# THE AMERICAN MATHEMATICAL MONTHLY

Volume 117, Number 9 November 2010

AN OFFICIAL PUBLICATION OF THE MATHEMATICAL ASSOCIATION OF AMERICA

# Irreducible Cubics Modulo Five

**Hendrik Lenstra**

**Abstract.** Finite fields are finite, and they are fields, and as a result one can combine algebraic arguments with counting arguments in their study. This was illustrated in a lecture given at the 2009 April Fools' meeting of the Leiden bachelor seminar. Here is the text of that lecture.

**INTRODUCTION.** On a recent algebra test, I asked the students to factor the polynomial $h = X^3 - 3X^2 - X - 3$ into irreducible factors in the polynomial ring $\mathbf{F}_5[X]$, with $\mathbf{F}_5$ denoting the field of integers modulo 5. Keeping the interests of the students in mind, I always make sure that I can do a test problem myself without thinking too much, and in the present case the following solution had been built in. From

$$h = (X^3 - X) - 3 \cdot (X^2 + 1) = X \cdot (X - 1) \cdot (X + 1) - 3 \cdot (X - 2) \cdot (X + 2)$$

one sees that $h$ can be written as the sum of two polynomials with the property that each element of $\mathbf{F}_5 = \{0, 1, 2, -2, -1\}$ is a zero of one of them but not of the other. As a consequence, the polynomial $h$ has no zero in $\mathbf{F}_5$, and since its degree is only 3, it is irreducible.

Generally, if $f, g \in \mathbf{F}_5[X]$ are such that $\deg f = 3$, $\deg g = 2$, and $f \cdot g = u \cdot \prod_{x \in \mathbf{F}_5}(X - x)$ for some nonzero element $u \in \mathbf{F}_5$, then by the same argument the sum $h = f + g$ is irreducible in $\mathbf{F}_5[X]$; and in addition, it has a particularly brief irreducibility proof. Which irreducible cubics in $\mathbf{F}_5[X]$ are lucky enough to admit such an easy proof?

**A BIJECTIVE MAP.** Let me do some counting. Denote by $S$ the set of pairs $(f, g)$ with the properties just mentioned. Writing down an element of $S$ is equivalent to writing down, first, a subset of size 2 of $\mathbf{F}_5$, which is going to be the set of zeroes of $g$ as well as the complement of the set of zeroes of $f$, and second, a pair of nonzero elements of $\mathbf{F}_5$, which are going to be the leading coefficients of $f$ and $g$. Thus, the cardinality of $S$ equals $\binom{5}{2} \cdot 4^2 = 160$.

Next denote by $T$ the set of irreducible polynomials in $\mathbf{F}_5[X]$ of degree 3. To count $T$, let $\bar{\mathbf{F}}_5$ be an algebraic closure of $\mathbf{F}_5$, and let $\mathbf{F}_{125} = \{x \in \bar{\mathbf{F}}_5 : x^{125} = x\}$ be the unique subfield of $\bar{\mathbf{F}}_5$ of cardinality $5^3 = 125$. Each polynomial in $T$ with leading coefficient 1 is the irreducible polynomial, over $\mathbf{F}_5$, of precisely 3 elements of $\mathbf{F}_{125}$ that are not in $\mathbf{F}_5$. Since there are 4 possibilities for the leading coefficient, this yields $\#T = 4 \cdot (125 - 5)/3$, which also equals 160.

**Theorem.** *There is a bijection $S \to T$ sending $(f, g)$ to $f + g$.*

In other words, each irreducible cubic in $\mathbf{F}_5[X]$ admits a unique irreducibility proof of the type described.

doi:10.4169/000298910X521670

I proved already that one has $f+g \in T$ for any $(f, g) \in S$. Since $S$ and $T$ have the same size, the theorem will follow if I prove that the map is injective. So, suppose that $(f_0, g_0), (f_1, g_1) \in S$ satisfy $f_0 + g_0 = f_1 + g_1$. If $\gcd(g_0, g_1) = 1$, then since $g_0$ divides $f_1 g_1$, it already divides $f_1$ and therefore also $f_1 - g_0$, and likewise $g_1$ divides $f_0 - g_1$; but now the polynomial $f_0 - g_1 = f_1 - g_0$ of degree 3 is divisible by each of the two coprime polynomials $g_0$ and $g_1$, hence also by their product $g_0 g_1$; this cannot be, since $g_0 g_1$ has degree 4. It follows that $g_0$ and $g_1$ have a zero in common, so that $g_0 g_1$ has at most three zeroes in $\mathbf{F}_5$. Thus, at least two elements of $\mathbf{F}_5$ are not among the zeroes of $g_0 g_1$, and these must be among the common zeroes of $f_0$ and $f_1$. That gives at least three zeroes for the polynomial $f_0 - f_1 = g_1 - g_0$, but since the latter has degree at most 2 it must be the zero polynomial. Therefore one has $f_0 = f_1$ and $g_0 = g_1$, which proves the theorem.

**GENERATING IRREDUCIBLE CUBICS.** The theorem may be seen as providing a good way of *generating* irreducible cubics in $\mathbf{F}_5[X]$, since drawing an element of $S$ is easy, as is the evaluation of the map $S \to T$. If the element of $S$ is drawn from the uniform distribution, then all irreducible cubics are found with the same probability. One may wonder whether the same purpose can similarly be achieved for other degrees or over other finite fields. Instead of pursuing this problem, I shall address a different algorithmic issue that is suggested by the theorem.

Suppose that an irreducible cubic $h \in \mathbf{F}_5[X]$ is given. How can one quickly determine the unique pair $(f, g) \in S$ with $f + g = h$? There is a lovely method for doing this. To illustrate it, I am faced with the problem of having to write down an irreducible cubic $h$ to start with. Generating $h$ by means of the method just described is not very convincing; nobody will be impressed if I can write $h$ as $f + g$ if I computed $h$ as $f + g$ in the first place. Thus, I need a different method for generating $h$, and I will use a very straightforward one: namely, I will pick $h = aX^3 + bX^2 + cX + d$ coefficient by coefficient.

The leading coefficient $a$ should be nonzero, so it has four possibilities. For $b$ there are five possibilities. With $c$ one has to be careful, since, as I will prove below, $aX^3 + bX^2 + cX + d$ is automatically reducible if $b^2 = 3ac$. Given $a$ and $b$, there are exactly four values of $c$ with $b^2 \neq 3ac$, and for each of them, as I will also prove below, exactly two elements of $\mathbf{F}_5$ are not of the form $ax^3 + bx^2 + cx$, with $x \in \mathbf{F}_5$. Letting $-d$ be one of these two elements, one finds a polynomial $h = aX^3 + bX^2 + cX + d$ that has no zeroes in $\mathbf{F}_5$, and as it is cubic, it is automatically irreducible. Note that the total number of possibilities equals $4 \cdot 5 \cdot 4 \cdot 2 = 160$, in accordance with my earlier count.

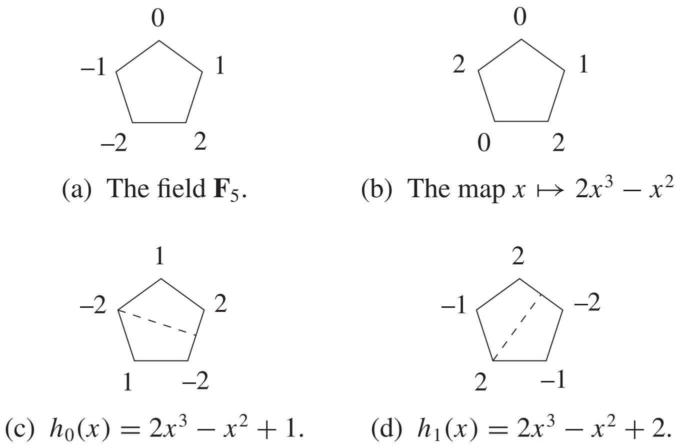
Figure 1 serves as an illustration. I identify the elements of $\mathbf{F}_5$ with the vertices of a regular pentagon, as in Figure 1a, and I graph a function $i$ defined on $\mathbf{F}_5$ by writing $i(x)$ at vertex $x$, for each $x \in \mathbf{F}_5$. For the map $x \mapsto 2x^3 - x^2$, which arises if I choose $a = 2$, $b = -1$, $c = 0$, I did this in Figure 1b. The map misses indeed exactly two values, namely $-1$ and $-2$. The two resulting irreducible polynomials are

$$h_0 = 2X^3 - X^2 + 1, \qquad h_1 = 2X^3 - X^2 + 2.$$

The graphs of $h_0$ and $h_1$, viewed as maps $\mathbf{F}_5 \to \mathbf{F}_5$, are shown in Figures 1c and 1d.

**THE ALGORITHM.** Figure 2 shows an algorithm that, given $h \in T$, finds $(f, g) \in S$ with $f + g = h$, where $S$ and $T$ are as in the theorem. I explain the several steps, using the polynomials $h_0$ and $h_1$ just constructed as examples.

One obtains the function $|h|$ by omitting the signs of the values of $h$. The map $|h|$ has exactly one *symmetry axis*, as illustrated with dotted lines in Figures 1c and 1d; so,



(a) The field $\mathbf{F}_5$.

(b) The map $x \mapsto 2x^3 - x^2$.

(c) $h_0(x) = 2x^3 - x^2 + 1$.

(d) $h_1(x) = 2x^3 - x^2 + 2$.

**Figure 1.** The graphs of three functions $\mathbf{F}_5 \to \mathbf{F}_5$.

$$\begin{aligned}
r &= (\text{reflection point of } |h| \text{ on } \mathbf{F}_5)\\
Y &= \{\text{symmetry points of } h \text{ on } \mathbf{F}_5\}\\
Z &= \{\text{antisymmetry points of } h \text{ on } \mathbf{F}_5\}\\
s &= (\text{leading coefficient of } h)\\
t &= (\text{coefficient of } X^2 \text{ in } h) - 2 \cdot r \cdot s\\
f &= s \cdot \prod_{x \in Y} (X - x), \qquad g = t \cdot \prod_{x \in Z} (X - x)
\end{aligned}$$

**Figure 2.** An algorithm for writing $h = f + g$.

reflecting the graph in the symmetry axis affects only the signs. Each symmetry axis passes through one of the vertices of the pentagon; the element of $\mathbf{F}_5$ identified with this vertex is the *reflection point* $r$. So, in the case $h = h_0$ one has $r = -1$, and for $h = h_1$ one finds $r = -2$.

Bringing back in the signs, one can distinguish vertices where the reflection in the symmetry axis does not change the sign from vertices where the reflection does change the sign. The former are called the *symmetry points*, the latter the *antisymmetry points*. For example, $r$ is among the symmetry points. Since 0 is not assumed as a value, $\mathbf{F}_5$ is the disjoint union of the set $Y$ of symmetry points and the set $Z$ of antisymmetry points. For $h = h_0$ one sees $Y = \{0, -2, -1\}$ and $Z = \{1, 2\}$, whereas $h = h_1$ yields $Y = \{2, -2, -1\}$ and $Z = \{0, 1\}$.

The polynomials $f$ and $g$ to be computed have $Y$ and $Z$ as their respective sets of zeroes. The algorithm includes formulas for their leading coefficients $s$ and $t$, and these lead to

$$\begin{aligned}
h_0 &= 2X(X+2)(X+1) - 2(X-1)(X-2),\\
h_1 &= 2(X-2)(X+2)(X+1) + 2X(X-1).
\end{aligned}$$

**TWO LEMMAS.** Two familiar lemmas from the theory of finite fields will help explain why everything works as stated.

**Lemma 1.** *For any finite field $k$, the map from $\{h \in k[X] : \deg h < \#k\}$ to the set of functions $k \to k$ that sends $h$ to the function $x \mapsto h(x)$ is bijective.*

Since no two distinct polynomials of degree less than $\#k$ can coincide at $\#k$ distinct points, the map is certainly injective. Surjectivity follows by counting.

**Lemma 2.** *If $k$ is a finite field and $h \in k[X]$ satisfies $\deg h < \#k - 1$, then $\sum_{x\in k} h(x) = 0$.*

By linearity, it suffices to prove the lemma for $h = X^j$, with $0 \leq j < \#k - 1$. The case $j = 0$ is trivial, so let $j > 0$. Choose $u \in k$ with $u \neq 0$ and $u^j \neq 1$. Since $x \mapsto ux$ permutes $k$, one has $\sum_{x\in k} x^j = \sum_{x\in k}(ux)^j$, so $(u^j - 1) \cdot \sum_{x\in k} x^j = 0$ and therefore $\sum_{x\in k} x^j = 0$, as desired.

**COUNTING CUBICS.** There are $4 \cdot 5 \cdot 1 \cdot 5 = 100$ cubic polynomials $aX^3 + bX^2 + cX + d \in \mathbf{F}_5[X]$ with $b^2 = 3ac$. The identity

$$aX^3 + bX^2 + \frac{b^2}{3a}X + d = a\left(X + \frac{b}{3a}\right)^3 - \frac{b^3}{27a^2} + d$$

and the fact that the map $x \mapsto x^3$ permutes $\mathbf{F}_5$ combine to prove that these cubics all permute $\mathbf{F}_5$. Consequently, each of them has a zero in $\mathbf{F}_5$ and is therefore reducible, as I asserted above. Together with the $4 \cdot 5 = 20$ first-degree polynomials $aX + b \in \mathbf{F}_5[X]$, which also permute $\mathbf{F}_5$, they account by Lemma 1 for all 120 permutations of $\mathbf{F}_5$. Again by Lemma 1, any other polynomial of degree less than 5 in $\mathbf{F}_5[X]$ fails to permute $\mathbf{F}_5$. In particular, any cubic polynomial $aX^3 + bX^2 + cX \in \mathbf{F}_5[X]$ with $b^2$ *different* from $3ac$ misses at least one value. I claim that it misses at least *two* values. Suppose not. Then there are four elements of $\mathbf{F}_5$ where it assumes four distinct values. By Lemma 2, the value it assumes at the fifth element equals minus the sum of the other four values; but that must be the missing value, as, again by Lemma 2, the sum of all elements of $\mathbf{F}_5$ vanishes. Therefore the cubic does permute $\mathbf{F}_5$ after all, which is a contradiction. Thus, if $b^2 \neq 3ac$, then $aX^3 + bX^2 + cX$ misses at least two values, and therefore gives rise to at least two irreducible cubics $aX^3 + bX^2 + cX + d$. Since one cannot expect to generate more than 160 irreducible cubics, equality holds throughout. Thus, the coefficient-wise generation of irreducible cubics has all the properties stated.

It is of interest to notice that the value of the expression $b^2 - 3ac$ completely determines the fibre sizes of a cubic polynomial $h = aX^3 + bX^2 + cX + d \in \mathbf{F}_5[X]$ when viewed as a map $\mathbf{F}_5 \to \mathbf{F}_5$: they are 1, 1, 1, 1, 1 if $b^2 - 3ac = 0$; they are 2, 2, 1, 0, 0 if $b^2 - 3ac \in \{1, -1\}$; and they are 3, 1, 1, 0, 0 if $b^2 - 3ac \in \{2, -2\}$. One may prove this by relating the number of fibres of size 2 to the discriminant of the derivative $3aX^2 + 2bX + c$ of $h$. Alternatively, one may define two cubic polynomials $h$, $h^* \in \mathbf{F}_5[X]$ to be equivalent if there are $a_0, b_0, a_1, b_1 \in \mathbf{F}_5$ with $a_0$ and $a_1$ nonzero such that $h(a_0X + b_0) = a_1 \cdot h^* + b_1$, and relate the three possibilities given to the three equivalence classes.

**JUSTIFYING THE ALGORITHM.** Let $h \in \mathbf{F}_5[X]$ be an irreducible cubic, and let $f$, $g$ be the polynomials produced by the algorithm. I will now explain why one does have $(f, g) \in S$ and $h = f + g$. Since $h$ has no zero in $\mathbf{F}_5$, the value set of $|h|$ is contained in $\{1, 2\}$; actually, it *equals* $\{1, 2\}$, since if all values of $h$ were the same up to sign, then by Lemma 2 the sign would be the same as well, and $h$ would be constant on $\mathbf{F}_5$, in contradiction with Lemma 1. A moment's reflection shows that any map defined on $\mathbf{F}_5$ of which the image has size 2 has exactly one symmetry axis.

Denote by $r$ the reflection point, and write $\hat{h} = h(2r - X)$. Since reflection in the symmetry axis is given by $x \mapsto 2r - x$, one has $|\hat{h}(x)| = |h(x)|$ for all $x \in \mathbf{F}_5$, so $\hat{h}^2$ and $h^2$ define the same function on $\mathbf{F}_5$. Hence there exists $v \in \mathbf{F}_5[X]$ with

$$h^2 - \hat{h}^2 = v \cdot \prod_{x \in \mathbf{F}_5} (X - x).$$

Since $h^2$ and $\hat{h}^2$ are polynomials of degree 6 with the same leading coefficient, one has actually $v \in \mathbf{F}_5$. Comparing the leading coefficients and the values at $r$, one discovers $h \neq \pm\hat{h}$, so that $v$ is nonzero.

Define $F = (h - \hat{h})/2$ and $G = (h + \hat{h})/2$. Then one has $\deg F = 3$ and $F \cdot G = (v/4) \cdot \prod_{x \in \mathbf{F}_5} (X - x)$, and consequently $\deg G = 2$ and $(F, G) \in S$. Since one also has $F + G = h$, it remains to verify $F = f$ and $G = g$. The zeroes of $F$ are those $x \in \mathbf{F}_5$ for which $h(x) = \hat{h}(x)$, so they coincide with the elements of $Y$. In particular, $Y$ has size 3, consisting of $r$ and two elements adding up to $2r$. Since the leading coefficient of $F$ equals the leading coefficient $s$ of $h$, one concludes $F = f$. Similarly, the zeroes of $G$ are those $x \in \mathbf{F}_5$ for which $h(x) = -\hat{h}(x)$, which are the elements of $Z$. Comparing coefficients of $X^2$ in $F + G = h$, one finds that the leading coefficient of $G$ equals the element $t$ computed by the algorithm, so that $G = g$. This completes the proof.

The argument given provides an independent proof of the surjectivity of the map $S \to T$ and, combined with the injectivity proof, of the equality $\#T = \#S = 160$.

**ACKNOWLEDGMENT.** The assistance of Ronald van Luijk is gratefully acknowledged.

*Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands*

# A Short Proof of Combinatorial Nullstellensatz

**Mateusz Michałek**

**Abstract.** In this note we give a short, direct proof of the combinatorial Nullstellensatz.

The following theorem is due to Alon [**1**].

**Theorem 1 (Combinatorial Nullstellensatz [1]).** *Let $\mathbb{F}$ be an arbitrary field, and let $P(x_1, \dots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \dots, x_n]$. Suppose the degree* $\deg(P)$ *of $P$ is $\sum_{i=1}^{n} k_i$, where each $k_i$ is a nonnegative integer, and suppose the coefficient of $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ in $P$ is nonzero. Then for any subsets $A_1, \dots, A_n$ of $\mathbb{F}$ satisfying $|A_i| \geq k_i + 1$ for $i = 1, 2, \dots, n$, there are $a_1 \in A_1, \dots, a_n \in A_n$ so that $P(a_1, \dots, a_n) \neq 0$.*

doi:10.4169/000298910X521689