Bull. Aust. Math. Soc. **106** (2022), 404–407
doi:10.1017/S0004972722000260

SOLVABILITY OF A SYSTEM OF POLYNOMIAL EQUATIONS MODULO PRIMES

OLLI JÄRVINIEMI

(Received 4 February 2022; accepted 17 February 2022; first published online 23 March 2022)

Abstract

Let F be a system of polynomial equations in one or more variables with integer coefficients. We show that there exists a univariate polynomial $D \in \mathbb{Z}[x]$ such that F is solvable modulo p if and only if the equation $D(x) \equiv 0 \pmod{p}$ has a solution.

2020 *Mathematics subject classification*: primary 11D79; secondary 11R04, 11R09.

Keywords and phrases: prime numbers, polynomial congruences, prime divisors of polynomials, algebraic numbers.

1. Introduction

Let P be a univariate polynomial with integer coefficients. A prime p is said to be a prime divisor of P if p divides $P(n)$ for some integer n. Denote the set of prime divisors of P by $S(P)$.

Consider the structure of the sets $S(P)$. One may easily prove, by elementary means, that $S(P)$ is infinite when P is nonconstant. The Chebotarev density theorem proves that $S(P)$ in fact has positive density in the set of primes (again when P is nonconstant). However, no simple description of the set $S(P)$ is known in the general case, though quadratic reciprocity yields a characterisation in the case $\deg(P) = 2$.

One may further ask what one can say about finite intersections $S(P_1) \cap \cdots \cap S(P_n)$. Again, Chebotarev's theorem shows that such sets have positive density. Nagell [3] has given a more elementary argument proving the infinitude of $S(P_1) \cap S(P_2)$. A somewhat easier proof can be found in [2, Theorem 7].

It turns out that such intersections are again of the form $S(D)$ for some $D \in \mathbb{Z}[x]$.

THEOREM 1.1. *Let $A, B \in \mathbb{Z}[x]$ be nonconstant. There exists a nonconstant polynomial $D \in \mathbb{Z}[x]$ such that $S(A) \cap S(B) = S(D)$.*

Let F be a system of polynomial equations with integer coefficients in finitely many variables. Ax [1] proved that the set $S(F)$ of primes p such that F is solvable modulo

© The Author(s), 2022. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/S0004972722000260 Published online by Cambridge University Press

p may be written as a finite combination of unions, intersections and complements of sets of the form $S(P)$ with $P \in \mathbb{Z}[x]$. This has been improved by van den Dries [4]: one may write $S(F)$ as a finite intersection of sets $S(P)$. Combining this with Theorem 1.1 immediately gives the following result.

THEOREM 1.2. *Let $F_1, \dots, F_m \in \mathbb{Z}[x_1, \dots, x_n]$ be arbitrary. There exists a polynomial $D \in \mathbb{Z}[x]$ such that for any prime p, the system of equations*

$$\begin{cases} F_1(x_1, \dots, x_n) \equiv 0 \pmod{p} \\ F_2(x_1, \dots, x_n) \equiv 0 \pmod{p} \\ \vdots \\ F_m(x_1, \dots, x_n) \equiv 0 \pmod{p} \end{cases}$$

is solvable if and only if $p \in S(D)$.

Clearly, if there are some $G_1, \dots, G_m \in \mathbb{Z}[x_1, \dots, x_n]$ such that $F_1G_1 + \cdots + F_mG_m$ is a nonzero constant, then there are only finitely many primes p with $F_1 \equiv \cdots \equiv F_m \equiv 0 \pmod{p}$ solvable. By the Nullstellensatz, this is equivalent to the assertion that the system $F_1 = \cdots = F_m = 0$ has no complex solutions. In any other case, there are infinitely many such p [4, Proposition 2.7] and D in Theorem 1.2 is nonconstant.

It seems that the results above are known to experts. However, it is relatively difficult to find references for the results, especially if one wishes to find elementary treatments. A proof of Theorem 1.2 (using algebraic geometric language) may be found in [5]. An elementary exposition, which falls a little short of Theorem 1.1, is given in [2] (in particular Theorem 11 there).

The purpose of this note is to give a short, self-contained and elementary proof of Theorem 1.1. Our approach is not far from the ideas of [2]. The proof is constructive, allowing one to take $\deg(D) \le \deg(A)\deg(B)$. This is optimal in the general case (see the remarks after the proof).

The result of Theorem 1.2 is considerably more difficult: one needs some version of the Lang–Weil bound to deduce that 'generic' systems with $m < n$ are solvable modulo p for p large enough, and such results are not easy to prove.

2. Proof of Theorem 1.1

We begin by proving that to obtain Theorem 1.1, it suffices to show that for any monic $A, B \in \mathbb{Z}[x]$, there exists $D \in \mathbb{Z}[x]$ such that $S(A) \cap S(B)$ and $S(D)$ differ by only finitely many primes. This follows from the following two lemmas.

LEMMA 2.1. *Let $P \in \mathbb{Z}[x]$ and p be given. There exist polynomials $P_+, P_- \in \mathbb{Z}[x]$ such that $S(P_+) = S(P) \cup \{p\}$ and $S(P_-) = S(P) \setminus \{p\}$.*

PROOF. Take $P_+(x) = pP(x)$. If $P(0) = 0$, take $P_-(x) = px + 1$. Otherwise, let $P_-(x) = P(p^{k+1}x)/p^k$, where p^k is the largest power of p dividing $P(0)$. One easily checks that this works. □

https://doi.org/10.1017/S0004972722000260 Published online by Cambridge University Press

LEMMA 2.2. *Let $P \in \mathbb{Z}[x]$ be given. There exists a monic polynomial $Q \in \mathbb{Z}[x]$ such that $S(P)$ and $S(Q)$ differ by only finitely many elements.*

PROOF. Let c be the leading coefficient of P. One easily checks that the polynomial $Q(x) = c^{\deg(P)-1}P(x/c)$ works. □

We make the further reduction that A and B may be assumed to be irreducible. Assume we have proven Theorem 1.1 for irreducible and monic A, B. Now, by Gauss's lemma, write $A = A_1 \cdots A_a$ and $B = B_1 \cdots B_b$, where $A_i, B_j \in \mathbb{Z}[x]$ are irreducible and monic. Let $D_{i,j} \in \mathbb{Z}[x]$ be such that $S(A_i) \cap S(B_j) = S(D_{i,j})$. Then $S(A) \cap S(B) = S(D)$, where D is the product of all the $D_{i,j}$.

Hence, assume A and B are monic and irreducible. Fix any root α of A. As usual, denote by $\mathbb{Z}/p\mathbb{Z}$ the integers modulo p and let $\mathbb{Z}[\alpha] = \{P(\alpha) \mid P \in \mathbb{Z}[x]\}$.

LEMMA 2.3. *Let $p \in S(A)$ be a prime and let a be an integer such that $A(a) = 0$. There exists a homomorphism $\varphi : \mathbb{Z}[\alpha] \to \mathbb{Z}/p\mathbb{Z}$ with $\varphi(\alpha) \equiv a \pmod p$.*

PROOF. For $\beta \in \mathbb{Z}[\alpha]$, write $\beta = P(\alpha), P \in \mathbb{Z}[x]$, and define $\varphi(\beta) \equiv P(a) \pmod p$. This is well defined, since if $\beta = P_1(\alpha) = P_2(\alpha)$, then $P_1 - P_2$ has α as its root and thus is divisible by the minimal polynomial A, resulting in $P_1(a) \equiv P_2(a) \pmod p$. Clearly, φ is a homomorphism with $\varphi(\alpha) \equiv a \pmod p$. □

Factorise B in $\mathbb{Q}(\alpha)[x]$ into a product $E_1E_2 \cdots E_t$ of irreducibles. By Gauss's lemma, we may take the coefficients of E_i to lie in $\mathbb{Z}[\alpha]$. Let $\beta_1, \ldots, \beta_t$ be some roots of $E_1, \ldots, E_t$. By the primitive element theorem, let $G_1, \ldots, G_t \in \mathbb{Z}[x, y]$ be such that $\mathbb{Q}(\alpha, \beta_i) = \mathbb{Q}(G_i(\alpha, \beta_i))$. (One may take $G_i(x, y) = x + n_i y$ for some suitable $n_i \in \mathbb{Z}$.) Let D_i be the minimal polynomial of $G_i(\alpha, \beta_i)$ and let

$$D = D_1 \cdots D_t.$$

We show that $S(A) \cap S(B)$ and $S(D)$ differ by only finitely many primes, which proves the theorem. This is done in the following two lemmas.

LEMMA 2.4. *We have $S(A) \cap S(B) \subset S(D) \cup T$ for some finite set T.*

PROOF. For each i, define $D_i^*(x) = D_i(G_i(\alpha, x))$. Hence, $D_i^* \in \mathbb{Z}[\alpha][x]$ has β_i as its root, so D_i^* is divisible by E_i. Write $D_i^* = E_iF_i$, where the coefficients of F_i are polynomials in α with rational coefficients. Let $c \in \mathbb{Z}_+$ be such that $cF_i \in \mathbb{Z}[\alpha][x]$ for all i.

Assume $p \in S(A) \cap S(B)$ does not divide c. Let $a, b \in \mathbb{Z}$ be such that $A(a) \equiv B(b) \equiv 0 \pmod p$, and let φ be as in Lemma 2.3. Then modulo p,

$$0 \equiv \varphi(0) \equiv \varphi(B(b)) \equiv \varphi(E_1(b) \cdots E_t(b)) \equiv \varphi(E_1(b)) \cdots \varphi(E_t(b)) \pmod p.$$

Let i be such that $\varphi(E_i(b)) \equiv 0 \pmod p$. Now,

$$0 \equiv \varphi(E_i(b))\varphi(cF_i(b)) \equiv \varphi(cD_i^*(b)) \equiv c\varphi(D_i(G_i(\alpha, b))) \equiv cD_i(G_i(a, b)) \pmod p,$$

and hence $p \in S(D_i) \subset S(D)$. □

LEMMA 2.5. *We have $S(D) \subset (S(A) \cap S(B)) \cup T$ for some finite set T.*

https://doi.org/10.1017/S0004972722000260 Published online by Cambridge University Press

PROOF. The argument is relatively standard (see, for example, [2, Theorem 2]).

It suffices to show that for any i and any large enough prime $p \in S(D_i)$, we have $p \in S(A) \cap S(B)$. We show that $p \in S(A)$ for large $p \in S(D_i)$. The proof for B is similar. Let $\gamma_i = G_i(\alpha, \beta_i)$. By the choice of G_i, there exists $P \in \mathbb{Q}[x]$ such that $P(\gamma_i) = \alpha$. Now $A(P(\gamma_i)) = 0$, so we may write $A(P(x)) = D_i(x)Q(x)$ for $Q \in \mathbb{Q}[x]$. Let $c \in \mathbb{Z}_+$ be such that $cQ \in \mathbb{Z}[x]$.

Assume that $p \in S(D_i)$ does not divide c nor the denominator of any coefficient of P. Let $d \in \mathbb{Z}$ be such that $D_i(d) \equiv 0 \pmod{p}$. Then $cA(P(d)) = D_i(d) \cdot cQ(d) \equiv 0 \pmod{p}$. Hence, there is a rational number $P(d) = r/s$ with $p \nmid s$ such that $cA(r/s)$ is an integer divisible by p. A calculation reveals that $cA(rs^{p-2})$ is divisible by p, corresponding to the fact that r/s may be interpreted modulo p as $rs^{p-2} \pmod{p}$ (by Fermat's little theorem), and therefore $p \in S(A)$. □

REMARK 2.6. An easy calculation shows the constructed D has degree $\deg(A)\deg(B)$.

REMARK 2.7. There are A and B such that any D with $S(A) \cap S(B) = S(D)$ satisfies $\deg(D) \geq \deg(A)\deg(B)$. By the Chebotarev density theorem, the density of $S(P)$ is at least $1/\deg(P)$ for any nonconstant $P \in \mathbb{Z}[x]$. If A and B are such that $S(A) \cap S(B)$ has density $1/\deg(A)\deg(B)$ (take A and B to be, for example, the nth and mth cyclotomic polynomials for $(n, m) = 1$), then $S(A) \cap S(B) = S(D)$ implies $\deg(D) \geq \deg(A)\deg(B)$.

REMARK 2.8. Combining the results of the previous remarks shows that the density of $S(P_1) \cap \cdots \cap S(P_n)$ is at least $1/\deg(P_1) \cdots \deg(P_n)$ for nonconstant P_i. Some equality cases are given by quadratic or cyclotomic polynomials.

REMARK 2.9. With slightly more care, one can prove the following strengthening of Theorem 1.1: for any A, B, there exists D such that $A(x) \equiv B(y) \equiv 0 \pmod{m}$ is solvable if and only if $D(z) \equiv 0 \pmod{m}$, where the modulus m is not necessarily a prime. (One needs the following consequence of Hensel's lemma: if $P \in \mathbb{Z}[x]$ is given, for all but finitely many primes $p \in S(P)$, the equation $P(x) \equiv 0 \pmod{p^k}$ is solvable for any $k \in \mathbb{Z}_+$.)

References

[1] J. Ax, 'Solving Diophantine problems modulo every prime', *Ann. of Math. (2)* **85**(2) (1967), 161–183.

[2] I. Gerst and J. Brillhart, 'On the prime divisors of polynomials', *Amer. Math. Monthly* **78**(3) (1971), 250–266.

[3] T. Nagell, 'Sur les diviseurs premiers des polynômes', *Acta Arith.* **3**(15) (1969), 235–244.

[4] L. van den Dries, 'A remark on Ax's theorem on solvability modulo primes', *Math. Z.* **208**(1) (1991), 65–70.

[5] R. van Dobben de Bruyn, 'Set of primes p such that $\mathsf{Hom}(a, F_p) = \varnothing$', *MathOverflow*. Available at https://mathoverflow.net/q/392425.

OLLI JÄRVINIEMI, Department of Mathematics and Statistics,
University of Turku, FI-20014 Turun yliopisto, Finland
e-mail: olli.a.jarviniemi@utu.fi

https://doi.org/10.1017/S0004972722000260 Published online by Cambridge University Press