CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS OF DEGREE n IN $\mathbb{Z}_2$.

Muhammed Bello, Mustapha Danjuma

ABSTRACT

An irreducible polynomial is, roughly speaking, a non-constant polynomial that may not be factored into the product of two non-constant polynomials, that is a polynomial is said to be reducible over a given field if it is expressible as a product of lower degree polynomials with coefficients in that field.Irreducible polynomials are the most widely used in approximating some functions such as the use of splines, encoding objects and give information about some other objects among others. For instance the characteristic polynomial of a matrix or linear operator contains information about the operator's eigen values. And the chromatic polynomial of a graph counts the number of proper colorings of that graph.

In this paper irreducible polynomials of degree n, in the field of integer modulo 2, has been constructed where theorem 1.7 provides support for the construction since the Eisenstein's criterion cannot be applied directly due to the fact that the coefficients are unity since the research is conducted in integer modulo 2 where the coefficients must be 0 or 1.

Introduction

An irreducible polynomial is, roughly speaking, a non-constant polynomial that may not be factored into the product of two non-constant polynomials, that is a polynomial is said to be reducible over a given field if it is expressible as a product of lower degree polynomials with coefficients in that field. So the property of irreducibility depends on the field or ring to which the coefficients are considered to belong. For example, the polynomial $x^2 - 2$ is irreducible if the coefficients $1\ and\ -2$ are considered as integers and factors as $(x-\sqrt{2})(x+\sqrt{2})$ if the coefficients are considered as real numbers. One says "the polynomial $x^2 - 2$ is irreducible over the integers but not over the reals".

Hilbert gave examples of irreducible polynomials $f(x) \in \mathbb{Z}[x]$ of degree 4 which are reducible mod p for all primes p, namely $x^4 + 2ax^2 + b^2$. Note that this polynomial is irreducible over $\mathbb{Q}(a,b)$ hence (by Hilbert's irreducibility theorem) is irreducible over $\mathbb{Q}$ for infinitely many specializations of a and b into $\mathbb{Q}$. The underlying reason for this phenomenon from the Galois theoretic point of view is that the Galois group of $x^4 + 2ax^2 + b^2$ over $\mathbb{Q}$ (a, b) is Klein's four group. Therefore for any p not dividing the discriminant of f , the decomposition group is a cyclic group of order at most 2, so f is reducible mod p. (Note that for p dividing the discriminant of f, f is reducible mod p as well.) The phenomenon is thus forced by the structure of the Galois group. This also explains why there can be no such examples of polynomials of prime degree. Indeed, suppose $f(x) \in \mathbb{Z}[x]$ has prime degree ` and is irreducible in $\mathbb{Z}$ [x]. Then its Galois group has an element of order `, so by Chebotarev's density theorem there exists p such that the splitting field of f over $\mathbb{F}_p$ has Galois group C`, the cyclic group of order `, hence f must be irreducible over $\mathbb{F}_p$. We will give a proof that the degree of f being prime is the only obstacle, namely that for any composite n, there exist irreducible $f(x) \in \mathbb{Z}$ [x] of degree n which are reducible mod p for all p. Brandl [2] has proved the same result by similar methods. We give a short proof of a generalization of this.

In fact, there is an irreducible $f(t,x) \in \mathbb{Z}$ [t, x] of degree n such that $f(t_0, x)$ is reducible mod p for all specializations t = t_0 in Z and all p. We will also prove the more delicate result that for any composite n, there exist irreducible f(x) ∈ $\mathbb{Q}$ [x] of degree n which are reducible over $\mathbb{Q}_p$ for all p, and that this result generalizes to arbitrary global fields.

Note that Hilbert's example does not satisfy this last condition for all a, b, e.g. $x^4 + 1$ is irreducible over $\mathbb{Q}_2$.

It is worthwhile pointing out here that a random polynomial $f(x) \in \mathbb{Z}$ of composite degree n is not reducible mod p for all p, as its Galois group over $\mathbb{Q}$ is S_n [6], and since S_n contains an n-cycle, Chebotarev's density theorem implies that there are infinitely many primes p for which $f(x)$ is irreducible mod p.

Definition 1.0

Let F be a field. The set $F[x] = \{\sum_{i=0}^{n} a_i x^i : a_i \in F, n \in \mathbb{Z} \geq 0\}$ is called a polynomial ring over *F*.

Definition 1.1 If $n \neq 0$, then the integer *n*, as in the definition 1.0 above is called the degree of the polynomial $f(x)$.

Definition 1.2

A non-zero polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \ of \ degree \ n$ is said to be monic/minimum polynomial if $a_n = 1$ that is the polynomial of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + c_0$$

Theorem (Division Algorithm)

Let f, g be polynomials with rational (or real or complex or any other field) coefficients where $g \neq 0$. Then there exist unique polynomials q, r with coefficients in the same field as f and g so that $f = qg + r$

$where \ r = 0 \ or \ deg(r) < deg(g).$

Proof

We start with existence. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0$ be polynomials where $a_n \neq 0$ and $b_m \neq 0$ (Note: if $f = 0, 0 = 0g + 0$. (Note: If $f = 0, 0 = 0g + 0$, so the assumption that $a_n \neq 0$ either $f = c = (cd^{-1})g$ where $g = d$ has degree 0 or $f = 0g + f$ where degree(g) > 0 satisfies the conditions. Assume that, if $n < k$, then there exist polynomials q, r with coefficients in the same field as f so that $f = qg + r$ where $r = 0 \ or \ deg(r) < deg(g)$. Now assume that the degree of $f \ is \ k. \ If \ k < m, then \ f = 0g + f$ satisfies the conditions. If $m \leq n$, then $f(x) - a_k(b^{-1}m)x^{n-m} \ g(x)$ has degree at most k − 1 < k. So there exist q_1, r so that $f(x) - a_k(b^{-1}m)x^{n-m} \ g(x) = q_1(x)g(x) + r(x)$ where r = 0 or deg(r) < deg(g). Thus $(x) = (a_k(b^{-1}mx^{n-m} \ g(x) + q_1(x)g(x) + r(x)$. Letting $q(x) = a_k b^{-1}x^{n-m} + q_1(x)$ we see that $f = qg + r$ with the coeffiecients of q, r in the same field as f, as required.

Example

1. We can use long division to find that $x^4 + 3x^3 - 2x^2 + 7x - 16 = (x^2 + 6x + 12)(19x - 64)$
2. If $f(x) = 8x^7 + 6x^5 - 3x + 2 \ and \ g(x) = 2x^3 - 3, then \ f(x) = (4x^4 + 3x^2 + 6x)g(x) + 9x^2 + 15x + 2$

Corollary

Remainder Theorem: Let f be a polynomial with coefficients in a field or in the integers or in any ring. Let a be a number in the ground ring. Then there exists a polynomial q with coefficients in the same field or ring as f such that $f = (x - a)q + f(a)$.

Proof

Since the leading coefficient of $x - a \ is \ 1$, we may apply the Division Algorithm to $f(x) \ and \ (x - a)$ and get that $f = q(x - a) + r$ where the coefficients of q, r are in the same field or ring as those of f and either $r = 0 \ or \ deg \ r < deg(x - a) = 1$. So $r(x)$ is a constant. Evaluating at a, we get $f(a) = q(a)(a - a) + r = r$. By the uniqueness part of the Division Algorithm, $f(x) = (x - a)q(x) + f(a)$.

Corollary

Factor Theorem: The number a is a root of f if and only if $x - a$ is a factor of $f(x)$.

Proof

The number a is a root of f if and only if $f(a) = 0$ if and only if $f(x) = (x - a)q(x)$.

Theorem

A polynomial of degree n with coefficients in a field or in $\mathbb{Z}$ has at most n roots in that field or in $\mathbb{Z}$..

Proof

Let f be a polynomial of degree *n*. Let a_1,... be the roots of $f(x)$. By repeated applications of the factor theorem, after t roots we have $(x) = (x - a_1)\, g_1\,(x) = (x - a_1)(x - a_2)\, g_2\,(x) = \cdots = (x - a_1)\ldots(x - a_t)\, g_t\,(x)$. Then $n = deg\, f(x) = t + deg\, g_t(x)$. So $t \leq n$. Thus the number of roots is finite and at most *n*.

Definition 1.3

If F is a field, a non-constant polynomial is irreducible over *F* if its coefficients belong to *F* and it cannot be factored into the product of two non-constant polynomials with coefficients in F.

A polynomial with integer coefficients, or, more generally, with coefficients in a unique factorization domain *R* is sometimes said to be *irreducible over R* if it is an irreducible element of the polynomial ring (a polynomial ring over a unique factorization domain is also a unique factorization domain), that is, it is not invertible, nor zero and cannot be factored into the product of two non-invertible polynomials with coefficients in *R*. Another definition is frequently used, saying that a polynomial is *irreducible over R* if it is irreducible over the field of fractions of *R* (the field of rational numbers, if *R* is the integers). Both definitions generalize the definition given for the case of coefficients in a field, because, in this case, the non constant polynomials are exactly the polynomials that are non-invertible and non zero.

Definition 1.4

If there exist a prime number p such that $p \nmid a_n\,, p|a_i\,, \forall\ i = 0,1,2,\ldots,(n - 1)\ and\ p^2 \nmid a_0,$
$then\ f(x)\ is\ irredicible\ over\ \mathbb{Q}.$

$Such\ a\ polynomial\ f(x)$ is called Eisenstein polynomial.

Theorem (Eisenstein's Irreducibility Criterion)

Let f(x) = $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ be a polynomial with integer coefficients and of positive degree. Suppose there is a prime p so that p does not divide an, p divides $a_i, i = 0,1,2,\ldots,n-1,$ $and\ p^2$ does not divide a_0. Then f is irreducible over the rational numbers.

Proof

Since we are interested in irreducibility over the rational numbers, we may assume that the a_i have no prime factor in common – i.e., that the a_i are relatively prime. By the previous theorem we need only prove that f is irreducible over the integers. We will do so by contradiction. Suppose f is reducible over the integers. Then there exist polynomials $g(x) = b_r x^r + \cdots + b_0$, $h(x) = c_s x^s + \cdots + c_0 \in \mathbb{Z}[x]\ with\ r, s \geq 1$ so that f = gh. Since p divides $a_0 = b_0 c_0$, and p^2 does not divide $a_0 = b_0 c_0$, either p divides b_0 or p divides c_0 but not both. Without loss of generality we may assume that p divides b_0. Since p does not divide $a_n = b_r c_s$, p does not divide b_r. Let k be the least integer so that p divides b_i for i < k and

p does not divide b_k. So $1 \leq k \leq r < n$. Then $a_k = b_0c_k + \cdots + b_{k-1}c_1 + b_kc_0$. Since p divides a_k (since k < n) and p divides b_i , i = 0,...,k − 1 (by choice of k), p divides b_kc_0. But p does not divide c_0 nor b_k. Contradiction. Therefore f is irreducible over the rational numbers.

Example

$3x^{19} - 7x^{15} + 49x^{10} - 28x^6 - 35$ is irreducible over the rational numbers because 7 does not divide 3, 7 does divide −7, 49, −28, −35 and 7^2 = 49 does not divide −35.

We can make Eisenstein's Irreducibility Criterion more widely applicable by changing variables.

Theorem

Let f be a polynomial over a field (such as the rationals). Then f is irreducible if and only if $g = f(ax + b)$, $a \neq 0$, is irreducible. If f is a polynomial over the integers, then f is irreducible if and only if $g = f(x + b)$ is irreducible.

Proof

We shall prove the contrapositive, namely, f is reducible over a field (resp., the integers) if and only if $= f(ax + b)$, $a \neq 0$, (resp., $f(x + b)$) is reducible.

Suppose f is reducible. Then $f = pq$ for some polynomials p,q of positive degree. By substituting $ax + b\ for\ x$, we get that $g(x) = f(ax + b) = p(ax + b)q(ax + b)$, whence g is reducible. Note that there is no difference here between fields and integers.

Suppose $g = f(ax + b)$ is reducible. Then $g = g(x) = f(ax + b) = p(x)q(x)$ for some polynomials p, q of positive degree. By substiting $a^{-1}(x - b)$ for x we get that $f(x) = p(a^{-1}(x - b)q(a^{-1}(x - b))$ hence f is reducible. Note that we used the fact that in a field, a non-zero element has an inverse. Over the integers, if f(x + b) is reducible, we can duplicate the argument with $a = 1$.

CONSTRUCTION

Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}_2[x]$ - - - - (1)

be a polynomial of degree *n*, for (1) to be monic and irreducible, it will become

$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + 1$ - - - (2)

The coefficients of (2) are in $\mathbb{Z}_2[x]$ and must be chosen so that the equation has no zero in $\mathbb{Z}_2[x]$. To achieve this, we may not have the situation where by $f(0) = 0 \ \ or\ f(1) = 0$.

Now, since the roots are in $\mathbb{Z}_2[x]$ and we do not want $f(0) = 0 \ \ or\ f(1) = 0$, then we must have that $f(0) = 1$, no matter how the choice of the other coefficients will be $f(1) = sum\ of\ the\ coefficients$. Now the sum is 1 and we have n possibilities as below;

$f_1(x) = x^n + x^{n-1} + 1$

$f_2(x) = x^n + x^{n-2} + 1$

$f_3(x) = x^n + x^{n-3} + 1$

... = ……. ……

... = ……. ……

... = ……. ……

RESULTS

Irreducible polynomials of degree *n*, in $\mathbb{Z}_2[x]$, has been constructed where theorem ….. provides support for the construction since the Eisenstein's criterion cannot be applied directly due to the fact that the coefficients are unity since the research is conducted in $\mathbb{Z}_2[x]$ where the coefficients must be 0 or 1.

On the construction

As stated above some Eisenstein's criterion cannot be directly applied to some polynomials, more especially those polynomials whose coefficient are 1(the polynomials constructed in this paper), for instance, the polynomial $f(x) = x^2 + x + 1$ is irreducible over the rational numbers since, by the quadratic formula, the roots of $f(x)\ are\ \frac{(-1\pm i\sqrt{3})}{2}$ All the coefficients are 1. But $f(x+1) = (x+1)^2 + (x+1) + 1 = x^2 + 3x + 3$ which is irreducible by Eisenstein's Irreducibility Criterion. Thus f is also irreducible over the rational numbers.

Conclusion

The most important factor which shows that a polynomial is irreducible is that it is monic and that for the constant in the polynomial to be 1 as we have seen in this paper.

References

- Fraleigh (2002),"**A first course in abstract algebra"**, Addison-Wesley publishing company, P 195-285
- Hamma S. et al (2013),"**On Polynomial Rings and their reducibility by Eisenstein's criterion**", Jewel Journal of scientific research, Maiden edition, 2013.
- Mohamed Ayad,"**on irreducible polynomials over $\mathbb{Q}$ which are reducible over $\mathbb{F}_p$ forall** p", Rocky mountain journal of mathematics, V 40 No. 5, 2010.