COLLOQUIUM MATHEMATICUM

VOL. 147 2017 NO. 2

A SIMPLE PROOF OF A THEOREM OF HAJDU–JARDEN–NARKIEWICZ

BY

PAUL POLLACK (Athens, GA)

Abstract. Let K be an algebraic number field, and let G be a finitely generated subgroup of $K^\times$. We give a short proof that for every positive integer n, there is an element of $\mathcal{O}_K$ not expressible as a sum of n elements of G.

1. Introduction. Let K be an algebraic number field. The following theorem was proved by Jarden and Narkiewicz [6] when $G = U(\mathcal{O}_K)$ and by Hajdu [5] in general.

THEOREM 1.1. *Let K be a number field. Let G be a finitely generated subgroup of $K^\times$. For each positive integer t, there is an $\alpha \in \mathcal{O}_K$ not expressible as a sum of t elements of G.*

The proofs in [5] and [6] depend crucially on the modern theory of S-unit equations. It is the purpose of this note to outline an entirely different, very short, and seemingly more elementary proof of Theorem 1.1.

We let $\lambda(n)$ denote *Carmichael's function*, defined as the exponent of the group $U(\mathbb{Z}/n\mathbb{Z})$. The following lemma—which seems possibly of some independent interest—is the key ingredient in our proof of Theorem 1.1.

LEMMA 1.2. *Let $\mathcal{P}$ be a set of primes of positive upper (relative) density. For each $\kappa > 0$, there are infinitely many squarefree natural numbers n which are divisible only by primes in $\mathcal{P}$ and which satisfy $\lambda(n) < n^\kappa$.*

If we do not restrict the prime factors of n, then $\lambda(n)$ is occasionally as small as $(\log n)^{O(\log\log\log n)}$, as shown by Erdős–Pomerance–Schmutz [4]. That estimate has been applied in a context similar to the present one by several authors (beginning in work of Ádám, Hajdu, and Luca [1]), but only when $K = \mathbb{Q}$. The upper bound of Lemma 1.2 on the values of $\lambda(n)$ is weaker than that of [4], but the ability to restrict the support of n facilitates applications to arbitrary number fields.

2010 *Mathematics Subject Classification*: Primary 11R27; Secondary 11N56.
Key words and phrases: S-unit, sum of units, Carmichael's function.
Received 8 August 2016; revised 13 September 2016.
Published online 9 January 2017.

DOI: 10.4064/cm7054-9-2016

Without further ado, we show how to deduce Theorem 1.1 from Lemma 1.2.

Proof of Theorem 1.1. Suppose that $\eta_1, \ldots, \eta_m$ generate G. Let $\mathcal{P}$ be the set of rational primes that split completely in K and are not below any prime ideal appearing in the factorizations of the η_i. Then $\mathcal{P}$ has positive upper density; in fact, by Landau's prime ideal theorem [7] applied to the Galois closure L (say) of $K/\mathbb{Q}$, the density of $\mathcal{P}$ is $1/[L:\mathbb{Q}]$. So by Lemma 1.2, there are infinitely many squarefree n composed of primes from $\mathcal{P}$ that satisfy $\lambda(n) < n^{1/(mt)}$. Since n is a squarefree product of split completely primes, $\mathcal{O}_K/n\mathcal{O}_K \cong (\mathbb{Z}/n\mathbb{Z})^{[K:\mathbb{Q}]}$, and so the group $U(\mathcal{O}_K/n\mathcal{O}_K)$ has exponent $\lambda(n)$. By the choice of $\mathcal{P}$, it is sensible to reduce the η_i modulo n, and hence (with the obvious notation)

$$\#G \bmod n\mathcal{O}_K \le \lambda(n)^m < n^{1/t}.$$

Hence, any sum of t elements of G falls into one of $< (n^{1/t})^t = n$ residue classes modulo $n\mathcal{O}_K$. But $\#\mathcal{O}_K/n\mathcal{O}_K = n^{[K:\mathbb{Q}]} \ge n$. So the set of elements of $\mathcal{O}_K$ that cannot be written as a sum of t elements of G includes an entire residue class modulo $n\mathcal{O}_K$, and in particular is nonempty. ∎

2. Proof of Lemma 1.2. This proof rests on the following simple consequence of Brun's sieve, first noticed by Erdős [3].

LEMMA 2.1. *Let $\delta > 0$. There is an $\epsilon > 0$ such that, for all $X > X_0(\delta, \epsilon)$,*

$$\#\{\textit{primes } p \le X : p-1 \textit{ has a prime factor} > X^{1-\epsilon}\} < \delta \frac{X}{\log X}.$$

Proof (*sketch*). In fact, if $\epsilon > 0$ is fixed, Erdős's arguments show that for all $X > X_0(\epsilon)$,

$$\#\{\text{primes } p \le X : p-1 \text{ has a prime factor} > X^{1-\epsilon}\} \le C\epsilon \frac{X}{\log X},$$

where C is an absolute constant. (See [3, p. 213]. A reference with notation more similar to that used here is [2, second display on p. 192].) So we may choose any $\epsilon < \delta/C$. ∎

Proof of Lemma 1.2. By assumption, there is a constant $\delta > 0$ and a sequence of X tending to infinity with $\#\{p \in \mathcal{P} : p \le X\} > \delta X/\log X$. If ϵ is fixed sufficiently small in terms of δ, then for all large enough X in our sequence,

$$\#\{p \in \mathcal{P} : p \le X, \text{ all prime factors } \ell \text{ of } p-1 \text{ are} \le X^{1-\epsilon}\} > \frac{\delta}{2} \frac{X}{\log X}.$$

For these X, we set

$$n = \prod_{\substack{p\in\mathcal{P}\cap[(\delta/8)X,X]\\ \ell|p-1\Rightarrow\ell\le X^{1-\epsilon}}} p.$$

Assuming X is large, the total number of primes up to $(\delta/8)X$ is smaller than $(\delta/4)X/\log X$, by the prime number theorem. Hence, the number of prime factors of n is at least $(\delta/4)X/\log X$, and

$$n \ge \left(\frac{\delta}{8}X\right)^{(\delta/4)X/\log X} > \exp\left(\frac{\delta}{8}X\right),$$

once X is large enough. We now turn attention to $\lambda(n)$. Since $\lambda(n) = \mathrm{lcm}_{p|n}[p-1]$, each prime power divisor of $\lambda(n)$ is smaller than X. Moreover, if ℓ divides $\lambda(n)$, then $\ell \le X^{1-\epsilon}$. Thus, there are (very crudely) no more than $X^{1-\epsilon}$ such primes ℓ. It follows that

$$\lambda(n) < X^{X^{1-\epsilon}} = \exp(X^{1-\epsilon}\log X).$$

Comparing this upper bound for $\lambda(n)$ with the displayed lower bound for n, it is clear that $\lambda(n) < n^{\kappa}$ once X is sufficiently large. (In fact, $\lambda(n) < \exp((\log n)^{1-\epsilon/2})$.) ∎

Acknowledgements. The author's research was partly supported by the National Science Foundation (NSF grant no. DMS-1402268).

REFERENCES

[1] Zs. Ádám, L. Hajdu, and F. Luca, *Representing integers as linear combinations of S-units*, Acta Arith. 138 (2009), 101–107.

[2] J.-M. De Koninck and F. Luca, *Analytic Number Theory*, Grad. Stud. Math. 134, Amer. Math. Soc., Providence, RI, 2012.

[3] P. Erdős, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function*, Quart. J. Math. 6 (1935), 205–213.

[4] P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function*, Acta Arith. 58 (1991), 363–385.

[5] L. Hajdu, *Arithmetic progressions in linear combinations of S-units*, Period. Math. Hungar. 54 (2007), 175–181.

[6] M. Jarden and W. Narkiewicz, *On sums of units*, Monatsh. Math. 150 (2007), 327–332.

[7] E. Landau, *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes*, Math. Ann. 56 (1903), 645–670.

Paul Pollack
Department of Mathematics
University of Georgia
Boyd Graduate Studies Research Center
Athens, GA 30602, U.S.A.
E-mail: pollack@uga.edu