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 $\mathbf{Q}$.