Irreducible polynomials and prime numbers

Andrzej Nowicki and **Adela Świątek**

Department of Mathematics and Informatics,
N. Copernicus University, 87-100 Toruń, Poland

E-mail: (anow @ mat.uni.torun.pl) (swiatek @ mat.uni.torun.pl),

22 November, 1998

In this article we will be occupied with polynomials in one variable x over integer coefficients. The set of all such polynomials we denote by $\mathbb{Z}[x]$.

Let $f(x)$ be a polynomial of positive degree belonging to $\mathbb{Z}[x]$. We say that $f(x)$ is *irreducible* in $\mathbb{Z}[x]$ (or shortly irreducible), if $f(x)$ cannot be expressed as the product of two polynomials from $\mathbb{Z}[x]$ of positive degrees.

Every polynomial of the form $ax + b$, where $0 \neq a, b$ are integers, is of course irreducible. It is easy to check that the following polynomials

$$x^2 + 1,\ x^2 + x + 1,\ x^3 + 5,\ x^3 + x^2 + 2,\ x^4 + 5x^2 + 15.$$

are also irreducible. However, the polynomials $x^3 + 1$, $x^4 + 4$, $x^5 + x^4 + 1$ are not irreducible, because:

$$\begin{aligned} x^3 + 1 &= (x + 1)(x^2 - x + 1), \\ x^4 + 4 &= (x^2 - 2x + 2)(x^2 + 2x + 2), \\ x^5 + x^4 + 1 &= (x^2 + x + 1)(x^3 - x + 1). \end{aligned}$$

There are some theorems which determine whether a given polynomial (in $\mathbb{Z}[x]$) is irreducible. One of these theorems is the following Eisenstein Criterion (see [2]). If a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ has integer coefficients and there exists such a prime number p that $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$, then $f(x)$ is irreducible. Using this criterion we may easily determine that the polynomials:

$$x^4 + 5x + 15, \quad 2x^5 + 3x^4 - 6x - 3, \quad x^{12} + 7x^4 - 7x + 14$$

are irreducible. We can write out a lot of irreducible polynomials of this kind.

There is also one more (less known) way of writing irreducible polynomials. This way is described in the book of Pólya and Szegö [3] (Theorem 128, page 351; see also [1]).

One only needs to know prime numbers. It is possible to construct irreducible polynomials using digits of any prime number. Let us look at the following examples. The numbers 113, 127, 251, 857 are prime. From these numbers we obtain the following irreducible polynomials:

$$1x^2 + 1x + 3, \quad 1x^2 + 2x + 7, \quad 2x^2 + 5x + 1, \quad 8x^2 + 5x + 7.$$

Similarly, the numbers 1997 and 1999 are prime and we have the irreducible polynomials $1x^3 + 9x^2 + 9x + 7$ and $1x^3 + 9x^2 + 9x + 9$. The polynomial $2x^5 + 9x^4 + 9x^3 + 9x^2 + 7x + 7$ is irreducible because the number 299977 is prime.

This can be done with any prime number.

The purpose of this article is to present a proof of this fact. The proof we present can be found in [4]. We will prove two theorems. Theorem 1 will concern the decimal system. In Theorem 2 we will show that the digits of prime numbers written in any numbering system

(based on $q > 2$) have the same feature. In our proofs we use some lemmas concerning complex roots of polynomials from $\mathbb{Z}[x]$.

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ (where $a_n \geqslant 1$) be a given polynomial belonging to $\mathbb{Z}[x]$.

Lemma 1. *Assume that $a_{n-1} \geqslant 0$ and $|a_i| \leqslant c$ for $i = 0, 1, \ldots, n-2$, where $c \geqslant 1$ is some natural number. Then any complex root z of the polynomial $f(x)$ satisfies the inequality* $\mathrm{Re}\,(z) < \frac{1+\sqrt{4c+1}}{2}$.

Proof. Let us suppose that there exists a complex root z such that $\mathrm{Re}\,(z) \geqslant \frac{1+\sqrt{4c+1}}{2}$. Then $|z| \geqslant \mathrm{Re}\,(z) \geqslant \frac{1+\sqrt{4c+1}}{2} > 1$ and hence $\mathrm{Re}\,(1/z) > 0$ and $|z|^2 - |z| - c \geqslant 0$. Moreover:

$$\begin{aligned}
0 = |f(z)| &= |(a_n z^n + a_{n-1}z^{n-1}) + (a_{n-2}z^{n-2} + \cdots + a_1 z + a_0)| \\
&\geqslant |a_n z^n + a_{n-1}z^{n-1}| - |a_{n-2}z^{n-2} + \cdots + a_1 z + a_0| \\
&\geqslant |a_n z^n + a_{n-1}z^{n-1}| - (|a_{n-2}||z|^{n-2} + \cdots + |a_1||z| + |a_0|) \\
&\geqslant |a_n z^n + a_{n-1}z^{n-1}| - c(|z|^{n-2} + \cdots + |z| + 1) \\
&= |a_n z^n + a_{n-1}z^{n-1}| - c\tfrac{|z|^{n-1}-1}{|z|-1} \\
&> |a_n z^n + a_{n-1}z^{n-1}| - c\tfrac{|z|^{n-1}}{|z|-1} \\
&> |z|^n |a_n + a_{n-1}/z| - c\tfrac{|z|^{n-1}}{|z|-1} \\
&\geqslant |z|^n \mathrm{Re}\,(a_n + a_{n-1}/z) - c\tfrac{|z|^{n-1}}{|z|-1} \\
&= |z|^n (a_n + a_{n-1}\mathrm{Re}\,(1/z)) - c\tfrac{|z|^{n-1}}{|z|-1} \\
&\geqslant |z|^n a_n - c\tfrac{|z|^{n-1}}{|z|-1} \geqslant |z|^n - c\tfrac{|z|^{n-1}}{|z|-1} \\
&= |z|^{n-1}\tfrac{|z|^2-|z|-c}{|z|-1} \geqslant 0.
\end{aligned}$$

Therefore we have a contradiction: $0 = |f(z)| > 0$. $\square$

Lemma 2. *Let k be an integer. If any complex root z of the polynomial $f(x)$ satisfies the inequality* $\mathrm{Re}\,(z) < k - \frac{1}{2}$, *then $|f(k-1)| < |f(k)|$.*

Proof. The polynomial f(x) is (up to a constant factor) the product of polynomials of the form:

$$g(x) = x - r \quad \text{and} \quad h(x) = (x - (a+bi))(x - (a-bi)) = (x-a)^2 + b^2,$$

where r, a, b are real numbers. $r < k - \frac{1}{2}$ and $a < k - \frac{1}{2}$. It is enough to show that $|g(k-1)| < |g(k)|$ and $|h(k-1)| < |h(k)|$. The first inequality is obvious. We are checking the other one:

$$|h(k)|^2 - |h(k-1)|^2 = (k-a)^2 + b^2 - (k-1-a)^2 - b^2 = 2\left(k - \tfrac{1}{2}\right) - 2a > 2a - 2a = 0.$$

Therefore $|h(k-1)| < |h(k)|$. $\square$

Lemma 3 ([3] Theorem 127 page 350)**.** *If there exists such an integer k that:*

(1) *every complex root z of the polynomial $f(x)$ satisfies the inequality* $\mathrm{Re}\,(z) < k - \frac{1}{2}$,

(2) $f(k-1) \neq 0$,

(3) $f(k)$ *is prime,*

then the polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Dowód. Suppose that $f(x) = g(x) \cdot h(x)$, where $g(x)$ and $h(x)$ are some polynomials from $\mathbb{Z}[x]$ of degrees $\geqslant 1$. It is evident that $g(x)$ and $h(x)$ satisfy the assumptions of Lemma 2. Hence $|g(k)| > |g(k-1)| \geqslant 1$ and $|h(k)| > |h(k-1)| \geqslant 1$. This implies that $f(k) = |f(k)| = |g(k)| \cdot |h(k)|$ which contradicts with the fact that $f(k)$ is prime. □

Lemma 4. *Assume that $a_{n-1} \geqslant 0$ and $|a_i| \leqslant c$ for $i = 0, 1, \ldots, n-2$, where $c \geqslant 1$ is some natural number. If there exists such an integer k that $k \geqslant 1 + \frac{1}{2}\sqrt{4c+1}$, $f(k-1) \neq 0$ and $f(k)$ is prime, then the polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

Proof. Let z be a complex root of $f(x)$. Then $\mathrm{Re}\,(z) < \frac{1}{2}(1 + \sqrt{4c+1})$ (by Lemma 1) and we have:

$$\mathrm{Re}\,(z) < \tfrac{1}{2} + \tfrac{1}{2}\sqrt{4c+1} = 1 + \tfrac{1}{2}\sqrt{4c+1} - \tfrac{1}{2} \leqslant k - \tfrac{1}{2}.$$

Therefore, by Lemma 3, the polynomial $f(x)$ is irreducible. □

Theorem 1 (A. Cohn, see [3] page 351)**.** *Let $f(x)$ be a polynomial of positive degree and integral coefficients belonging to the set $\{0, 1, ..., 9\}$. If the number $f(10)$ is prime, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

Proof. Put $k = 10$, $c = 9$ and use Lemma 4. □

Theorem 2. *Let $q > 2$ be a natural number and let $f(x)$ be a polynomial of positive degree and integral coefficients belonging to the set $\{0, 1, \ldots, q-1\}$. If the number $f(q)$ is prime, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

Proof. Let $k = q$, $c = q - 1$. Since $q > 2$, then it is easy to check that $k \geqslant 1 + \frac{1}{2}\sqrt{4c+1}$ (we use the assumption that $q > 2$). Therefore $f(x)$ is irreducible (by Lemma 4). □

Let us end with the following question:

Is Theorem 2 *also true for $q = 2$?*

The authors do not know the answer. There have been a lot of polynomials tested using a computer simulation. No counterexample has been found.

References

[1] H. L. Dorwart, *Irreducibility of polynomials*, The American Mathematical Monthly, 42(6)(1935), 369 - 381.

[2] S. Lang, *Algebra*, Addison Wesley Publ. Comp. 1965.

[3] G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, II, Berlin, 1925.

[4] G. M. Szapiro, *Higher algebra* (in Russian), Moscow, 1938.