Scientific Research Publishing

Open Journal of Discrete Mathematics, 2019, 9, 52-61
http://www.scirp.org/journal/ojdm
ISSN Online: 2161-7643
ISSN Print: 2161-7635

Irreducible Polynomials in $\mathbb{Z}[x]$ That Are Reducible Modulo All Primes

Shiv Gupta

Department of Mathematics, West Chester University, West Chester, USA
Email: sgupta@wcupa.edu

How to cite this paper: Gupta, S. (2019) Irreducible Polynomials in $\mathbb{Z}[x]$ That Are Reducible Modulo All Primes. *Open Journal of Discrete Mathematics*, **9**, 52-61.
https://doi.org/10.4236/ojdm.2019.92006

Received: December 20, 2018
Accepted: March 30, 2019
Published: April 2, 2019

Abstract

The polynomial x^4+1 is irreducible in $\mathbb{Z}[x]$ but is locally reducible, that is, it factors modulo p for all primes p. In this paper we investigate this phenomenon and prove that for any composite natural number N there are monic irreducible polynomials in $\mathbb{Z}[x]$ which are reducible modulo every prime.

Keywords

Irreducible Polynomial, Reducible Polynomial, Galois Theory

1. Introduction

The polynomials of the title of this article have been discussed by Brandl [1], and Guralnick *et al.* [2]. Brandl's paper excludes those N which are such that $(N,\varphi(N))=1$. These are precisely the composite integers N for which there is only one abstract group of order N. The paper by Guralnick *et al.* does show the existence of such polynomials for all composite N's. Our proof of the same is different, more elementary, and in some cases even constructive.

We shall first enumerate the known results which we shall use in this article. Several of these results are true more generally but we shall state them as needed in this article.

1) Let $f(x)\in\mathbb{Q}[x]$ be a non-constant polynomial. Then the Galois group of $f(x)$ over $\mathbb{Q}$ acts transitively on its roots if and only if $f(x)$ is a power of an irreducible polynomial over $\mathbb{Q}$.

2) Let $\mathbb{K}_1/\mathbb{Q}, \mathbb{K}_2/\mathbb{Q}$ be finite normal extensions that is, splitting fields of some polynomial. Let $\mathbb{K}_1\mathbb{K}_2$ denote the compositum of the fields $\mathbb{K}_1, \mathbb{K}_2$, that is, the smallest subfield of containing $\mathbb{K}_1, \mathbb{K}_2$. Then $\mathbb{K}$ is a normal extension

of $\mathbb{Q}$ and if $\left[\mathbb{K}_1:\mathbb{Q}\right]$ and $\left[\mathbb{K}_2:\mathbb{Q}\right]$ are coprime. Then

$$Aut\left(\mathbb{K}/\mathbb{Q}\right)=Aut\left(\mathbb{K}_1/\mathbb{Q}\right)\times Aut\left(\mathbb{K}_2/\mathbb{Q}\right)$$

3) Every finite solvable group can be realized as a Galois group of some polynomials over $\mathbb{Q}$. Same is true of the symmetric groups S_n and alternating groups A_n. We shall only need this result for cyclic groups, Frobenius groups and for the groups S_n and A_n [3] [4] and [5].

4) Let $f\left(x\right)\in\mathbb{Q}\left[x\right]$ be an irreducible polynomials of degree *n*. Let $\alpha_1,\alpha_2,\cdots,\alpha_n$ be its roots. Let *r* be an integer, $1<r<n-1$ and $C_n^r=m$. Let $f_r\left(x\right)$ denote the polynomial whose roots are all sums of *r* different α_1. Then $f_r\left(x\right)\in\mathbb{Q}\left[x\right]$ and $f\left(x\right)$ and $f_r\left(x\right)$ have the same splitting field [6].

5) Let $f\left(x\right)\in\mathbb{Z}\left[x\right]$ be a monic irreducible polynomial of degree *n* and *p* a prime which does not divide the discriminant of *f*(*x*). Let $G=Gal\left(f\right)$ be the Galois group of $f\left(x\right)$ over $\mathbb{Q}$. Suppose that modulo *p* the polynomial $f\left(x\right)$ factors into irreducible polynomials of degrees $n_1,n_2,\cdots,n_t$ so $n_1+n_2+\cdots+n_t=n$. Then there is $\sigma\in G$ such that as a permutation on the *n* roots of $f\left(x\right)$, $\sigma=\sigma_1\sigma_2\cdots\sigma_t$, where σ_i is acyclic permutation of length n_i for $1\le i\le n$. See [7].

6) Let *N* be any composite natural number and $f\left(x\right)\in\mathbb{Z}\left[x\right]$ be a monic irreducible polynomial of degree *N* whose Galois group over $\mathbb{Q}$ does not have any element of order *N*. Then $f\left(x\right)$ is reducible modulo every prime. This is an immediate consequence of **(5)** above.

2. Theorem and Proof

Theorem: For every composite natural number *N* there is a monic irreducible polynomial $f\left(x\right)\in\mathbb{Z}\left[x\right]$ of degree *N* which is reducible modulo every prime.

Case I *N* is *not* square-free

We write $N=p^tm$ where $t>1$ and *p* is a prime which does not divide *m*. Let G_1 be any non-cyclic group of order p^t and G_2 a cyclic group of order *m*. Let $f_1\left(x\right)\in\mathbb{Z}\left[x\right]$ be an irreducible polynomial of degree p^t with Galois group isomorphic to G_1 and $f_2\left(x\right)\in\mathbb{Z}\left[x\right]$ be an irreducible polynomial of degree *m* with Galois group isomorphic to G_2. Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be splitting fields of $f_1\left(x\right)$ and $f_2\left(x\right)$ respectively. Let $\mathbb{K}=\mathbb{K}_1\mathbb{K}_2$ be the compositum of the fields $\mathbb{K}_1$ and $\mathbb{K}_2$. Then $\mathbb{K}$ is of degree *N* over $\mathbb{Q}$ and $G=Aut\left(\mathbb{K}/\mathbb{Q}\right)$ is isomorphic to $G_1\times G_2$ and so it does not have any element of order *N*. Let α be any algebraic integer such that $\mathbb{K}=\mathbb{Q}\left(\backslash\alpha\right)$. Let $f\left(x\right)$ be the minimum polynomial of α. Then $f\left(x\right)\in\mathbb{Z}\left[x\right]$ is a monic irreducible polynomial of degree *N* and its Galois group does not have any element of order *N* and therefore $f\left(x\right)$ has the desired property.

Case II *N* is square-free and gcd(*N*, φ(*N*)) > 1

In this case we can write $N=pqm$ where *p*, *q* are primes, *p* divides $q-1$ and $\gcd\left(pq,m\right)=1$. Let G_1 be a non-abelian group of order *pq* and G_2 a cyclic group of order *m*. Just as in the previous case we get a monic irreducible

polynomial in $\mathbb{Z}[x]$ of degree N whose Galois group does not contain an elementof order N.

Case III, N is square-free and gcd(N, $\varphi(N)$) = 1

In this case N is necessarily odd. First we assume that N is a product of just two primes. So let $N = pq$, where p and q are distinct primes, $p < q$ and p does not divide $q-1$. Let t be the order of p modulo q. So $t > 1$ is the smallest integer such that $p^t \equiv 1 (\mathrm{mod}\, q)$. Let G_1 be an elementary Abelian p-group of order p^t and G_2 be a group of order q. We note that $Aut(G_1)$ is isomorphic to $GL(t, p)$ and so its order is divisible by q. Let $G = G_1 \times G_2$ be the semi-direct product of G_1 by G_2. Evidently G is not a direct product of G_1 and G_2. Therefore G_2 is not a normal subgroup of G. We claim that G_2 is its own normalizer in G. For otherwisethe index of the normalizer of G_2 in G would be p^r, for some r, $1 \le r < t$ which would contradict the fact that t is the smallest integer satisfying $p^t \equiv 1 (\mathrm{mod}\, q)$. Since G_2 has prime order q it is disjoint from its conjugates. Therefore G is a Frobenius group of order p^t, q and every non-identity element of G_2 induces a fixed-point-free automorphism of G_1.

Let $\mathbb{K}$ be a normal extension of $\mathbb{Q}$ with Galois group isomorphic to G. Then $[\mathbb{K} : \mathbb{Q}] = p^t q$. Let H be a subgroup of G of order p^{t-1} and let $\mathbb{F} \subseteq \mathbb{K}$ be its fixed subfield.

Then by FTGT ({*Fundamental Theorem of Galois Theory*}) the field $\mathbb{F}$ is of degree pq over $\mathbb{Q}$. We also note that as H is not a normal subgroup of G, $\mathbb{F}$ is not a normal extension of $\mathbb{Q}$. Let α be an algebraic integer such that $\mathbb{F} = \mathbb{Q}(\alpha)$ and let $f(x)$ be its minimal polynomial over $\mathbb{Q}$. Then $f(x) \in \mathbb{Z}[x]$ is irreducible of degree pq.

We claim that $\mathbb{K}$ is the splitting field of $f(x)$ (*i.e.* it is the normal closure of the field $\mathbb{F}$) and G is its Galois group over $\mathbb{Q}$.

If the normal closure of $\mathbb{F}$ were a proper subfield of $\mathbb{K}$ then it would imply that G has a proper normal subgroup of order p^r where $r < t$, but this is not possible, as G is a Frobenius group. So $f(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomials of degree $N = pq$ and its Galois group over $\mathbb{Q}$ does not have any element of order $N = pq$.

Finally assume that N and $\varphi(N)$ are coprime and N is a product of more than two primes. We write $N = pqm$, where p, q are primes and $\gcd(pq, m) = 1$. Let t = order of p modulo q. As discussed in the previous case let $f_1(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree pq whose Galois group is the semi-direct product of an elementary group of order p^t by a cyclic group of order q and is a Frobenius group.

Let G_1 denote this Frobenius group of order $p^t q$ and $\mathbb{K}_1$ denote the splitting field of $f_1(x)$. Let G_2 be a cyclic group of order m and $f_2(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomialof degree m whose splitting field is $\mathbb{K}_2$ and Galois group over $\mathbb{Q}$ is G_2.

Let $\mathbb{K} = \mathbb{K}_1 \mathbb{K}_2$ be the compositum of the fields $\mathbb{K}_1$ and $\mathbb{K}_2$. Let $pq = n$ and

$$f_1(x)=\prod_{i=1}^{n}(x-\alpha_i)$$

$$f_2(x)=\prod_{j=1}^{m}(x-\beta_j)$$

$$f(x)=\prod_{j=1}^{m}\prod_{i=1}^{n}(x-\alpha_i\beta_j)$$

We note the following:

1) $[\mathbb{K}_1:\mathbb{Q}]=p^tq,[\mathbb{K}_2:\mathbb{Q}]=m,[\mathbb{K}:\mathbb{Q}]=p^tqm$;

2) $\mathbb{K}_1=\mathbb{Q}(\alpha_1,\alpha_2,\cdots,\alpha_n)$;

3) $\mathbb{K}_2=\mathbb{Q}(\beta_1,\beta_2,\cdots,\beta_m)$;

4) $\mathbb{K}=\mathbb{Q}(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta_1,\beta_2,\cdots,\beta_m)$;

5) $G=Aut(\mathbb{K}/\mathbb{Q})$ is a group of order p^tqm isomorphic to the direct product of aFrobenius group of order p^tq and a cyclic group of order m. Therefore it *does not* have an element of order $N=pqm$. Note that this Frobenius groupdoes not have any subgroup of order pq.

6) The group G transitively permutes the nm algebraic numbers $\alpha_i\beta_j, 1\le i\le n, 1\le j\le m$. So $f(x)\in\mathbb{Z}[x]$ is an irreducible polynomial of degree $N=pqm$, whose Galois group does not have any element of order N. This completes the proof of our theorem.

3. Alternate Methods

As we noticed the construction of irreducible polynomials in $\mathbb{Z}[x]$ of odd composite degree $N$where $\gcd(N,\varphi(N))=1$, and whose Galois group does not contain an element of order $N$is not so straight forward. In some case such as $N=15$ or $N=35$ there is another interesting method of construction of such polynomials. In fact it works for most N's (with very few exceptions) which are such that $C_n^r=N$ for some n and r such that $1<r<n-1$. The method we are about to describe fails in cases where $C_n^r=N$ but the symmetric group S_n does have an element of order N, as it happens when $n=15, r=2$ and $N=105$.

As the symmetric group on 15 letters does have an element of order $105=C_{15}^2$, namely a permutation which is a product of 3, 5 and a 7-cycle. Let $f(x)\in\mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n>4$ whose Galois group is isomorphic to either A_n or S_n. Let r be such that $1<r<n-1$ and $C_n^r=N$. Further assume that S_n does not have any element order N. We know that S_n is n-transitive and A_n is $(n-2)$-transitive on n letters. Let $f_r(x)$ denote a polynomial of degree $N=C_n^r$ whose roots are sum of all r different roots of $f(x)$. Let the roots of $f_r(x)$ be β_i, where $1\le i\le N$. The polynomials $f(x)$ and let $f_r(x)$ have the same splitting field. Since both S_n. and A_n transitively permute the N, roots of Let $f_r(x)$ this polynomial is irreducible. So the polynomial let $f_r(x)$ is the required polynomial of degree N, whose Galois group does not have any element of order N.

4. Examples

1) The first interesting case is for $N=15$. Let $f(x)\in\mathbb{Z}[x]$ be an irreducib-

lemonic polynomial of degree six whose Galois group over $\mathbb{Q}$ is isomorphic to symmetric oralternating group on five or six letters. Then $f_2(x) \in \mathbb{Z}[x]$ is an irreducible monic polynomial whose Galois group is the same as that of $f(x)$ and so does not have any element of order 15. Therefore $f_2(x)$ is reducible modulo every prime. For instance let $f(x) = x^6 + 24x - 20$ whose discriminant is $2^{16} \cdot 3^6 \cdot 5^6$. We note that

$$f(x) \equiv (x+3)\left(x^5 + 4x^4 + 2x^3 + x^2 + 4x + 5\right) (\mathrm{mod}\, 7)$$

$$f(x) \equiv (x+7)(x+12)(x+21)\left(x^3 + 6x^2 + 13x + 16\right) (\mathrm{mod}\, 23)$$

$$f(x) \equiv \left(x^2 + 26x + 10\right)\left(x^4 + 3x^3 + 28x^2 + 25x + 27\right) (\mathrm{mod}\, 29)$$

It follows that $f(x)$ is irreducible over $\mathbb{Q}$ and its Galois group G over $\mathbb{Q}$ is 2-transitive on its roots and has a 3-cycle. Therefore G is isomorphic to A_6 the alternating group on six letters [8]. We know that A_6 is 4-transitive on six letters. Let $f_2(x)$ represent the polynomial of degree 15 whose $15 = C_6^2$ roots are the sumsof the roots of $f(x)$ taken two at a time. This polynomial turns out to be

$$x^{15} - 240x^{10} + 520x^9 - 6912x^5 - 8640x^4 - 10800x^3 - 13824$$

The Galois group of this polynomial is the same as that of $f(x)$ and so is isomorphic to A_6. As A_6 has no element of order 15 this polynomial is reducible modulo every prime.

2) The second example is for $N = 35$. As $C_7^3 = 35$, we start with a some monic polynomial $f(x)$ of degree 7 with Galois group isomorphic to S_7 or A_7. The polynomial of degree 35 whose roots are the sums of three different roots of $f(x)$ is the required polynomial whose Galois group (being isomorphic to S_n or A_n) does not have any element of order 35. To illustrate this we begin with the polynomial $f(x) = x^7 - 2x^6 + 2x + 2$ of degree 7. We observe that the discriminant of the polynomial is $50808364 = 2^6 \cdot 3^8 \cdot 11^2$ and $f(x)$ is irreducible modulo 5. Also

$$f(x) \equiv \left(x^2 + 7x + 1\right)\left(x^2 + 11x + 8\right)\left(x^3 + 6x^2 + x + 10\right) (\mathrm{mod}\, 13)$$

So $f(x)$ is an irreducible polynomial of degree 7 whose discriminant is a square and Galois group G has a 3-cycle. So G is isomorphic to A_7 [8].

Suppose that the roots of $f(x)$ are $\alpha_i, 1 \le i \le 7$. The polynomial $f_2(x)$ of degree $C_7^2 = 21$ whose roots are $\alpha_i + \alpha_j, 1 \le i < j \le 7$, is

$$\begin{aligned} &x^{21} - 12x^{20} + 60x^{19} - 160x^{18} + 240x^{17} - 192x^{16} + 14x^{15} + 282x^{14} \\ &- 384x^{13} - 896x^{12} + 3456x^{11} - 4032x^{10} + 1452x^9 + 936x^8 - 3348x^7 \\ &+ 8208x^6 - 10800x^5 + 6912x^4 - 1944x^3 + 648x^2 - 648x + 216 \end{aligned}$$

This polynomial is irreducible over $\mathbb{Q}$. As its Galois group is isomorphic to A_7 which does not have any element of order 21 this polynomial is reducible modulo every prime.

The polynomial $f_3(x)$ of degree $C_7^3 = 35$ whose roots are $\alpha_i + \alpha_j + \alpha_k, 1 \le i < j < k \le 7$, is

$$x^{35}-30x^{34}+420x^{33}-3640x^{32}+21840x^{31}-96096x^{30}+320400x^{29}$$
$$-824892x^{29}+1651824x^{27}-2520656x^{26}+2467968x^{25}+1014144x^{24}$$
$$-13570744x^{23}+43939464x^{22}-97466448x^{21}+165719040x^{20}$$
$$-229091136x^{19}+279559296x^{18}-328973632x^{17}+369175728x^{16}$$
$$-339989856x^{15}+197554480x^{14}-25543680x^{13}+5507328x^{12}$$
$$-229676208x^{11}+582038592x^{10}-837493056x^{9}+855433568x^{8}$$
$$-666645072x^{7}+405962976x^{6}-192746432x^{5}+69432960x^{4}$$
$$-17666304x^{3}+2572800x^{2}-58368x-18432$$

This polynomial is irreducible over $\mathbb{Q}$ and its Galois group is isomorphic to A_7. As A_7 does not have any element of order 35 this polynomial is reducible modulo every prime. Its discriminant is the following 311-digit number

$$2^{296}\cdot 3^{154}\cdot 11^{20}\cdot 2260889^{2}\cdot 73504388212873^{2}\cdot 307711591051853^{6}$$

Note: The composite natural numbers N below 100 which are such that $\gcd\left(N,\varphi\left(N\right)\right)=1$ are

$$15,33,35,51,65,69,77,85,91,95.$$

Among these numbers the method described above works for N = 15, 35 and 91. This is so because $C_6^2=15$, $C_7^3=35$, and $C_{14}^2=91$. As starting with a polynomial of degree 7 with Galois group isomorphic to A_7 or S_7, we constructed an irreducible polynomial of degree 35 which is reducible modulo every prime, likewise starting with a polynomial of degree14 with Galois group isomorphic to A_{14} or S_{14} we can construct an irreducible polynomial of degree 91 which is reducible modulo every prime.

3) The method discussed in the previous examples above does not work for $N=33$. For this we proceed as in the proof of our theorem. As the order of 11 modulo 3 is 2 we construct a Frobenius group G of order $11^2\cdot 3$ which is a semi-direct product of $\mathbb{Z}_{11}\times\mathbb{Z}_{11}$ by a group of order 3. More specifically we extend the group $\mathbb{Z}_{11}\times\mathbb{Z}_{11}=\langle x\rangle\times\langle y\rangle$ by the group $\langle\varphi\rangle$ of order three where φ is the automorphism of $\langle x\rangle\times\langle y\rangle$ given by $\varphi\left(x\right)=x^6y,\varphi\left(y\right)=xy^4$. It is easily seen that this automorphism has order three and is fixed-point-free.The resulting group, the semi-direct product of $\mathbb{Z}_{11}\times\mathbb{Z}_{11}$ by $\langle\varphi\rangle$ is a Frobenius group of order 363 having the subgroup $\mathbb{Z}_{11}\times\mathbb{Z}_{11}$ as its kernel and the group $\langle\varphi\rangle$ as its complement.

This Frobenius group of order 363 does not have any subgroup of order 33. Let $\mathbb{K}/\mathbb{Q}$ be a normal extension whose Galois group is isomorphic to G.

Let H be a subgroup of G of order 11 and $\mathbb{F}$ be its fixed subfield. By FTGT (*Fundamental Theorem of Galois Theory*) the field $\mathbb{F}$ has degree 33 over $\mathbb{Q}$. Let α be an algebraic integer such that $\mathbb{F}=\mathbb{Q}\left(\alpha\right)$ and let $f\left(x\right)\in\mathbb{Z}\left[x\right]$ be its minimum polynomial. As proved in the theorem this polynomial has degree 33 and its Galois group is a Frobenius group of order $11^2\times 3=363$ which does not have any subgroup of order 33 andtherefore the irreducible polynomials $f\left(x\right)$ is reducible modulo every prime.

5. Construction of the Polynomials $f_r(x)$

It remains to be seen that given a degree n polynomial $f(x) \in \mathbb{Z}[x]$ how we can compute the polynomial $f_r(x) \in \mathbb{Z}[x]$, for $1 < r < n-1$. This can be done with thehelp of the concept of the resultant of two polynomials. Let

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n, g(x) = b_0 x^m + b_1 x^{m-1} + \cdots + b_m,$$

be polynomials of degree $n > 0$ and $m > 0$ respectively (so $a_0, b_0 \neq 0$) with coefficients in a field $\mathbb{F}$. Let $\alpha_i, 1 \leq i \leq n, \beta_j, 1 \leq j \leq m$ be the zeros of $f(x)$ and $g(x)$ in some extension of $\mathbb{F}$. Writing $f(x)$ and $g(x)$ as simply f and g, and resultant simply as *Res* we have

$$Res(f, g) = a_0^m b_0^n \prod_{j=1}^{n} \prod_{i=1}^{n} (\alpha_i - \beta_j)$$

As this resultant is equal to the following determinant of order $m+n$, its value can be computed with the help of any symbolic computation package such as *MATHEMATICA*.

$$Res(f, g) = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots & \\ & a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots \\ & & \vdots & & \vdots & & \vdots \\ & & & a_0 & \cdots & a_{n-1} & a_n \\ & b_0 & b_1 & \cdots & b_m & & \\ & & \vdots & & \vdots & & \\ & & & & & & \\ & & & b_0 & b_1 & \cdots & b_m \end{bmatrix}$$

In this determinant all the missing entries are zeros. The entries in the first m rows are the coefficients of $f(x)$ and those in the last n rows are the coefficients of $g(x)$. If f and g are polynomials in two variables x and y then we can determine their resultant with respect to any of the variable. For the discussion of the calculation of $f_r(x)$ for a given polynomial $f(x)$ it will be convenient to deal with monic polynomials. Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be a polynomial of degree n with zeros $\alpha_1, \backslash\alpha_2, \cdots, \backslash\alpha_n$. The polynomial $(-1)^n f(x-y)$ can be regarded as a monic polynomial of degree n in y with coefficientsin the polynomial ring $\mathbb{F}[x]$. As a polynomial in y its n zeros are $x - \alpha_i, 1 \leq i \leq n$. We note that

$$(-1)^n f(x-y) = (-1)^n \prod_{1 \leq i \leq n} (x - y - \alpha_i) = \prod_{1 \leq i \leq n} (y - (x - \alpha_i)).$$

This observation and (and similar ones) will be used repeatedly in what follows. As before we let $f_r(x)$ denote the monic polynomial of degree C_n^r with zeros $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r}$ where $1 \leq i_1 < i_2 < i_3 < \cdots < i_r \leq n$.

We shall show how to find $f_r(x)$ for $r = 2, 3$. The method discussed can be easily generalized to larger values of r.

5.1. Computation of $f_2(x)$

Let

$$R_2(x) = Res_y\left((-1)^n f(x-y), f(y)\right) = \prod_{j=1}^{n}\prod_{i=1}^{n}\left(x-\alpha_i-\alpha_j\right)$$

Then $R_2(x)$ is a polynomial of degree n^2 with zeros $\alpha_i+\alpha_j$. So the n^2 zeros of $R_2(x)$ are $2\alpha_i, 1\le i\le n$ and $\alpha_i+\alpha_j, i<j$, each appearing twice. Let

$$A_2(x) = 2^n f\left(\frac{x}{2}\right)$$

Then $A_2(x)$ is a monic polynomial of degree n with zeros $2\alpha_i, 1\le i\le n$. Therefore, $R_2(x)/A_2(x)$ is a polynomial of degree n^2-n, with zeros $\alpha_i+\alpha_j, i<j$, each zeroappearing twice. Therefore,

$$f_2(x) = \left(\frac{R_2(x)}{A_2(x)}\right)^{\frac{1}{2}}$$

is a polynomial of degree $\frac{n^2-n}{2} = C_n^2$ with zeros $\alpha_i+\alpha_j, i<j$.

5.2. Computation of $f_3(x)$

We first note that, as a polynomial in y, $f_2(x-y)$ has degree $\frac{n(n-1)}{2}$ and has roots $x-\alpha_i-\alpha_j$ for $1\le i<j\le n$. In other words we can write

$$\begin{aligned} f_2(x-y) &= \prod_{1\le i<j\le n}\left(x-y-\left(\alpha_i+\alpha_j\right)\right) \\ &= (-1)^{\frac{n(n-1)}{2}}\prod_{1\le i<j\le n}\left(y-x+\alpha_i+\alpha_j\right) \end{aligned}$$

Let

$$R_3(x) = Res_y\left((-1)^{\frac{n(n-1)}{2}} f_2(x-y), f(y)\right) = \prod_{i<j}^{1\le k\le n}\left(x-\alpha_i-\alpha_j-\alpha_k\right).$$

Then $R_3(x)$ is a polynomial of degree $C_n^2\cdot n = \frac{n^2(n-1)}{2}$ whose zeros are of following types.

$\alpha_i+\alpha_j+\alpha_k, i<j<k$, each appearing three times.

$$2\alpha_i+\alpha_j, i\ne j.$$

We check that the total number adds up to the right degree, namely

$$3\cdot C_n^3 + 2\cdot C_n^2 = \frac{n(n-1)(n-2)}{2} + n(n-1) = \frac{n^2(n-1)}{2}$$

We shall now find a polynomial with zeros $2\alpha_i+\alpha_j, i\ne j$. Let

$$A_3(x) = Res_y\left((-1)^n f\left(\frac{x-y}{2}\right)2^n, f(y)\right)$$

Here as before we have multiplied by $(-1)^n$ to ensure that the first polynomial in the argument of Res_y is monic. We note that as a polynomial in y the roots of $f\left(\frac{x-y}{2}\right)$ are $x-2\alpha_i$, for $1\le i\le n$. Also $A_3(x)$ is a polynomial of degree n^2. In fact

$$A_3(x)=\prod_{j=1}^{n}\prod_{i=1}^{n}\left(x-2\alpha_i-\alpha_j\right)$$

So the zeros of $A_3(x)$ are $3\alpha_i, 1\le i\le n$ and $2\alpha_i+\alpha_j, i\ne j$. Let

$$B(x)=f\left(\frac{x}{3}\right)3^n, C(x)=\frac{A_3(x)}{B(x)}$$

So $B(x)$ is a monic polynomial with zeros $3\alpha_i, 1\le i\le n$ and $C(x)$ is a monic polynomial of degree n^2-n with zeros $2\alpha_i+\alpha_j, i\ne j$, $1\le i, j\le n$. We also note that

$$\frac{R(x)}{C(x)}=\frac{R_3(x)\cdot B(x)}{A_3(x)}$$

is a polynomial of degree $\frac{n^2(n-1)}{2}-\left(n^2-n\right)=\frac{n(n-1)(n-2)}{2}$ with zeros $\alpha_i+\alpha_j+\alpha_k, i<j<k$, each repeated three times. Therefore

$$f_3(x)=\left(\frac{R_3(x)}{C(x)}\right)^{\frac{1}{3}}$$

is the required polynomial of degree C_n^3.

6. Addendum

Bernard Dominique [9] sent us a list of following eighteen irreducible polynomials of degree 33 and informed us that these are reducible for all primes $p<500000$.

$$x^{33}+2x^3+1, x^{33}+x^6+1, x^{33}+x^6+2x^3+1,$$

$$x^{33}+x^6+1 \& x^{33}+x^6+x^3+1, x^{33}+x^9+1,$$

$$x^{33}+x^9+x^3+1, x^{33}+x^9+2x^3+1, x^{33}+x^9+x^6+x^3+1,$$

$$x^{33}+x^9+2x^6+1x^{33}+x^9+2x^6+2x^3+1x^{33}+2x^9+1,$$

$$x^{33}+2x^9+2x^3+1x^{33}+2x^9+x^6+1x^{33}+2x^9+x^6+x^3+1,$$

$$x^{33}+2x^9+x^6+2x^3+1, x^{33}+2x^9+2x^6+x^3+1, x^{33}+2x^9+2x^6+2x^3+1.$$

If the Galois group of any of these polynomials regarded as a permutation on its 33 roots had a 33-cycle then according to Cebotarev Density Theorem the density of primes p for which any of these polynomials is irreducible should be $\ge\frac{1}{13}$ [10]. As there is no such prime $p<500000$ we believe that these polynomials are reducible for all primes. However, in the absence of any information about their Galois group we do not have a proof that any of these polynomials is locally reducible for all primes.

7. Conclusion

In this paper we have shown that for any composite natural number N there are polynomials of degree N with integer coefficients which are irreducible in $\mathbb{Z}[x]$

but which are reducible modulo p for every prime p and we have given method of construction of such polynomials for various values of N.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Brandl, R. (1986) Integer Polynomials That Are Reducible Modulo All Primes. *American Mathematical Monthly*, **93**, 286-288. https://doi.org/10.1080/00029890.1986.11971807

[2] Guralnick, R., Schacher, M.M. and Sonn, J. (2005) Irreducible Polynomials Which Are Locally Reducible Everywhere. *Proceedings of the American Mathematical Society*, **133**, 3171-3177. https://doi.org/10.1090/S0002-9939-05-07855-X

[3] Safarevic, I.R. (1956) Construction of Fields of Algebraic Numbers with a Given Soluble Galois Group. *Isv. Nauk. SSSR*, **18**, 274.

[4] Schur, I. (1930) Gleichungen ohne Affeckt. Gesammelte Abhandlungen, Band III, No. 67, 191-197.

[5] Serre, J.-P. (2008) Topics in Galois Theory. A K Peters, Ltd.

[6] Erbach, D.W., Fisher, J. and McKay, J. (1979) Polynomials with PSL (2,7) as Galois Group. *Journal of Number Theory*, **11**, 69-75. https://doi.org/10.1016/0022-314X(79)90020-9

[7] Lang, S. (1993) Algebra. 3rd Edition, Addison Wesley, Boston.

[8] Wielandt, H. (1964) Finite Permutation Groups. Academic Press, New York.

[9] Bernard Dominique, Email Communication.

[10] Stevenhagen, P. and Lenstra, H.W. (1996) Chebotarev and His Density Theorem. *The Mathematical Intelligencer*, **18**, 26-37. https://doi.org/10.1007/BF03027290