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 Mihály Bauer and Alfred 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 worthy of note 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 realize early on that they have wandered into the woods of analytic number theory. So 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

---

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.

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 as Exercise 6 on p. 205 of Marcus's text on algebraic number theory [**8**].

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,** pp. 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 mth cyclotomic polynomial, one can prove in an elementary way that

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

(This follows quickly 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 mth roots of unity.* For an explicit reference, see [**5,** Theorem 8].) It is straightforward to prove that the left-hand side of (1) is infinite — indeed, a simple variant of Euclid's argument shows that $\mathcal{P}(f)$ is infinite for any nonconstant f (see [**13,** pp. 40–41] or [**5,** Theorem 1]). Hence, the right-hand side of (1) is also infinite.

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

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

Theorem B (Bauer)**.** *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 noticed by Brauer **[3]** that one can push Theorem B further in the direction of Theorem A.

Theorem C (Brauer)**.** *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 $-1 \bmod m$. Then the set $\mathcal{P}(f)$ contains infinitely many primes p with $p \bmod m \notin H$.*

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

Theorem 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 $g \bmod m$. 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 $p \bmod m \notin H$.*

In keeping with the goal of staying 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. 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 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), $\mathcal{P}(f) = \mathcal{P}(\Phi_8) \doteq \{\text{primes } p \equiv 1 \pmod 8\}$. Consequently, we have proved in an elementary, algebraic way that there are infinitely many primes $p \equiv 17 \pmod{24}$.

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

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

2. Proof of Theorem 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 usual finite primes $2, 3, 5, 7, \dots$, together 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 (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 we are given an element $\alpha_p \in \mathbb{Q}_p$. For every $\epsilon > 0$, there is an $\alpha \in \mathbb{Q}$ with*

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

and

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

While we do not give its proof here, Proposition 2 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,** pp. 67–68].

Lemma 3. *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, $q(\alpha_n) \to q(\alpha)$ as $n \to \infty$. Since $q(\alpha) \neq 0$, we have $\nu_p(q(\alpha_n)) = \nu_p(q(\alpha)) = C$ (say) for all large enough n. So $\nu_p(f(\alpha_n)) = n + C$ for all large n, and the lemma follows. □

We can now prove the main theorem.

Proof of Theorem 1. 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 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 so 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 $\mathbb{Q}[x]$, only 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

$$f(x) = 1 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{2}$$

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 the theorem 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 integer, thought of as fixed, and 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 3, since f has a simple root over $\mathbb{Q}_p$ for all $p \in \mathcal{S}_1$. If $g < 0$, we are assuming 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,

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

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

$$\nu_p(f(\alpha)) = B\nu_p(g) \quad \text{for all finite primes } p \in \mathcal{S}_1, \tag{3}$$

with

$$\operatorname{sgn}(f(\alpha)) = \operatorname{sgn}(g), \tag{4}$$

with

$$\nu_p(\alpha) \geq B \quad \text{if } p \in \mathcal{S}_2 \cup \mathcal{S}_3, \tag{5}$$

and with

$$\nu_p(\alpha) \geq 0 \quad \text{for all } p \notin \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \{p_0\}. \tag{6}$$

Conditions (3) and (4) can be enforced by selecting α sufficiently close to α_p for all $p \in \mathcal{S}_1$, while (5) 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).

Conditions (3) and (4) together imply that

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

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

$$\nu_p(r) = 0 \quad \text{for all finite primes } p \mid g. \tag{7}$$

We now impose the condition that B is odd and that $\gcd(B, \varphi(m)) = 1$. Then $\operatorname{sgn}(g) = \operatorname{sgn}(g)^B$, and so in fact

$$f(\alpha) = g^B r. \tag{8}$$

From the form of f in (2) and the valuation conditions in (5),

$$\nu_p(f(\alpha) - 1) \geq B > 0 \quad \text{for each } p \in \mathcal{S}_2 \cup \mathcal{S}_3. \tag{9}$$

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

$$\nu_p(r) = 0 \quad \text{for all } p \in \mathcal{S}_2 \cup \mathcal{S}_3. \tag{10}$$

Since both sides of (8) are integral at all primes dividing m, it makes sense to reduce (8) modulo m. Assuming that B is sufficiently large, (8) and (9) yield

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

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

Clearly, $P \neq p_0$, since $p_0 \bmod m = 1 \bmod m \in H$ whereas $P \bmod m \notin H$. From (7) and (10), we deduce that $P \notin \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$. Recalling (6), 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 $P \bmod m \notin H$ and with $P \notin \mathcal{S}_3$. This contradicts the definition of $\mathcal{S}_3$. $\square$

Acknowledgements. 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. The VIGRE group is supported by NSF RTG award DMS-1344994, and the author's research is supported by NSF award DMS-1402268.

REFERENCES

1. P.T. Bateman and M.E. Low, *Prime numbers in arithmetic progressions with difference* 24, Amer. Math. Monthly **72** (1965), 139–143.

2. M. Bauer, *Über die arithmetische Reihe*, J. Reine Angew. Math. **131** (1906), 265–267.

3. A. 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. Reprint of the 1967 original.

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

6. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*, 2nd ed., Chelsea Publishing Co., New York, 1953.

7. H.W. Lenstra, Jr. and P. Stevenhagen, *Primes of degree one and algebraic cases of Čebotarev's theorem*, Enseign. Math. (2) **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. Comment. Math. **35** (2006), 249–259.

11. T. Nagell, *Introduction to number theory*, 2nd ed., Chelsea Publishing Co., New York, 1964.

12. W. Narkiewicz, *The development of prime number theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

13. I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungsber. Berliner Math. Ges. **11** (1912), 40–50.

14. A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Ann. of Math. (2) **50** (1949), 297–304.

15. H.N. Shapiro, *On primes in arithmetic progression. II*, Ann. of Math. (2) **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** (1966/1967), 97–109.

18. ———, *A refinement of a theorem of Schur on primes in arithmetic progressions. III*, Acta Arith **15** (1968/1969), 193–197.

19. H. Zassenhaus, *Über die Existenz von Primzahlen in arithmetischen Progressionen*, Comment. Math. Helv. **22** (1949), 232–259.

University of Georgia, Department of Mathematics, Boyd Graduate Studies Research Center, Athens, Georgia 30602
Email address: **pollack@uga.edu**