AN EASY GENERALIZATION OF EULER'S THEOREM ON THE SERIES OF PRIME RECIPROCALS

PAUL POLLACK

ABSTRACT. It is well-known that Euclid's argument can be adapted to prove the infinitude of primes of the form $4k-1$. We describe a simple proof that the sum of the reciprocals of all such primes diverges. More generally, if q is a positive integer, and H is a proper subgroup of the units group $(\mathbf{Z}/q\mathbf{Z})^\times$, we show that

$$\sum_{\substack{p \text{ prime} \\ p \bmod q \notin H}} \frac{1}{p} = \infty.$$

1. INTRODUCTION

Perhaps no argument in number theory is more famous than Euclid's proof of the infinitude of primes. It is a traditional exercise in a first course in number theory to extend Euclid's argument to certain special arithmetic progressions. For example, take the progression $2, 5, 8, 11, \dots$ consisting of the positive integers of the form $3m-1$. Let $p_1, \dots, p_k$ be any finite list of primes of the form $3m-1$, and consider the integer $P := 3p_1 \cdots p_k - 1$. Now P factors into primes, all of which are either of the form $3m+1$ or $3m-1$. The product of numbers of the form $3m+1$ is again of the form $3m+1$, whereas P has the form $3m-1$. Thus, P must have some prime divisor of the form $3m-1$, and clearly this prime cannot be any of the p_i. It follows that we can extend the list $p_1, \dots, p_k$ indefinitely; that is, there are infinitely many primes in the progression $3m-1$.

Reasoning along similar lines, one obtains a proof of the following result, which is given as an exercise in D. A. Marcus's text on algebraic number theory [5, Exercise 6, p. 205]. We write $p \bmod q$ for the element of $\mathbf{Z}/q\mathbf{Z}$ representing the reduction of p modulo q.

Theorem A. *Let q be a positive integer. Suppose that H is a proper subgroup of the unit group $(\mathbf{Z}/q\mathbf{Z})^\times$. Then there are infinitely many primes p for which $p \bmod q \notin H$.*

Our primary objective here is to showcase a proof, almost as simple, for the following strengthening of Theorem A.

Theorem 1. *Let q be a positive integer. Suppose that H is a proper subgroup of the unit group $(\mathbf{Z}/q\mathbf{Z})^\times$. Then*

$$\sum_{\substack{p \text{ prime} \\ p \bmod q \notin H}} \frac{1}{p} = \infty.$$

Theorem 1 bears the same relation to Theorem A as Euler's result on the divergence of the series of prime reciprocals bears to Euclid's theorem.

Note that except in very special cases, the complement of H is a union of several progressions modulo q and not a single progression. Indeed, we only get

a divergence result from Theorem 1 for an individual progression when $\phi(q) = 2$ and $|H| = 1$, corresponding to $q \in \{3, 4, 6\}$ and $H = \{1 \bmod q\}$. (Note also that the $q = 6$ result is the same as the result for $q = 3$.) Thus, Theorem 1 is much weaker than Dirichlet's 1837 result that the primes belonging to any given coprime progression modulo q have divergent reciprocal sum. However, all known proofs of Dirichlet's theorem are much more difficult than the simple argument we give for Theorem 1.

In the case when $\phi(q) = 2$, a short, elementary proof of Theorem 1 was given earlier by Tibor Šalát [7]. However, the argument of this note — which is a close relative of a proof of Euler's theorem published by Pinasco [6] — seems more natural.

At the conclusion of this note, we show how Theorem 1 can be used to estimate the proportion of positive integers represented by a given binary quadratic form.

2. Proof of Theorem 1

2.1. **A useful definition.** The proof runs a little more smoothly if we have at hand the notion of *density*. If $\mathscr{A}$ is a subset of the natural numbers, its (natural) *density* is defined as the limit

$$\lim_{x\to\infty} \frac{1}{x} \#\mathscr{A} \cap \{1, 2, 3, \dots, \lfloor x \rfloor\}. \tag{1}$$

This limit need not exist. Consider, for instance, the set $\mathscr{A}$ of integers with leading decimal digit 1. For $x \in [2 \cdot 10^{k-1}, 10^k - 1]$, the counting function of $\mathscr{A}$ is constant:

$$\#\mathscr{A} \cap [1, x] = 1 + 10 + \cdots + 10^{k-1} = \frac{10^k - 1}{9}.$$

Thinking of k as large, we see that as x ranges from $2 \cdot 10^{k-1}$ to $10^k - 1$, the ratio $\frac{1}{x}\#\mathscr{A} \cap [1, x]$ transitions from $\approx 5/9$ to $1/9$. Thus, the limit in (1) is not defined. However, if in (1) we replace the limit with the lim inf or lim sup, then the corresponding quantities certainly do exist, and are known as the *lower* and *upper densities*, respectively. In our example, the lower density is $1/9$ and the upper density is $5/9$.

The most important special case for us is when $\mathscr{A}$ is a union of k distinct residue classes modulo a positive integer m. In that case, it is straightforward to prove that $\mathscr{A}$ has density k/m.

2.2. **Proof of Theorem 1.** Let $\mathscr{P}$ be the set of all primes p not dividing q for which $p \bmod q \notin H$. The idea of the proof is to study, by two different methods, the density of natural numbers n for which we have simultaneously

(i) $n \bmod q \in (\mathbf{Z}/q\mathbf{Z})^\times \setminus H$, *and*
(ii) n has no prime factors from $\mathscr{P}$.

Method 1. Since H is a subgroup of $(\mathbf{Z}/q\mathbf{Z})^\times$, any natural number coprime to q whose reduction mod q is missing from H must have a prime in its factorization whose reduction is also missing from H. In other words, any n satisfying (i) fails (ii). So the density in question is just the density of the empty set, which is 0.

Method 2. Now suppose for a contradiction that the reciprocal sum of the primes in $\mathscr{P}$ converges. We then show that the set of n satisfying (i) and (ii) has positive lower density, contradicting what we found above and proving Theorem 1.

Since $1 - t = \exp(-(t + \frac{t^2}{2} + \frac{t^3}{3} + \dots)) \geq \exp(-t/(1-t)) \geq \exp(-2t)$ for $0 \leq t \leq \frac{1}{2}$, we deduce that

$$\Delta := \prod_{p \in \mathscr{P}} \left(1 - \frac{1}{p}\right) \geq \exp\left(-2 \sum_{p \in \mathscr{P}} \frac{1}{p}\right) > 0.$$

Moreover, we can fix a large number z with the property that

$$\sum_{\substack{p > z \\ p \in \mathscr{P}}} \frac{1}{p} < \frac{\Delta}{q}.$$

We continue in two steps. First, we determine the density when (ii) is replaced by the weaker requirement (ii′) that n has no prime factors from $\mathscr{P}$ *not exceeding* z. Condition (i) places n in $\phi(q) - |H|$ residue classes mod q, while (ii′) places n in $\phi(P)$ residue classes modulo the number $P := \prod_{p \leq z,\ p \in \mathscr{P}} p$. Since P and q are relatively prime, the Chinese remainder theorem tells us that (i) and (ii′) together put n in one of $(\phi(q) - |H|)\phi(P)$ residue classes modulo qP, and so the density of these n is

$$\begin{aligned}\left(\frac{\phi(q) - |H|}{q}\right)\left(\frac{\phi(P)}{P}\right) &\geq \frac{1}{q}\frac{\phi(P)}{P} \\ &= \frac{1}{q} \prod_{\substack{p \leq z \\ p \in \mathscr{P}}} \left(1 - \frac{1}{p}\right) \geq \frac{\Delta}{q}.\end{aligned}$$

Second, we eliminate those n satisfying (ii′) but not (ii). Such n have a prime factor from $\mathscr{P}$ that exceeds z. For a given prime p, the number of multiples of p up to a generic height x is $\lfloor x/p \rfloor$. Hence, the number of $n \leq x$ possessing a prime factor from $\mathscr{P} \cap (z, \infty)$ does not exceed

$$\sum_{\substack{p > z \\ p \in \mathscr{P}}} \lfloor x/p \rfloor \leq x \sum_{\substack{p > z \\ p \in \mathscr{P}}} \frac{1}{p}.$$

Thus, the set of n satisfying (ii′) but not (ii) has upper density at most

$$\sum_{\substack{p > z \\ p \in \mathscr{P}}} \frac{1}{p} < \frac{\Delta}{q}.$$

Combining the results of the last two paragraphs, we find that the lower density of of n satisfying (i) and (ii) is indeed positive.

3. An application to quadratic forms

We quickly sketch an application of Theorem 1 to the theory of representations by binary quadratic forms. Given integers a, b, and c, let

$$F(x, y) = ax^2 + bxy + cy^2.$$

We say n is *represented* by F if there are integers x and y with $F(x, y) = n$, and we ask: *What proportion of the positive integers can be represented by F?*

The simplest nontrivial example is perhaps $a = c = 1$ and $b = 0$, where we are asking what proportion of the positive integers are sums of two squares.

Using Theorem 1, we give an elementary proof of the following result.

Corollary 1. *Let $F(x, y) = ax^2 + bxy + cy^2$ be a quadratic form with integer coefficients a, b, and c whose* discriminant *$D := b^2 - 4ac$ is either 0 or not a perfect square. The set of positive integers n that are representable by F has density zero.*

Remark. Alaca, Alaca, and Williams [1] show that a binary quadratic form with integer coefficients represents all elements from an infinite arithmetic progression of natural numbers if and only if its discriminant is a nonzero square. Corollary 1 is a strengthening of the "only if" half of that result. On the other hand, the (easier) "if" direction of their result shows that the conclusion of Corollary 1 fails if our hypothesis on D is violated.

Proof of Corollary 1. If $D = 0$, then $F(x, y) = R(Ax + By)^2$ for some integers R, A, and B. So all of the numbers represented by F are the product of R with a square. But only a density zero set of positive integers arise in that way. So we may assume that D is nonzero and not a square.

Using the identities $4aF(x, y) = (2ax + by)^2 - Dy^2$ and $4cF(x, y) = (2cy + bx)^2 - Dx^2$, we see that if $n = F(x, y)$ and p is a prime dividing n, then

$$(2ax + by)^2 \equiv Dy^2 \pmod{p} \quad \text{and} \quad (2cy + bx)^2 \equiv Dx^2 \pmod{p}.$$

If either x or y is invertible modulo p, these congruences allow us to deduce that D is a square modulo p (possibly $0 \bmod p$). On the other hand, if p divides both x and y, then $p^2 \mid F(x, y) = n$. Consequently, if n is a representable integer and p is a prime that shows up to precisely the first power in n, then D is a square modulo p.

According to the law of quadratic reciprocity, there is an index 2 subgroup H of $(\mathbf{Z}/4|D|\mathbf{Z})^\times$ with the property that for odd primes p,

$$D \text{ is a nonzero square modulo } p \Longleftrightarrow p \bmod 4|D| \in H.$$

(This formulation of quadratic reciprocity goes back to Euler; see [3, Chapter 1], especially Corollary 1.19, for a discussion.) Let $\mathscr{P}$ be the set of odd primes not dividing D for which $p \bmod 4|D| \notin H$. If n is representable by F, then every prime from $\mathscr{P}$ that divides n has to occur to at least the second power in the prime factorization of n.

It follows that each representable n avoids the $p - 1$ residue classes p, $2p$, $3p$, $\dots$, $(p - 1)p \bmod p^2$ for all primes $p \in \mathscr{P}$. The density of n that avoid these residue classes for all $p \in \mathscr{P}$ up to a finite height z is, by an argument similar to that occurring in the proof of Theorem 1, precisely

$$\prod_{\substack{p \le z \\ p \in \mathscr{P}}} \left(1 - \frac{p-1}{p^2}\right).$$

Since $1 - t \le \exp(-t)$ and $\frac{p-1}{p^2} \ge \frac{1}{2p}$, the product is bounded above by

$$\exp\left(-\frac{1}{2} \sum_{\substack{p \le z \\ p \in \mathscr{P}}} \frac{1}{p}\right).$$

As $z \to \infty$, Theorem 1 shows that this final expression tends to zero. $\square$

Remark. In the doctoral thesis of Paul Bernays [2], it is shown if F satisfies the hypotheses of Corollary 1 with $D \neq 0$, then the number of positive integers $n \leq x$ representable by F is asymptotic to $c_F \cdot x/\sqrt{\log x}$ as $x \to \infty$. Here c_F is a positive constant depending on a, b, and c. The special case when $a = c = 1$ and $b = 0$ had been treated by Bernays' advisor, Edmund Landau [4]. Both of these results lie much deeper than our Corollary 1.

Acknowledgments

The author would like to thank Andrew Granville, from whom he first learned about Theorem A. He is also grateful to Pete L. Clark, Mitsuo Kobayashi, and Enrique Treviño for helpful conversations. Finally, he thanks the referee for suggestions that led to improvements in the exposition.

References

1. A. Alaca, Ş. Alaca, and K. S. Williams, *Arithmetic progressions and binary quadratic forms*, Amer. Math. Monthly **115** (2008), 252–254.
2. P. Bernays, *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht-quadratischen Diskriminante*, Ph.D. thesis, Georg-August-Universität Göttingen, 1912.
3. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989.
4. E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindeszahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. **13** (1908), 305–312.
5. D. A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York, 1977.
6. J. P. Pinasco, *New proofs of Euclid's and Euler's theorems*, Amer. Math. Monthly **116** (2009), 172–174.
7. T. Šalat, *An elementary proof of divergence of certain infinite series of the type $\sum 1/p$*, Friendship of Brotherly Universities (Bratislava, Brno, Debrecen, Cracow, Kiev) (Russian), Izdat. Kiev. Univ., Kiev, 1966, pp. 191–198.

Department of Mathematics, University of Georgia, Boyd Graduate Studies Research Center, Athens, Georgia 30602, USA

E-mail address: pollack@uga.edu