# van der Waerden and the primes

**Levent Alpoge**

**Abstract.** In this note we prove the infinitude of the primes via an application of van der Waerden's theorem.

The purpose of this note is to present an amusing consequence of the tension between the additive regularity of the integers and their unique factorization into primes. Namely, it turns out the following theorem of van der Waerden implies the infinitude of the primes.

**Theorem 1 (van der Waerden, [1]).** *Suppose the positive integers are colored with finitely many colors. Then there are arbitrarily many arithmetic progressions containing integers all of the same color.*

More formally, let $f : \mathbb{Z}^+ \to S$ be any function to a finite set $S$. Then, for each $k > 0$, there are $n$ and $d$ for which

$$f(n) = f(n + d) = \cdots = f(n + kd).$$

What a beautiful theorem! Khinchin [**2**] called it one of the "pearls of number theory," and we can't help but agree. Now to the amusing consequence.

**Theorem 2.** *There are infinitely many primes.*

We will write $v_p(n)$ for the largest power of the prime $p$ dividing the positive integer $n$ — hence

$$n = \prod_p p^{v_p(n)}.$$

Notice that $v_p(ab) = v_p(a) + v_p(b)$, and

$$v_p(a + b) \geq \min\left(v_p(a), v_p(b)\right), \tag{1}$$

with equality if $v_p(a) \neq v_p(b)$.

*Proof.* Suppose there were finitely many. Color the positive integers by the list of primes dividing them and the parities of their exponents. So, if $P$ is the finite set of primes, define $f : \mathbb{Z}^+ \to (\{0, 1\} \times \{0, 1\})^P$ via

$$f(n) = \left( \begin{Bmatrix} 1 & p|n \\ 0 & p \nmid n \end{Bmatrix}, v_p(n) \bmod 2 \right)_p \quad \text{if } n = \prod_p p^{v_p(n)}.$$

This is a coloring of the integers with a finite set of colors, so it has arbitrarily long monochromatic arithmetic progressions. Let $r$ be larger than the square of any prime, and choose a monochromatic arithmetic progression $a, a + d, \ldots, a + dr$. Suppose $p$ divides $a$. Since all the integers in the progression have the same prime factors, $p$ divides $a + d$, and hence $p$ divides $d = (a + d) - a$.

**Claim.** $v_p(a) < v_p(d)$.

Indeed, if $v_p(a) > v_p(d)$, observe that

$$v_p(a + pd) = v_p(a + d) + 1 \not\equiv v_p(a + d) \bmod 2$$

by (1) (here $v_p(a + d) \leq v_p(a) - 2$ since $v_p(a + d) = v_p(d) < v_p(a)$ by (1), and both sides are of the same parity). If $v_p(a) = v_p(d)$ then

$$v_p(a + kd) = v_p(a) + 1 \not\equiv v_p(a) \pmod 2$$

for $k$ chosen so that $1 \leq k \leq p^2$ and $A + kD \equiv p \bmod p^2$, where $A$ and $D$ are the prime-to-$p$ parts of $a$ and $d$, respectively.

Therefore $v_p(a) < v_p(d)$ for every prime $p$ dividing $a$. So we see that $a$ and $a + d$ have all the same prime factors, and $v_p(a) = v_p(a + d)$ for each of them (again by (1)). This contradicts unique factorization if $d \geq 1$. ∎

REFERENCES

1. B. L. van der Waerden, Beweis einer Baudetschen Vermutung, *Nieuw Archief voor Wiskunde* **15** (1927) 212–216.
2. Ya. A. Khinchin, *Three Pearls of Number Theory*, Dover, Mineola NY, 1998.

**LEVENT ALPOGE** (alpoge@college.harvard.edu) is a senior at Harvard, from Dix Hills, New York.
*9 Tree Hollow Lane, Dix Hills NY, 11746*
*alpoge@college.harvard.edu*