$, *there exist infinitely many natural numbers* n *such that* $f(n)$ *is composite.*

Proof. It is true if $f(n)$ is composite for every $n \geqslant 1$. Assume that there exists $n_0 \geqslant 1$ such that $f(n_0) = p$ is a prime. Since $\lim_{n \to \infty} |f(n)| = \infty$, there exists $n_1 \geqslant n_0$ such that if $n \geqslant n_1$ then $|f(n)| > p$. Take any h such that $n_0 + ph \geqslant n_1$. Then $|f(n_0+ph)| > p$, but $f(n_0+ph) = f(n_0) + (\text{multiple of } p) = \text{multiple of } p$, so $|f(n_0+ph)|$ is composite. □

On the other hand, must a non-constant polynomial $f(X) \in \mathbf{Z}[X]$ always assume a prime value?

The question is interesting if $f(X)$ is irreducible, primitive (that is, the greatest common divisor of its coefficients is equal to 1) and, even more, there is no prime p dividing all values $f(n)$ (for arbitrary integers n).

Bouniakowsky, and later Schinzel & Sierpiński (1958) conjectured that any polynomial $f(X) \in \mathbf{Z}[X]$ satisfying the above conditions assumes a prime value. This has never been proved for arbitrary polynomials. For the specific

polynomials $f(X) = aX + b$, with $gcd(a, b) = 1$, it is true — this is nothing else than the famous theorem of Dirichlet: every arithmetic progression

$$\{a + kb \mid k = 0, 1, 2, ...\} \quad \text{with} \quad gcd(a, b) = 1 ,$$

contains infinitely many primes.

In my new book entitled "The Book of Prime Number Records" (Springer Verlag, 1988), I indicated many astonishing consequences of the hypothesis of Bouniakowsky, which were derived by Schinzel & Sierpiński. But this is not the subject of the present lecture.

Despite the theorem and what I have just said, for many polynomials it is easy to verify that they assume prime values, and it is even conceivable that they assume prime values at many consecutive integers. For example, Euler's famous polynomial $f(X) = X^2 + X + 41$ is such that $f(n)$ is a prime for $n = 0, 1, ..., 39$ (40 successive prime values):

41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.

However, $f(40) = 40^2 + 40 + 41 = 40 \times 41 + 41 = 41^2$.
Note that if $n > 0$ then $(-n)^2 + (-n) + 41 = (n-1)^2 + (n-1) + 41$, so $X^2 + X + 41$ assumes also prime values for all integers

$$n = -40, -39, ..., -2, -1 .$$

Which other polynomials are like the above?

Some of these polynomials may be easily obtained from $X^2 + X + c$ by just changing X into $X - a$, for some $a \geqslant 1$. For example, $(X-a)^2 + (X-a) + 41 = X^2 - (2a-1)X + (a^2-a+41)$; taking $a = 1$ gives $X^2 - X + 41$, which assumes primes values for every integer n, $-39 \leqslant n \leqslant 40$, while taking $a = 40$, gives $X^2 - 79X + 1601$, which assumes primes values for every integer n, $0 \leqslant n \leqslant 79$, but these are the same values assumed by $X^2 + X + 41$, taken twice. In summary, it is interesting to concentrate the attention on polynomials of the form $X^2 + X + c$ and their values at consecutive integers $n = 0, 1, ...$ If the value at 0 is a prime q then $c = q$. Since $(q-1)^2 + (q-1) + q = q^2$, then at best $X^2 + X + q$ assumes prime values for $0, 1, 2, ..., q - 2$ (like when $q=41$). For example, if $f(X) = X^2 + X + q$ and $q = 2, 3, 5, 11, 17, 41$ then $f(n)$ is a prime for $n = 0, 1, ..., q - 2$. However if $q = 7, 13, 19, 23, 29, 31, 37$ this is not true, as it may be easily verified.

Can one find $q > 41$ such that $X^2 + X + q$ has prime value for $n = 0, 1, ..., q - 2$?

Are there infinitely many, or only finitely many such primes q? If so, what is the largest possible q?

The same problem should be asked for polynomials of first degree $f(X) = aX + b$, with $a, b \geqslant 1$. If $f(0)$ is a prime q, then $b = q$. Then $f(q) = aq + q = (a+1)q$ is composite. So, at best, $aX + q$ assumes prime values for X equal to $0, 1, ..., q - 1$.

Can one find such polynomials? Equivalently, can one find arithmetic progressions of q prime numbers, of which the first number is equal to q?

For small values of q this is not difficult.

If $q = 3$, take: 3, 5, 7, so $f(X) = 2X + 3$.

If $q = 5$, take: 5, 11, 17, 23, 29, so $f(X) = 6X + 5$.

If $q = 7$, take: 7, 157, 307, 457, 607, 757, 907, so $f(X) = 150X + 7$.

Quite recently, Keller communicated to me that for $q = 11, 13$ the smallest such arithmetic progressions are given by polynomials $f(X) = d_{11}X + 11$, respectively $f(X) = d_{13}X + 13$ with

$$d_{11} = 1536160080 = 2 \times 3 \times 5 \times 7 \times 7315048,$$
$$d_{13} = 9918821194590 = 2 \times 3 \times 5 \times 7 \times 11 \times 4293861989;$$

this determination required a considerable amount of computation, done by Keller & Löh.

It is not known whether for every prime q there exists an arithmetic progression of q primes of which the first number is q. Even the problem of finding arbitrarily large arithmetic progressions consisting only of prime numbers (with no restriction on the initial term or the difference) is still open. The largest known such arithmetic progression consists of 19 primes, and was found by Pritchard (1985).

The determination of all polynomials $f(X) = X^2 + X + q$ such that $f(n)$ is a prime for $n = 0, 1, ..., q - 2$, is intimately related with the theory of imaginary quadratic fields. In order to understand this relationship, I shall indicate now the main results which will be required.

A) Quadratic extensions

Let d be an integer which is not a square, and let $K = \mathbf{Q}(\sqrt{d})$ be the field of all elements $\alpha = a + b\sqrt{d}$, where $a, b \in \mathbf{Q}$. There is no loss of generality to assume that d is square-free, hence $d \not\equiv 0 \pmod 4$. $K \mid \mathbf{Q}$ is a quadratic extension, that is, K is a vector space of dimension 2 over $\mathbf{Q}$.

Conversely, if K is a field, which is a quadratic extension of $\mathbf{Q}$, then it is necessarily of the form $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer.

If $d > 0$ then K is a subfield of the field $\mathbf{R}$ of real numbers: it is called a real quadratic field.

If $d < 0$ then K is not a subfield of $\mathbf{R}$, and it is called an imaginary quadratic field.

If $\alpha = a + b\sqrt{d} \in K$, with $a, b \in \mathbf{Q}$, its conjugate is $\alpha' = a - b\sqrt{d}$. Clearly, $\alpha = \alpha'$ exactly when $\alpha \in \mathbf{Q}$.

The norm of α is $N(\alpha) = \alpha\alpha' = a^2 - db^2 \in \mathbf{Q}$. It is obvious that $N(\alpha) \neq 0$ exactly when $\alpha \neq 0$. If $\alpha, \beta \in K$ then $N(\alpha\beta) = N(\alpha)\,N(\beta)$; in particular, if $\alpha \in \mathbf{Q}$ then $N(\alpha) = \alpha^2$.

The trace of α is $\mathrm{Tr}(\alpha) = \alpha + \alpha' = 2a \in \mathbf{Q}$. If $\alpha, \beta \in K$ then $\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$; in particular, if $\alpha \in \mathbf{Q}$ then $\mathrm{Tr}(\alpha) = 2\alpha$.

It is clear that α, α' are the roots of the quadratic equation $X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) = 0$.

B) Rings of integers

Let $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer.

$\alpha \in K$ is an algebraic integer when there exist integers $m, n \in \mathbf{Z}$ such that $\alpha^2 + m\alpha + n = 0$.

Let A be the set of all algebraic integers of K. A is a subring of K, which is the field of fractions of A, and $A \cap \mathbf{Q} = \mathbf{Z}$. If $\alpha \in A$ then the conjugate $\alpha' \in A$. Clearly, $\alpha \in A$ if and only if both $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ are in $\mathbf{Z}$.

Here is a criterion for the element $\alpha = a + b\sqrt{d}$ $(a, b \in \mathbf{Q})$ to be an algebraic integer: $\alpha \in A$ if and only if

$$\begin{cases} 2a = u \in \mathbf{Z}, \quad 2b = v \in \mathbf{Z} \\ u^2 - d\,v^2 \equiv 0 \pmod 4. \end{cases}$$

Using this criterion, it may be shown:

If $d \equiv 2$ or $3 \pmod 4$ then $A = \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}$.

If $d \equiv 1 \pmod 4$ then $A = \left\{ \dfrac{a + b\sqrt{d}}{2} \;\middle|\; a, b \in \mathbf{Z},\ a \equiv b \pmod 2 \right\}$.

If $\alpha_1, \alpha_2 \in A$ are such that every element $\alpha \in A$ is uniquely of the form $\alpha = m_1\alpha_1 + m_2\alpha_2$, with $m_1, m_2 \in \mathbf{Z}$, then $\{\alpha_1, \alpha_2\}$ is called an integral basis of A. In other words, $A = \mathbf{Z}\alpha_1 \oplus \mathbf{Z}\alpha_2$.

If $d \equiv 2$ or $3 \pmod 4$ then $\{1, \sqrt{d}\}$ is an integral basis of A.

If $d \equiv 1 \pmod 4$ then $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis of A.

C) Discriminant

Let $\{\alpha_1, \alpha_2\}$ be an integral basis. Then

$$D = D_K = \det \begin{pmatrix} \mathrm{Tr}(\alpha_1^2) & \mathrm{Tr}(\alpha_1\alpha_2) \\ \mathrm{Tr}(\alpha_1\alpha_2) & \mathrm{Tr}(\alpha_2^2) \end{pmatrix}$$

is independent of the choice of the integral basis. It is called the discriminant of K. It is a non-zero integer.

If $d \equiv 2$ or $3 \pmod 4$ then

$$D = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} \quad \text{so } D = 4d\,.$$

If $d \equiv 1 \pmod 4$ then

$$D = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) \\ \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) & \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right)^2 \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} \text{ so } \quad D = d\,.$$

Every discriminant is $D \equiv 0$ or $1 \pmod 4$.

In terms of the discriminant,

$$A = \left\{ \frac{a + b\sqrt{D}}{2} \,\middle|\, a, b \in \mathbf{Z}\,, \quad a^2 \equiv Db^2 \pmod 4 \right\}.$$

D) Decomposition of primes

Let $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer, let A be the ring of integers of K.

The ideal $P \neq 0$ of A is a prime ideal if the residue ring A/P has no zero-divisors.

If P is a prime ideal there exists a unique prime number p such that $P \cap \mathbf{Z} = \mathbf{Z}p$, or equivalently, $P \supseteq Ap$.

If I, J are non-zero ideals of A, it is said that I divides J when there exists an ideal I_1 of A such that $I \,.\, I_1 = J$.

The prime ideal P containing the prime number p divides the ideal Ap.

If I is a non-zero ideal of A then the residue ring A/I is finite. The norm of I is $N(I) = \#(A/I)$.

Properties of the norm:

If I, J are non-zero ideals, then $N(I \,.\, J) = N(I)\, N(J)$.

If I divides J then $N(I)$ divides $N(J)$.

If $\alpha \in A$, $\alpha \neq 0$, then $N(A\alpha) = |\, N(\alpha)\,|$ (absolute value of the norm of α). In particular, if $a \in \mathbf{Z}$ then $N(Aa) = a^2$.

If the prime ideal P divides Ap then $N(P)$ is equal to p or to p^2.

Every ideal $I \neq 0$ is, in unique way, the product of powers of prime ideals:

$$I = \prod_{i=1}^{n} P_i^{e_i} .$$

If I, J are non-zero ideals, if $I \supseteq J$ then I divides J.

Every ideal $I \neq 0$ may be generated by two elements, of which one may be chosen in $\mathbf{Z}$; if $I \cap \mathbf{Z} = \mathbf{Z}n$ then $I = An + A\alpha$ for some $\alpha \in A$. In this case, the following notation is used: $I = (n, \alpha)$.

Consider now the special case where p is a prime number. Then Ap is of one of the following types:

$$\begin{cases} Ap = P^2, & \text{where } P \text{ is a prime ideal: } p \text{ is ramified in } K. \\ Ap = P, & \text{where } P \text{ is a prime ideal: } p \text{ is inert in } K. \\ Ap = P_1 P_2, & \text{where } P_1, P_2 \text{ are distinct prime ideals: } p \text{ is decomposed or splits in } K. \end{cases}$$

Note also that if $Ap = I \,.\, J$, where I, J are any ideals (different from A), not necessarily distinct, then I, J must in fact be prime ideals.

I shall now indicate when a prime number p is ramified, inert or decomposed, and also give generators of the prime ideals of A. There are two cases: $p \neq 2$, $p = 2$.

Denote by $\left(\frac{d}{p}\right)$ the Legendre symbol, so

$$\begin{cases} \left(\frac{d}{p}\right) = 0 & \text{when } p \text{ divides } d, \\ \left(\frac{d}{p}\right) = +1 & \text{when } d \text{ is a square modulo } p, \\ \left(\frac{d}{p}\right) = -1 & \text{when } d \text{ is not a square modulo } p. \end{cases}$$

Let $p \neq 2$.

1) If p divides d then $Ap = (p, \sqrt{d})^2$.
2) If p does not divide d and there does not exist $a \in \mathbf{Z}$ such that $d \equiv a^2 \pmod{p}$ then Ap is a prime ideal.
3) If p does not divide d and there exists $a \in \mathbf{Z}$ such that $d \equiv a^2 \pmod{p}$ then $Ap = (p, a+\sqrt{d})\,(p, a-\sqrt{d})$.

Hence

1) p is ramified if and only if $\left(\frac{d}{p}\right) = 0$.
2) p is inert if and only if $\left(\frac{d}{p}\right) = -1$.
3) p is decomposed if and only if $\left(\frac{d}{p}\right) = +1$.

Proof. The proof is divided into several parts.

a) If $\left(\frac{d}{p}\right) = -1$ then Ap is a prime ideal.

Otherwise $Ap = P \,.\, P'$ or P^2, with $P \cap \mathbf{Z} = \mathbf{Z}p$. Let $\alpha \in A$ be such that $P = (p, \alpha) \supseteq A\alpha$ so $P \mid A\alpha$, hence p divides $N(P)$, which divides $N(A\alpha)$ $= |N(\alpha)|$. If $p \mid \alpha$ then $\frac{\alpha}{p} \in A$ and $P = Ap \,.\, \left(1, \frac{\alpha}{p}\right) = Ap$, which is absurd. So $p \nmid \alpha$. Then,

$$\begin{cases} d \equiv 2 \text{ or } 3 \pmod 4 \\ \\ d \equiv 1 \pmod 4 \end{cases} \Rightarrow \begin{cases} \alpha = a + b\sqrt{d}\,, & \text{with} \quad a, b \in \mathbf{Z} \\ \\ \alpha = \dfrac{a + b\sqrt{d}}{2}\,, & \text{with} \quad a, b \in \mathbf{Z}, \quad a \equiv b \pmod 2 \end{cases}$$

$$\Rightarrow \begin{cases} N(\alpha) = a^2 - db^2 \\ \\ N(\alpha) = \dfrac{a^2 - db^2}{4} \end{cases} \Rightarrow \quad p \text{ divides } a^2 - db^2\,,$$

hence $a^2 \equiv db^2 \pmod{p}$ and so $p \nmid b$ (otherwise $p \mid a$, hence $p \mid \alpha$, which is absurd).

Let b' be such that $bb' \equiv 1 \pmod{p}$, so $(ab')^2 \equiv d \pmod{p}$, therefore either $p \mid d$ or $\left(\frac{d}{p}\right) = +1$, which is a contradiction.

b) If $\left(\frac{d}{p}\right) = 0$ then $Ap = (p, \sqrt{d})^2$.

Indeed, let $P = (p, \sqrt{d})$, so $P^2 = (p^2, p\sqrt{d}, d) = Ap\left(p, \sqrt{d}, \frac{d}{p}\right)$ since $\frac{d}{p} \in \mathbf{Z}$. But d is square-free, so $gcd\left(p, \frac{d}{p}\right) = 1$, hence $P^2 = Ap$ and this implies that P is a prime ideal.

c) If $\left(\frac{d}{p}\right) = -1$ then $Ap = (p, a+\sqrt{d})\,(p, a-\sqrt{d})$, where $1 \leqslant a \leqslant p-1$ and $a^2 \equiv d \pmod{p}$.

Indeed,

$$(p, a+\sqrt{d})\,(p, a-\sqrt{d}) = (p^2, pa+p\sqrt{d}, pa-p\sqrt{d}, a^2-d)$$

$$= Ap\left(p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p}\right) = Ap\left(p, a+\sqrt{d}, a-\sqrt{d}, 2a, \frac{a^2-d}{p}\right) = Ap,$$

because $gcd\,(p, 2a) = 1$. If one of the ideals $(p, a+\sqrt{d})$, $(p, a-\sqrt{d})$ is equal to A, so is the other which is not possible.

So $(p, a+\sqrt{d})$, $(p, a-\sqrt{d})$ are prime ideals. They are distinct: if $(p, a+\sqrt{d}) = (p, a-\sqrt{d})$ then they are equal to their sum

$$(p, a+\sqrt{d}, a-\sqrt{d}) = (p, a+\sqrt{d}, a-\sqrt{d}, 2a) = A,$$

which is an absurd.

Finally, these three cases are exclusive and exhaustive, so the converse assertions are also true. □

Note. If $d \equiv 1 \pmod{4}$ and $d \equiv a^2 \pmod{p}$ then

$$(p, a+\sqrt{d}) = (p, l(a-1)+\omega),$$

where $\omega = \frac{1+\sqrt{d}}{2}$ and $2l \equiv 1 \pmod{p}$. Hence, if $\left(\frac{d}{p}\right) \neq -1$ there exists $b \in \mathbf{Z}$, $0 \leqslant b \leqslant p-1$, such that p divides $N(b+\omega)$ and moreover if $b = p-1$ then $d \equiv 1 \pmod{p}$.

Indeed, $a + \sqrt{d} = a - 1 + 2\omega$. If $2l \equiv 1 \pmod{p}$ then

$$(p, a+\sqrt{d}) = (p, (a-1)+2\omega) = (p, l(a-1)+\omega).$$

If $\left(\frac{d}{p}\right) \neq -1$ then there exists a prime ideal P dividing Ap, where

$$P = (p, a+\sqrt{d}), 0 \leqslant a \leqslant p-1 .$$

So $P = (p, b+\omega)$ with $0 \leqslant b \leqslant p-1$, $b \equiv l(a-1) \pmod{p}$.

Since $P \supseteq A(b+\omega)$ then p divides $N(P)$, which divides $N(b+\omega)$. Finally, if p divides $N(p-1+\omega) = N\left(\frac{2p-1+\sqrt{d}}{2}\right) = \frac{(2p-1)^2 - d}{4}$ then p divides $\frac{1-d}{4}$ so $d \equiv 1 \pmod{p}$.

Let $p = 2$.

If $d \equiv 2 \pmod 4$ then $A2 = (2, \sqrt{d})^2$.

If $d \equiv 3 \pmod 4$ then $A2 = (2, 1+\sqrt{d})^2$.

If $d \equiv 1 \pmod 8$ then $A2 = (2, \omega)(2, \omega')$.

If $d \equiv 5 \pmod 8$ then $A2$ is a prime ideal.

Hence

1) 2 is ramified if and only if $d \equiv 2$ or $3 \pmod 4$.
2) 2 is inert if and only if $d \equiv 5 \pmod 8$.
3) 2 is decomposed if and only if $d \equiv 1 \pmod 8$.

Proof. The proof is divided into several parts.

a) If $d \equiv 5 \pmod 8$ then $A2$ is a prime ideal.

Otherwise, $A2 = P \,.\, P'$ or P^2, with $P \cap \mathbf{Z} = \mathbf{Z}2$. Then there exists $\alpha \in A$ such that $P = (2, \alpha) \supseteq A\alpha$, so P divides $A\alpha$ and 2 divides $N(P)$, which divides $N(\alpha)$.

If $2 \mid \alpha$ then $P = A2\left(l, \frac{\alpha}{2}\right) = A2$, which is absurd. Thus

$$2 \nmid \alpha = \frac{a + b\sqrt{d}}{2}, \quad \text{with} \quad a \equiv b \pmod 2, \quad \text{so} \quad N(\alpha) = \frac{a^2 - db^2}{4}.$$

From $2 \mid N(\alpha)$ then 8 divides $a^2 - db^2 \equiv a^2 - 5b^2 \equiv a^2 + 3b^2 \pmod 8$.

If a, b are odd then $a^2 \equiv b^2 \equiv 1 \pmod 8$, so $a^2 + 3b^2 \equiv 4 \pmod 8$, which is absurd. So a, b are even, $a = 2a'$, $b = 2b'$, and $\alpha = a' + b'\sqrt{d}$, 2 divides $N(\alpha) = a'^2 - db'^2$.

Since d is odd, then a', b' are both even or both odd.

If a', b' are even then 2 divides α, which is absurd.

If a', b' are odd then $\alpha = a' + b'\sqrt{d}$ = (multiple of 2) + 1 + $\sqrt{d}$ = (multiple of 2) + 2ω = (multiple of 2), which is absurd.

b) If $d \equiv 1 \pmod 8$ then $A2 = (2, \omega)(2, \omega')$.

Indeed,

$$(2, \omega)(2, \omega') = \left(4, 2\omega, 2\omega', \frac{1-d}{4}\right) = A2\left(2, \omega, \omega', \frac{1-d}{8}\right) = A2,$$

because $\omega + \omega' = 1$.

Also $(2, \omega) \neq (2, \omega')$, otherwise these ideals are equal to their sum $(2, \omega, \omega') = A$, because $\omega + \omega' = 1$.

c) If $d \equiv 2$ or $3 \pmod 4$ then $A2 = (2, \sqrt{d})^2$, respectively $(2, 1+\sqrt{d})^2$.

First let $d = 4e + 2$ then

$$(2, \sqrt{d})^2 = (4, 2\sqrt{d}, d) = A2(2, \sqrt{d}, 2e+1) = A2,$$

so $(2, \sqrt{d})$ is a prime ideal.

Now, let $d = 4e + 3$, then

$$(2, 1+\sqrt{d})^2 = (4, 2+2\sqrt{d}, 1+d+2\sqrt{d}) = (4, 2+2\sqrt{d}, 4(e+1)+2\sqrt{d})$$
$$= A2(2, 1+\sqrt{d}, 2(e+1)+\sqrt{d}) = A2(2, 2e+1, 1+\sqrt{d}, 2(e+1)+\sqrt{d}) = A2$$

and so $(2, 1+\sqrt{d})$ is a prime ideal.

Finally, these three cases are exclusive and exhaustive, so the converse assertions also hold. □

E) Units

The element $\alpha \in A$ is a unit if there exists $\beta \in A$ such that $\alpha\beta = 1$. The set U of units is a group under multiplication. Here is a description of the group of units in the various cases. First let $d < 0$.

Let $d \neq -1, -3$. Then $U = \{\pm 1\}$.

Let $d = -1$. Then $U = \{\pm 1, \pm i\}$, with $i = \sqrt{-1}$.

Let $d = -3$. Then $U = \{\pm 1, \pm \rho, \pm \rho^2\}$, with $\rho^3 = 1$, $\rho \neq 1$, i.e. $\rho = \dfrac{-1+\sqrt{-3}}{2}$.

Let $d > 0$. Then the group of units is the product $U = \{\pm 1\} \times C$, where C is a multiplicative cyclic group. Thus $C = \{\varepsilon^n \mid n \in \mathbf{Z}\}$, where ε is the smallest unit such that $\varepsilon > 1$. ε is called the fundamental unit.

F) THE CLASS NUMBER

The theory of quadratic number fields originated with the study of binary quadratic forms $aX^2 + bXY + cY^2$ (where a, b, c are integers and $ac \neq 0$). The discriminant of the form is, by definition, $D = b^2 - 4ac$. Note that $D \equiv 0$ or $1 \pmod 4$; let $d = \frac{D}{4}$ or $d = D$, respectively.

An integer m is said to be represented by the form if there exist integers x, y such that $m = ax^2 + bxy + cy^2$.

If a form $a'X'^2 + b'X'Y' + c'Y'^2$ is obtained from the above form by a linear change of variables

$$\begin{cases} X = hX' + kY' \\ Y = mX' + nY' \end{cases}$$

where h, k, m, n are integers and the determinant is $hn - km = 1$, then the two forms represent the same integers. In this sense, it is reasonable to consider such forms as being equivalent. Clearly, equivalent forms have the same discriminant.

In "Disquisitiones Arithmeticae" Gauss classified the binary quadratic forms with a given discriminant D. Gauss defined an operation of composition between equivalence classes of forms of a given discriminant. The classes constitute a group under this operation. Gauss showed that, for any given discriminant D, there exist only finitely many equivalence classes of binary quadratic forms.

The theory was later reinterpreted, associating to each form $aX^2 + bXY + cY^2$ of discriminant D, the ideal I of $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{D})$ generated by a and $\frac{-b + \sqrt{D}}{2}$. Define two non-zero ideals I, I' to be equivalent when there exists a non-zero element $\alpha \in \mathbf{Q}(\sqrt{d})$ such that $I = A\alpha . I'$. Then, equivalent binary quadratic forms correspond to equivalent ideals, and the composition of classes of forms corresponds to the multiplication of equivalence classes of ideals. Thus, $\mathbf{Q}(\sqrt{d})$ has finitely many classes of ideals. Denote by $h = h(d)$ the number of classes of ideals, or class number of the field $\mathbf{Q}(\sqrt{d})$.

The class number $h(d) = 1$ exactly when every ideal of $\mathbf{Q}(\sqrt{d})$ is a principal ideal.

Gauss conjectured that for every $h \geqslant 1$ there exist only finitely many imaginary quadratic fields $\mathbf{Q}(\sqrt{d})$ (with $d < 0$) such that the class number is equal to h. Soon, I shall say more about this conjecture.

I shall now indicate how to calculate the class number of the quadratic field $\mathbf{Q}(\sqrt{D})$. Define the real number θ as follows:

$$\theta = \begin{cases} \frac{1}{2}\sqrt{D} & \text{if} \quad D > 0\,, \\ \\ \frac{2}{\pi}\sqrt{-D} & \text{if} \quad D < 0\,. \end{cases}$$

A non-zero ideal I of A is said to be normalized if $N(I) \leqslant [\theta]$ (the largest integer less than or equal to θ). The ideal I is said to be primitive if there does not exist any prime number p such that Ap divides I.

Let $\mathcal{N}$ denote the set of normalized primitive ideals of A.

If $I \in \mathcal{N}$, if p is a ramified prime then $p^2 \nmid N(I)$, and if p is an inert prime, then $p \nmid N(I)$. So,

$$N(I) = \prod_{r \text{ ramified}} r \times \prod_{p \text{ decomposed}} p^{e(p)}\,.$$

It may be shown that every class of ideals contains a primitive normalized ideal. Since for every $m \geqslant 1$ there exist at most finitely many ideals I of A such that $N(I) = m$, this implies, once more, that the number of classes of ideals is finite.

Note that if $\mathcal{N}$ consists only of the unit ideal $A = A.1$, then $h = 1$. Thus, if every prime p such that $p \leqslant [\theta]$ is inert, then $h = 1$. Indeed, if $I \in \mathcal{N}$ then $N(I) = 1$, so I is the unit ideal, hence $h = 1$.

Denote by $N(\mathcal{N})$ the set of integers $N(I)$, where $I \in \mathcal{N}$.

In order to decide if the ideals $I, J \in \mathcal{N}$ are equivalent, it will be necessary to decide which integers $m \in N(\mathcal{N})$ are of the form $m = N(A\alpha)$.

Let $m \geqslant 1$, let

$$\alpha = \begin{cases} u + v\sqrt{d} & \text{when} \quad d \equiv 2 \text{ or } 3 \pmod 4, \quad \text{with} \quad u, v \in \mathbf{Z}\,, \\ \\ \dfrac{u + v\sqrt{d}}{2} & \text{when} \quad d \equiv 1 \pmod 4, \qquad \text{with} \quad u, v \in \mathbf{Z},\ u \equiv v \pmod 2\,. \end{cases}$$

Then: $A\alpha$ is a primitive ideal with $N(A\alpha) = m$ if and only if

$$\begin{cases} m = |\,u^2 - dv^2\,|\,, \ gcd\,(u, v) = 1 & \text{if} \quad d \equiv 2 \text{ or } 3 \pmod 4 \\ m = \dfrac{|\,u^2 - dv^2\,|}{4}, \ gcd\left(\dfrac{u-v}{2},\ v\right) = 1 & \text{if} \quad d \equiv 1 \pmod 4 \end{cases}$$

(this is called the primitive representation of m).

Proof. Let $d \equiv 2$ or $3 \pmod 4$, $m = N(A\alpha) = |u^2 - dv^2|$, also $gcd(u, v) = 1$, because $A\alpha$ is primitive.

Let $d \equiv 1 \pmod 4$, $m = N(A\alpha) = \dfrac{|u^2 - dv^2|}{4}$, also if p divides $\dfrac{u - v}{2}$ and p divides v then p divides $\alpha = \dfrac{u - v}{2} + v\left(\dfrac{1+\sqrt{d}}{2}\right)$, against the hypothesis.

Conversely, let $d \equiv 2$ or $3 \pmod 4$, so $N(A\alpha) = m$: if p divides $A\alpha$, since $\{1, \sqrt{d}\}$ is an integral basis then $p \mid u$, $p \mid v$, which is absurd.

Let $d \equiv 1 \pmod 4$, so $N(A\alpha) = m$; if p divides $A\alpha$, since

$$\alpha = \frac{u - v}{2} + v\left(\frac{1+\sqrt{d}}{2}\right) \quad \text{and} \quad \left\{1, \frac{1 + \sqrt{d}}{2}\right\}$$

is integral basis, then p divides $\dfrac{u - v}{2}$ and v, which is absurd. □

Calculation of the class number.

Let $d > 0$, so $\theta = \frac{1}{2}\sqrt{D}$.

$[\theta] = 1$.

Since $1 \leqslant \frac{1}{2}\sqrt{D} < 2$ then $4 \leqslant D < 16$, with $D \equiv 0$ or $1 \pmod 4$, hence $D \in \{4, 5, 8, 9, 12, 13\}$, and therefore $d \in \{5, 2, 3, 13\}$.

Now $N(\mathcal{N}) = \{1\}$, hence $\mathcal{N}$ consists only of the unit ideal, and therefore $h = 1$.

$[\theta] = 2$.

Since $2 \leqslant \frac{1}{2}\sqrt{D} < 3$ then $16 \leqslant D < 36$, with $D \equiv 0$ or $1 \pmod 4$, hence $D \in \{16, 17, 20, 21, 24, 25, 28, 29, 32, 33\}$ and therefore $d \in \{17, 21, 6, 7, 29, 33\}$.

Now $N(\mathcal{N}) = \{1, 2\}$.

Take, for example $d = 17$. Since $17 \equiv 1 \pmod 8$ then $A2 = P \cdot P'$, $N(P) = N(P') = 2$, $2 = \dfrac{|3^2 - 17 \times 1^2|}{4}$, $gcd\left(\dfrac{3-17}{2}, 17\right) = 1$, hence

$$P = A\alpha, \quad \alpha = \frac{3 + \sqrt{17}}{2},$$

$$P' = A\alpha', \quad \alpha' = \frac{3 - \sqrt{17}}{2}.$$

Therefore the class number is $h = 1$.

Let $d = 21$. Since $21 \equiv 5 \pmod 8$ then $A2$ is a prime ideal, 2 is inert, hence $h = 1$.

Let $d = 6$, then 2 divides $24 = D$, so 2 is ramified, $A2 = P^2$, and $2 = |2^2 - 6 \times 1^2|$, $gcd(2, 1) = 1$, hence $P = A\alpha$, with $\alpha = 2 + \sqrt{6}$. Therefore $h = 1$.

$[\theta] = 3$.

Since $3 \leqslant \frac{1}{2}\sqrt{D} < 4$ then $36 \leqslant D < 64$, with $D \equiv 0$ or $1 \pmod 4$, hence

$$D \in \{36, 37, 40, 41, 44, 45, 48, 49, 52, 53, 56, 57, 60, 61\}$$

and therefore

$$d \in \{37, 10, 41, 11, 53, 14, 57, 15, 61\}.$$

Now $N(\mathcal{N}) = \{1, 2, 3\}$.

Take, for example $d = 10$. Since 2 divides $40 = D$ then 2 is ramified, $A2 = R^2$. Since $\left(\frac{10}{3}\right) = \left(\frac{1}{3}\right) = 1$ then 3 is decomposed, $A3 = P.P'$. The ideals R, P, P' are primitive.

2 has no primitive representation: if $2 = |u^2 - 10v^2|$ then $u^2 = 10v^2 \pm 2 \equiv \pm 2 \pmod{10}$, which is impossible.

3 has no primitive representation: if $3 = |u^2 - 10v^2|$ then $u^2 = 10v^2 \pm 3 \equiv \pm 3 \pmod{10}$, which is impossible.

Thus, R, P, P' are not principal ideals. The ideals RP, RP' are primitive. Also

$$-2 \times 3 = -6 = 2^2 - 10 \times 1^2, \quad gcd(2, 1) = 1, \quad 2 \times 3 = N(RP) = N(RP'),$$

hence RP, RP' are principal ideals. In conclusion, $h = 2$.

Let $d < 0$, so $\theta = \frac{2}{\pi}\sqrt{-D}$.

$[\theta] = 1$.

Since $1 \leqslant \frac{2}{\pi}\sqrt{-D} < 2$ then $\frac{\pi^2}{4} \leqslant |D| < \pi^2$, and $|D| \equiv 0$ or $3 \pmod 4$, hence $|D| \in \{3, 4, 7, 8\}$, therefore $d \in \{-3, -1, -7, -2\}$. Now $N(\mathcal{N}) = 1$, hence $\mathcal{N}$ consists only of the unit ideal, so $h = 1$.

$[\theta] = 2$.

Since $2 \leqslant \frac{2}{\pi}\sqrt{-D} < 3$ then $\pi^2 \leqslant |D| < \frac{9}{4}\pi^2$, and $|D| \equiv 0$ or $3 \pmod 4$, hence $|D| \in \{11, 12, 15, 16, 19, 20\}$, therefore $d \in \{-11, -15, -19, -5\}$.

Take, for example, $d = -11$. Since $-11 \equiv 5 \pmod 8$ then 2 is inert, and therefore $h = 1$.

Let $d = -5$. Since 2 divides $D = -20$ so 2 is ramified, $A2 = P^2$.

2 has no primitive representation: if $2 = |u^2 + 5v^2|$ then $u^2 = -5v^2 + 2 \equiv 2 \pmod 5$, which is impossible. Also $-5 \equiv 3 \pmod 4$. So P is not principal and $h = 2$.

Let $d = -15$. Since $-15 \equiv 1 \pmod 8$ then $A2 = P \,.\, P'$.

2 has no primitive representation: if

$$2 = \frac{|u^2 + 15v^2|}{4}, \quad \text{with} \quad gcd\left(\frac{u-v}{2}, v\right) = 1,$$

then $u^2 + 15v^2 = 8$, so $u^2 \equiv 3 \pmod 5$, which is impossible. Also $-15 \equiv 1 \pmod 4$. Since P, P' are not principal ideals, then $h = 2$.

Let $d = -19$. Since $-19 \equiv 5 \pmod 8$ so 2 is inert, hence $h = 1$.

$[\theta] = 3$.

Since $3 \leqslant \frac{2}{\pi}\sqrt{-D} < 4$ then $\frac{9\pi^2}{4} \leqslant |D| < 4\pi^2$, and $|D| \equiv 0$ or $3 \pmod 4$, hence

$$|D| \in \{23, 24, 27, 28, 31, 32, 35, 36, 39\},$$

and therefore

$$d \in \{-23, -6, -31, -35, -39\}.$$

Take $d = -31$. Since $-31 \equiv 1 \pmod 8$ then $A2 = P \,.\, P'$. Since $\left(\frac{-31}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{1}{3}\right) = -1$, so $A3$ is a prime ideal.

2 has no primitive representation: if

$$2 = \frac{|u^2 + 31v^2|}{4}, \quad \text{with} \quad gcd\left(\frac{u-v}{2}, v\right) = 1,$$

then $8 = u^2 + 31v^2$, which is impossible. Since $-31 \equiv 1 \pmod 4$ then P, P' are not principal ideals. If P, P' are equivalent then $P = P' \,.\, A\alpha$ so $P^2 = P \,.\, P' \,.\, A\alpha = A(2\alpha)$, so $4 = N(P^2) = 4N(A\alpha)$, hence $N(A\alpha) = 1$, thus $A\alpha = A$, and $P = P'$, which is absurd. In conclusion, $h = 3$.

These examples are enough to illustrate how to compute the class number, at least for small values of the discriminant.

Determination of all quadratic fields with class number 1.

Let $d > 0$.

It is conjectured that there exist infinitely many $d > 0$ such that $\mathbf{Q}(\sqrt{d})$ has class number 1. This question is difficult to settle, but it is expected that the conjecture is true.

For example, there exist 142 fields $\mathbf{Q}(\sqrt{d})$, with $2 \leqslant d < 500$ having class number 1.

Let $d < 0$.

It was seen that if $\mathcal{N}$ consists only of the unit ideal, then $h = 1$. But conversely:

If $d < 0$ and $h = 1$ then $\mathcal{N} = \{A\}$.

Proof. If $|D| \leqslant 7$, it is true. Let $|D| > 7$, let $I \in \mathcal{N}$, $I \neq A$, so there exists a prime ideal P dividing I. Then $N(P) = p$ or p^2, where p is a prime number. If $N(P) = p^2$ then p is inert and $Ap = P$ divides I, so I would not be primitive, which is a contradiction. If $N(P) = p$, since P divides I then $p \leqslant N(I) \leqslant [\theta] \leqslant \frac{2}{\pi}\sqrt{|D|}$. If p has a primitive representation:

if $d \equiv 2$ or $3 \pmod 4$ then $d = \frac{D}{4}$, so $p = u^2 - dv^2$, hence $v \neq 0$, therefore $\frac{2}{\pi}\sqrt{|D|} \geqslant p \geqslant |d| = \frac{|D|}{4}$, so $7 \geqslant \frac{64}{\pi^2} \geqslant |D|$, which is absurd;

if $d \equiv 1 \pmod 4$ then $d = D$, so $p = \frac{u^2 - dv^2}{4}$, hence $v \neq 0$, therefore $\frac{2}{\pi}\sqrt{|D|} \geqslant p \geqslant \frac{|d|}{4} = \frac{|D|}{4}$, and again $7 \geqslant D$, which is absurd.

Therefore P is not a principal ideal and $h \neq 1$, which is against the hypothesis. □

Gauss developed a theory of genera and proved:

If $d < 0$ and if t is the number of distinct prime factors of D, then 2^{t-1} divides the class number of $\mathbf{Q}(\sqrt{d})$.

Hence if $h = 1$ then $D = -4$, -8 or $-p$, where p is a prime, $p \equiv 3 \pmod 4$, hence $d = -1$, -2 or $-p$.

From this discussion, it follows:

If $D = -3$, -4, -7, -8 then $h = 1$.
If $D \neq -3$, -4, -7, -8 and $D = -p$, $p \equiv 3 \pmod 4$ then $h = 1$ if and only if $\mathcal{N} = \{A\}$ and this is equivalent to the following conditions:

2 is inert in $\mathbf{Q}(\sqrt{-p})$, and if q is any odd prime, $q \leqslant [\theta]$, then $\left(\frac{-p}{q}\right) = -1$, i.e., q is inert in $\mathbf{Q}(\sqrt{-p})$.

This criterion is used in the determination of all $D < 0$, $|D| \leqslant 200$, such that $h = 1$.

$[\theta] = 1$. This gives the discriminants $D = -3, -4, -7, -8$.

$[\theta] = 2$. Now $-20 \leqslant D \leqslant -11$, with $D = -p$, $p \equiv 3 \pmod 4$, so $D = -11$ or -19.

Since $-11 \equiv 5 \pmod 8$ then 2 is inert, so if $D = -11$ then $h = 1$.

Similarly, since $-19 \equiv 5 \pmod 8$ then 2 is inert, so if $D = -19$ then $h = 1$.

$[\theta] = 3$. Now $-39 \leqslant D \leqslant -23$, with $D = -p$, $p \equiv 3 \pmod 4$, so $D = -23$ or -31. But $-23 \not\equiv 5 \pmod 8$, $-31 \not\equiv 5 \pmod 8$, so the class numbers of $\mathbf{Q}(\sqrt{-23})$ and of $\mathbf{Q}(\sqrt{-31})$ are not 1.

$[\theta] = 4$. Now $-59 \leqslant D \leqslant -40$, $D = -p$, $p \equiv 3 \pmod 4$, so $D = -43$, -47, -59. Since $-43 \equiv 5 \pmod 8$ and $\left(\frac{-43}{3}\right) = -1$ then $\mathbf{Q}(\sqrt{-43})$ has class number 1. Since $-47 \not\equiv 5 \pmod 8$ and $\left(\frac{-59}{3}\right) = 1$ then 3 is not inert. So the class numbers of $\mathbf{Q}(\sqrt{-47})$ and of $\mathbf{Q}(\sqrt{-59})$ are not equal to 1.

The same calculations yield:

$[\theta] = 5$: $D = -67$, with class number 1

$[\theta] = 6$: no discriminant

$[\theta] = 7$: no discriminant

$[\theta] = 8$: $D = -163$, with class number 1.

This process may continued beyond 200, but leads to no other discriminant for which the class number is 1. Of course, this does not allow to decide whether there exists any other such discriminant, nor to decide whether there are only finitely many imaginary quadratic fields with class number 1.

In a classical paper, Heilbronn and Linfoot showed in 1934, with analytical methods, that besides the above examples there exists at most another value of $d < 0$ for which $\mathbf{Q}(\sqrt{d})$ has class number 1. Lehmer showed that if such a discriminant d exists at all, then $|d| > 5 \times 10^9$. In 1952, Heegner proved that no other such d could exist, but his proof contained some steps which were unclear, perhaps even a gap. Baker reached

the same conclusion in 1966, with his method involving effective lower bounds on linear forms of three logarithms; this is also reported in his article of 1971. At about the same time, unaware of Heegner's result, but with similar ideas, concerning elliptic modular functions, Stark proved that no further possible value for d exists. So were determined all the imaginary quadratic fields with class number 1. It was somewhat an anticlimax when in 1968 Deuring was able to straighten out Heegner's proof. The technical details involved in these proofs are far beyond the scope of the present article.

This is the place to say that Gauss' conjecture was also solved in the affirmative. Thanks to the work of Hecke, Deuring, Mordell and Heilbronn, it was established that if $d < 0$ and $|d|$ tends to infinity, then so does the class number of $\mathbf{Q}(\sqrt{d})$. Hence, for every integer $h \geqslant 1$ there exists only finitely many fields $\mathbf{Q}(\sqrt{d})$ with $d < 0$, having class number h.

The determination of all imaginary quadratic fields with class number 2 was achieved by Baker, Stark, Weinberger.

An explicit estimate of the number of imaginary quadratic fields with a given class number was obtained by the efforts of Siegel, Goldfeld, Gross & Zagier. For this matter, I suggest reading the paper of Goldfeld (1985).

G) The main theorem

THEOREM. *Let q be a prime, let $f_q(X) = X^2 + X + q$. The following conditions are equivalent:*

1) $q = 2, 3, 5, 11, 17, 41$.

2) $f_q(n)$ *is a prime for* $n = 0, 1, 2, \ldots, q - 2$.

3) $\mathbf{Q}(\sqrt{1-4q})$ *has class number* 1.

Proof. The implication $1 \to 2$ is a simple verification.

The equivalence of the assertions 2 and 3 was first shown by Rabinovitch in 1912. In 1936, Lehmer proved once more that $2 \to 3$, while $3 \to 2$ was proved again by Szekeres (1974) and by Ayoub & Chowla (1981), who gave the simplest proof. The proof of $3 \to 1$ follows from the complete determination of all imaginary quadratic fields with class number 1. Since this implication requires deep results, I shall also give the proof of $3 \to 2$.

$2 \to 3$ Let $d = 1 - 4q < 0$, so $d \equiv 1 \pmod 4$. If $q = 2$ or 3 then $d = -7$ or -11 and $\mathbf{Q}(\sqrt{d})$ has class number 1, as it was already seen.

Assume now that $q \geqslant 5$. It suffices to show that every prime $p \leqslant \frac{2}{\pi}\sqrt{|d|}$ is inert in $\mathbf{Q}(\sqrt{d})$.

First let $p = 2$; since $q = 2t - 1$ then $d = 1 - 4q = 1 - 4(2t-1) \equiv 5 \pmod 8$, so 2 is inert in $\mathbf{Q}(\sqrt{d})$.

Now let $p \neq 2$, $p \leqslant \frac{2}{\pi}\sqrt{|d|} < \sqrt{|d|}$ and assume that p is not inert. Then $\left(\frac{d}{p}\right) \neq -1$ and, as it was noted, there exists $b \in \mathbf{Z}$, $0 \leqslant b \leqslant p-1$, such that p divides $N(b+\omega)$, where $\omega = \frac{1+\sqrt{d}}{2}$, that is, p divides

$$(b+\omega)(b+\omega') = b^2 + b(\omega+\omega') + \omega\omega' = b^2 + b + \frac{1-d}{4}$$

$$= b^2 + b + q = f_q(b).$$

It should be also noted that $b \neq p-1$, otherwise as it was shown, p divides $1 - d = 4q$, hence $p = q < \sqrt{|d|} = \sqrt{|1-4q|}$, so $q^2 < 4q - 1$, hence $q = 2$ or 3, against the hypothesis.

By hypothesis, $f_q(b)$ is therefore a prime number, hence $\sqrt{4q-1} > p = f_q(b) \geqslant f_q(0) = q$ and again $q = 2$ or 3, against the hypothesis.

This shows that every prime p less than $\frac{2}{\pi}\sqrt{|d|}$ is inert, hence $h = 1$.

$3 \to 1$ If $\mathbf{Q}(\sqrt{1-4q})$ has class number 1 then $d = 1 - 4q = -7, -11, -19, -43, -67, -163$, hence $q = 2, 3, 5, 11, 17, 41$. □

As I have already said, the proof is now complete, but it is still interesting to indicate the proof of $3 \to 2$.

Assume that $d = 1 - 4q$ and that the class number of $\mathbf{Q}(\sqrt{-d})$ is 1. Then either $d = -1, -2, -3, -7$, or $d < -7$, so $d = -p$ with $p \equiv 3 \pmod 4$ and $q > 2$.

As noted before, 2 is inert in $\mathbf{Q}(\sqrt{-p})$, so $p \equiv 3 \pmod 8$. Next, I show that if l is any odd prime, $l < q$, then $\left(\frac{l}{p}\right) = -1$. Indeed, if $\left(\frac{l}{p}\right) = 1$ then l splits in $\mathbf{Q}(\sqrt{-p})$. But $h = 1$, so there exists an algebraic integer $\alpha = \frac{a + b\sqrt{-p}}{2}$ such that $Al = A\alpha \,.\, A\alpha'$. Then $l^2 = N(Al) = N(A\alpha) \,.\, N(A\alpha')$ $= N(A\alpha)^2 = N(\alpha)^2$, so $l = N(\alpha) = \frac{a^2 + b^2 p}{4}$. Hence $p + 1 = 4q > 4l$

$= a^2 + b^2p$, thus $1 > a^2 + (b^2-1)p$ and necessarily $a^2 = 0, b^2 = 1$, hence $4l = p$, which is absurd.

Now assume that there exists $m, 0 \leqslant m \leqslant q-2$, such that $f_q(m) = m^2 + m + q$ is not a prime. Then there exists a prime l such that $l^2 \leqslant m^2 + m + q$ and $m^2 + m + q = al$, with $a \geqslant 1$. Since $m^2 + m + q$ is odd then $l \neq 2$. Also $4l^2 \leqslant (2m+1)^2 + p < \left(\frac{p-1}{2}\right)^2 + p = \left(\frac{p+1}{2}\right)^2$, hence $l < \frac{p+1}{4} = q$. As it was shown, $\left(\frac{l}{p}\right) = -1$. However,

$$4al = (2m+1)^2 + 4q - 1 = (2m+1)^2 + p,$$

hence $-p$ is a square modulo l, so by Gauss' reciprocity law,

$$1 = \left(\frac{-p}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}}\left(\frac{l}{p}\right)(-1)^{\frac{l-1}{2}\times\frac{p-1}{2}} = \left(\frac{l}{p}\right),$$

and this is absurd. □

BIBLIOGRAPHY

[1] AYOUB, R. and S. CHOWLA. On Euler's polynomial. *J. Nb. Th. 13* (1981), 443-445.

[2] BOREVICH, Z. I. and I. R. SHAFAREVICH. *Number Theory*. Academic Press, New York, 1966.

[3] COHN, H. *Advanced Number Theory*. Dover Publ., New York, 1962.

[4] GOLDFELD, D. Gauss' class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. 13* (1985), 23-37.

[5] LEHMER, D. H. On the function $x^2 + x + A$. *Sphinx 6* (1936), 212-214.

[6] PRITCHARD, P. A. Long arithmetic progressions of primes: some old, some new. *Math. of Comp. 45* (1985), 263-267.

[7] RABINOVITCH, G. Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörper. *Intern. Congress of Math.*, Cambridge, 1912, vol. 1, 418-421.

[8] RIBENBOIM, P. *Algebraic Numbers*. Wiley-Interscience, New York, 1972.

[9] —— *The Book of Prime Number Records*. Springer Verlag, New York, 1988.

[10] SCHINZEL, A. and W. SIERPIŃSKI. Sur certaines hypothèses concernant les nombres premiers. Remarques. *Acta Arithm. 4* (1958), 185-208 and *5* (1959), p. 259.

[11] SCHINZEL, A. Remarks on the paper « Sur certaines hypothèses concernant les nombres premiers ». *Acta Arithm. 7* (1961), 1-8.

[12] SZEKERES, G. On the number of divisors of $x^2 + x + A$. *J. Nb. Th. 6* (1984), 434-442.

(Reçu le 4 avril 1987)

Paulo Ribenboim

Queen's University
Kingston, Ontario
Canada K7L 3N6