

SUBGROUP AVOIDANCE FOR PRIMES DIVIDING THE VALUES OF A POLYNOMIAL

PAUL POLLACK

*In memory of those Jewish mathematicians, such as
Mihály Bauer and Alfred Brauer, persecuted during the Nazi era.*

ABSTRACT. For $f \in \mathbb{Q}[x]$, we say that a rational prime p is a *prime divisor* of f if p divides the numerator of $f(n)$ for some integer n . Let $\mathcal{P}(f)$ denote the set of prime divisors of f . We present an elementary proof of the following theorem, which generalizes results of Bauer and Brauer: fix a nonzero integer g . Suppose that $f(x) \in \mathbb{Q}[x]$ is a nonconstant polynomial having a root in \mathbb{Q}_p for every prime p dividing g , and having a root in \mathbb{R} if $g < 0$. Let m be a positive integer coprime to g , and let H be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ not containing $g \bmod m$. Then there are infinitely many primes $p \in \mathcal{P}(f)$ with $p \bmod m \notin H$.

1. Introduction. In 1837, Dirichlet showed that every arithmetic progression $a \bmod m$ with $\gcd(a, m) = 1$ contains infinitely many prime numbers. One of the most surprising aspects of Dirichlet's beautiful proof is the crucial use it makes of ideas and methods from analysis. A number of researchers have investigated how essential analytic methods are to obtaining Dirichlet's result. Particularly noteworthy are the works of Zassenhaus [19], Selberg [14] and Shapiro [15], where proofs are given that minimize analytic prerequisites, even avoiding any use of infinite series.

While the proofs of Zassenhaus, Selberg and Shapiro are elementary in a technical sense, the analysis is hidden just beneath the surface. Anyone picking up one of these papers will quickly realize that they

2010 AMS *Mathematics subject classification*. Primary 11N32, Secondary 11A41, 11N13.

Keywords and phrases. Primes in progressions, Dirichlet's theorem, elementary methods, prime divisors of polynomials.

The VIGRE group was supported by NSF RTG, grant No. DMS-1344994. The author was supported by NSF, grant No. DMS-1402268.

Received by the editors on December 16, 2015, and in revised form on January 18, 2016.

have wandered into the woods of analytic number theory. Thus, it is still reasonable to ask whether there exists an elementary *algebraic* approach to Dirichlet's result. It seems that no argument of this kind is known that yields the theorem for all coprime progressions. However, such proofs are available in several special cases.

The most famous examples are the progressions 2 mod 3 and 3 mod 4. That both of these progressions contain infinitely many primes can be established by a simple variant of Euclid's famous argument. Indeed, this is a common exercise in first courses in elementary number theory. Attempting to push this Euclidean method to its natural limit, one is led to the following "subgroup avoidance" theorem, which appears in Marcus's text on algebraic number theory [8, page 205, Exercise 6].

Theorem A. *Let m be a positive integer, and let H be a proper subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$. There are infinitely many primes p with $p \bmod m \notin H$.*

Another special case of Dirichlet's theorem that has often been discussed in the literature is that of the progression 1 mod m , see [12, pages 87–90] for several references. For each polynomial f with rational coefficients, define

$$\mathcal{P}(f) = \{\text{primes } p : \nu_p(f(n)) > 0 \text{ for some integer } n\}.$$

(Here ν_p is the usual p -adic valuation.) We refer to the elements of $\mathcal{P}(f)$ as the *prime divisors* of f . For two sets of primes \mathcal{P} and \mathcal{Q} , we write $\mathcal{P} \doteq \mathcal{Q}$ to mean that the symmetric difference of \mathcal{P} and \mathcal{Q} is finite. Letting Φ_m denote the m th cyclotomic polynomial, it can be proven in an elementary way that

$$(1.1) \quad \mathcal{P}(\Phi_m) \doteq \{\text{primes } p \equiv 1 \pmod{m}\}.$$

(This quickly follows from the cyclicity of $(\mathbb{Z}/p\mathbb{Z})^\times$ and the following well-known algebraic fact: *over any field of characteristic not dividing m , the roots of Φ_m are the primitive m th roots of unity.* For an explicit reference, see [5, Theorem 8].) It is straightforward to prove that the left-hand side of (1.1) is infinite; indeed, a simple variant of Euclid's argument shows that $\mathcal{P}(f)$ is infinite for any nonconstant f , see [5, Theorem 1] or [13, pages 40–41]. Hence, the right-hand side of (1.1) is also infinite.

This discussion shows that extra hypotheses are needed to prove an analogue of Theorem A where the primes p are restricted to a set $\mathcal{P}(f)$. Indeed, when $f = \Phi_m$, all but finitely many prime divisors p of f are $1 \pmod m$, and thus, $p \pmod m$ belongs to every subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$. In this note, these extra hypotheses are examined.

The first subgroup avoidance result for $\mathcal{P}(f)$ is due to Bauer [2], see [6, Section 108] and [11, Section 49] for expositions. It appears as a waystation in his elementary, algebraic proof that there are always infinitely many primes $p \equiv -1 \pmod m$.

Theorem B ([2]). *Let f be a nonconstant polynomial with rational coefficients and a real root of odd multiplicity. For every $m \geq 3$, the set $\mathcal{P}(f)$ contains infinitely many primes $p \not\equiv 1 \pmod m$.*

It was noted by Brauer [3] that Theorem B can be pushed further in the direction of Theorem A.

Theorem C ([3]). *Let f be a nonconstant polynomial with rational coefficients and at least one real root. Let m be a positive integer, and let H be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ not containing $-1 \pmod m$. Then, the set $\mathcal{P}(f)$ contains infinitely many primes p with $p \pmod m \notin H$.*

We will prove, in an elementary, algebraic way, the following natural generalization of Theorem C.

Theorem 1.1. *Fix a nonzero integer g . Let m be a positive integer prime to g , and let H be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ not containing $g \pmod m$. Suppose that f is a nonconstant polynomial with rational coefficients having a root in \mathbb{Q}_p for every prime p dividing g , and having a root in \mathbb{R} if $g < 0$. Then, there are infinitely many primes $p \in \mathcal{P}(f)$ with $p \pmod m \notin H$.*

In keeping with the goal of remaining as down to earth as possible, our proof will use none of the theory of algebraic numbers and only the bare rudiments of the theory of p -adic numbers.

Example 1.2. Let $g = 17$ and $m = 3$, and let H be the trivial subgroup of $(\mathbb{Z}/3\mathbb{Z})^\times$. A simple application of Hensel’s lemma shows that the conditions of Theorem 1.1 hold with $f(x) = x^4 + 1$. We deduce that there are infinitely many prime divisors of f with $p \equiv 2 \pmod 3$.

From (1.1),

$$\mathcal{P}(f) = \mathcal{P}(\Phi_8) \doteq \{\text{primes } p \equiv 1 \pmod{8}\}.$$

Consequently, we have proved, using an elementary, algebraic method, that there are infinitely many primes $p \equiv 17 \pmod{24}$.

In Example 1.2, any novelty claimed is for the approach, rather than the final result. Indeed, $17^2 \equiv 1 \pmod{24}$, and it was shown in 1912 by Schur [13] that, whenever $a^2 \equiv 1 \pmod{m}$, there is an algebraic proof of Dirichlet's theorem for the progression $a \pmod{m}$. Full details for the particular case $m = 24$ are presented in [1]. Conversely, Murty has shown that, in a certain precise sense, Schur's are the only progressions for which such proofs can be given, [9, 10].

The reader interested in a thorough development of the basic theory of prime divisors of polynomials from an elementary point of view should consult the article of Gerst and Brillhart [5]. Additional references concerning algebraic approaches to cases of Dirichlet's theorem include [7, 16, 17, 18].

2. Proof of Theorem 1.1. We need two lemmas. The first is a well-known result on independence of valuations. In what follows, the *primes* of \mathbb{Q} are the standard finite primes $2, 3, 5, 7, \dots$, along with ∞ . We let $|\cdot|_\infty$ denote the usual (Archimedean) absolute value, and, for finite p , we let $|\cdot|_p = p^{-\nu_p(\cdot)}$.

Proposition 2.1 (Strong approximation). *Fix a prime p_0 of \mathbb{Q} . Let \mathcal{S} be a finite set of primes of \mathbb{Q} distinct from p_0 . For each $p \in \mathcal{S}$, suppose that an element $\alpha_p \in \mathbb{Q}_p$ is given. For every $\epsilon > 0$, there is an $\alpha \in \mathbb{Q}$ with*

$$|\alpha - \alpha_p|_p < \epsilon \quad \text{for all } p \in \mathcal{S}$$

and

$$|\alpha_p|_p \leq 1 \quad \text{for all } p \notin \mathcal{S}, \text{ except possibly } p = p_0.$$

While we do not give its proof here, Proposition 2.1 is not deep; it is essentially equivalent to the classical Chinese remainder theorem. For a full treatment of the analogous result in a general global field, see [4, pages 67–68].

Lemma 2.2. *Let f be a nonconstant polynomial with rational coefficients. Suppose that f has a simple root in \mathbb{Q}_p , where p is a finite prime. Then, for all sufficiently large natural numbers ν , there is an $\alpha \in \mathbb{Q}_p$ with $\nu_p(f(\alpha)) = \nu$.*

Proof. Let α be a simple root of f in \mathbb{Q}_p , and write $f(x) = (x - \alpha)q(x)$, where $q(x) \in \mathbb{Q}_p[x]$ and $q(\alpha) \neq 0$. For each natural number n , let $\alpha_n = \alpha + p^n$. Then,

$$\nu_p(f(\alpha_n)) = \nu_p(\alpha_n - \alpha) + \nu_p(q(\alpha_n)) = n + \nu_p(q(\alpha_n)).$$

By continuity,

$$q(\alpha_n) \longrightarrow q(\alpha) \quad \text{as } n \rightarrow \infty.$$

Since $q(\alpha) \neq 0$, we have $\nu_p(q(\alpha_n)) = \nu_p(q(\alpha)) = C$ (say) for all large enough n . Therefore, $\nu_p(f(\alpha_n)) = n + C$ for all large n , and the lemma follows. □

We can now prove the main theorem.

Proof of Theorem 1.1. Put $f_0 = f$. Let $f_1(x) = f_0(x + t)$, where $t \in \mathbb{Z}$ is chosen so that $f(x + t)$ has a nonzero constant term. Let $f_2 = f_1 / \gcd(f_1, f_1')$, so that f_2 has only simple roots. Scale f_2 to have constant term 1, and call the result f_3 . Finally, let $f_4(x) = f_3(Ax)$, where the nonzero integer A is chosen such that $f_3(Ax)$ has integer coefficients. It is straightforward to check that $\mathcal{P}(f_i) \doteq \mathcal{P}(f_{i+1})$ for each $i = 0, 1, 2, 3$. (It is helpful here to observe that f_2 and f_1 have the same irreducible factors in $\mathbb{Q}[x]$, with possibly different multiplicities.) Hence, it suffices to verify the conclusion of the theorem for f_4 instead of f , that is, we can (and will) assume that f has the form

$$(2.1) \quad f(x) = 1 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

where each $a_i \in \mathbb{Z}$, and that f has no multiple roots.

We introduce three sets of primes defined as follows. Let

$$\mathcal{S}_1 = \{\text{finite primes dividing } g\} \cup \{\infty\},$$

$$\mathcal{S}_2 = \{\text{finite primes dividing } m\},$$

$$\mathcal{S}_3 = \{p \in \mathcal{P}(f) : p \nmid m, p \bmod m \notin H, p \notin \mathcal{S}_1\}.$$

Then, $\mathcal{S}_1, \mathcal{S}_2$ and \mathcal{S}_3 are pairwise disjoint. Clearly, \mathcal{S}_1 and \mathcal{S}_2 are finite sets. If the conclusion of Theorem 1.1 fails, then \mathcal{S}_3 is also finite.

We now suppose \mathcal{S}_3 is finite and proceed to derive a contradiction.

Let B be a large positive (fixed) integer, to be specified more precisely momentarily. For each finite prime $p \in \mathcal{S}_1$, fix an $\alpha_p \in \mathbb{Q}_p$ with

$$\nu_p(f(\alpha_p)) = B\nu_p(g).$$

That this is possible for all large enough B follows from Lemma 2.2, since f has a simple root over \mathbb{Q}_p for all $p \in \mathcal{S}_1$. If $g < 0$, we are assuming that f has a simple root over \mathbb{R} , and we fix $\alpha_\infty \in \mathbb{R}$ with $f(\alpha_\infty) < 0$. If $g > 0$, we set $\alpha_\infty = 0$, so that $f(\alpha_\infty) = 1$. In either case,

$$\text{sgn}(f(\alpha_\infty)) = \text{sgn}(g).$$

Finally, fix a prime $p_0 \equiv 1 \pmod{m}$ larger than any finite element of $\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$; the existence of p_0 follows from the (algebraic) results reviewed in the introduction.

We claim it is possible to choose $\alpha \in \mathbb{Q}$ with

$$(2.2) \quad \nu_p(f(\alpha)) = B\nu_p(g) \quad \text{for all finite primes } p \in \mathcal{S}_1,$$

with

$$(2.3) \quad \text{sgn}(f(\alpha)) = \text{sgn}(g),$$

with

$$(2.4) \quad \nu_p(\alpha) \geq B \quad \text{if } p \in \mathcal{S}_2 \cup \mathcal{S}_3,$$

and with

$$(2.5) \quad \nu_p(\alpha) \geq 0 \quad \text{for all } p \notin \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \{p_0\}.$$

Conditions (2.2) and (2.3) can be enforced by selecting α sufficiently close to α_p for all $p \in \mathcal{S}_1$, while (2.4) can be enforced by selecting α close to $0 \in \mathbb{Q}_p$ for $p \in \mathcal{S}_2 \cup \mathcal{S}_3$. The existence of the desired rational number α thus follows from strong approximation (Proposition 2.1).

Conditions (2.2) and (2.3) together imply that

$$f(\alpha) = \text{sgn}(g)|g|^B \cdot r$$

for a certain $r \in \mathbb{Q}$ with $r > 0$ and with

$$(2.6) \quad \nu_p(r) = 0 \quad \text{for all finite primes } p \mid g.$$

We now impose the conditions that B is odd and that $\gcd(B, \phi(m)) = 1$. Then, $\text{sgn}(g) = \text{sgn}(g)^B$, and thus, in fact,

$$(2.7) \quad f(\alpha) = g^B r.$$

From the form of f in (2.1) and the valuation conditions in (2.4),

$$(2.8) \quad \nu_p(f(\alpha) - 1) \geq B > 0 \quad \text{for each } p \in \mathcal{S}_2 \cup \mathcal{S}_3.$$

Note that this forces $\nu_p(f(\alpha)) = 0$ for all $p \in \mathcal{S}_2 \cup \mathcal{S}_3$, and hence,

$$(2.9) \quad \nu_p(r) = 0 \quad \text{for all } p \in \mathcal{S}_2 \cup \mathcal{S}_3.$$

Since both sides of (2.7) are integral at all primes dividing m , it makes sense to reduce (2.7) modulo m . Assuming that B is sufficiently large, (2.7) and (2.8) yield

$$1 \equiv f(\alpha) \equiv g^B r \pmod{m},$$

and hence, $r \pmod{m}$ generates the same subgroup as $g^B \pmod{m}$. Since B is coprime to $\phi(m)$, that subgroup coincides with the one generated by $g \pmod{m}$. Therefore, if $r \pmod{m}$ were in H , $g \pmod{m} \in H$, contrary to assumption. Hence, using $r > 0$, there must be some finite prime P having $\nu_P(r) \neq 0$ and $P \pmod{m} \notin H$.

Clearly, $P \neq p_0$ since $p_0 \pmod{m} = 1 \pmod{m} \in H$, whereas $P \pmod{m} \notin H$. From (2.6) and (2.9), we deduce that $P \notin \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$. Recalling (2.5), α is P -integral. Since f has integer coefficients and $P \nmid g$,

$$\nu_P(r) = \nu_P(f(\alpha)) \geq 0.$$

Since $\nu_P(r) \neq 0$, it must be that $\nu_P(f(\alpha)) > 0$. As α is P -integral, it follows that $P \in \mathcal{P}(f)$. Hence, P is a prime of $\mathcal{P}(f)$ not dividing mg with $P \pmod{m} \notin H$ and with $P \notin \mathcal{S}_3$. This contradicts the definition of \mathcal{S}_3 . □

Acknowledgments. The author was inspired to think about these questions while co-leading a Fall 2015 VIGRE graduate student research group, *Introduction to the process of mathematical research*. He thanks the student participants for useful in-class discussions, and he thanks his co-leader Pete L. Clark for many enlightening conversations. He is also grateful to Andrew Granville, from whom he first learned about Theorem A, and the referee, for a careful reading of the manuscript.

REFERENCES

1. P.T. Bateman and M.E. Low, *Prime numbers in arithmetic progressions with difference 24*, Amer. Math. Month. **72** (1965), 139–143.
2. Mihály Bauer, *Über die arithmetische Reihe*, J. reine angew. Math. **131** (1906), 265–267.
3. Alfred Brauer, *A theorem of M. Bauer*, Duke Math. J. **13** (1946), 235–238.
4. J.W.S. Cassels and A. Fröhlich, eds., *Algebraic number theory*, Academic Press, Inc., London, 1986.
5. I. Gerst and J. Brillhart, *On the prime divisors of polynomials*, Amer. Math. Month. **78** (1971), 250–266.
6. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Chelsea Publishing Company, New York, 1953.
7. H.W. Lenstra, Jr., and P. Stevenhagen, *Primes of degree one and algebraic cases of Čebotarev's theorem*, Enseign. Math. **37** (1991), 17–30.
8. D.A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York, 1977.
9. M.R. Murty, *Primes in certain arithmetic progressions*, J. Madras University **51** (1988), 161–169.
10. M.R. Murty and N. Thain, *Prime numbers in certain arithmetic progressions*, Funct. Approx. Comm. Math. **35** (2006), 249–259.
11. T. Nagell, *Introduction to number theory*, Chelsea Publishing Company, New York, 1964.
12. W. Narkiewicz, *The development of prime number theory*, Springer Mono. Math., Springer-Verlag, Berlin, 2000.
13. I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungsber. Berlin. Math. Ges. **11** (1912), 40–50.
14. A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Ann. Math. **50** (1949), 297–304.
15. H.N. Shapiro, *On primes in arithmetic progression*, II, Ann. Math. **52** (1950), 231–243.
16. J. Wójcik, *A refinement of a theorem of Schur on primes in arithmetic progressions*, Acta Arith. **11** (1966), 433–436.
17. ———, *A refinement of a theorem of Schur on primes in arithmetic progressions*, II, Acta Arith. **12** (1966), 97–109.
18. ———, *A refinement of a theorem of Schur on primes in arithmetic progressions*, III, Acta Arith. **15** (1968), 193–197.
19. H. Zassenhaus, *Über die Existenz von Primzahlen in arithmetischen progressionen*, Comm. Math. Helv. **22** (1949), 232–259.

UNIVERSITY OF GEORGIA, BOYD GRADUATE STUDIES RESEARCH CENTER, DEPARTMENT OF MATHEMATICS, ATHENS, GA 30602

Email address: pollack@uga.edu