

# VDW's Theorem Implies Primes Infinite

Exposition by William Gasarch

December 4, 2017

We present a proof by Levent Alpoge [?] that shows, from van Der Waerden's theorem, that the primes are infinite. We then compare this proof to other proofs quantitatively and speculate on what it means formalize the notion of proving  $A$  from  $B$

## 1 VDW implies Primes Infinite

We first state van Der Waerden's Theorem. A proof if it can be found in any Ramsey theory textbook.

**Notation 1.1** If  $n \in \mathbb{N}$  then  $[n]$  is the set  $\{1, \dots, n\}$ .

**Theorem 1.2** *For all  $k$ , for all  $c$ , there exists  $W = W(k, c)$  such that for all  $c$ -colorings  $COL : [W] \rightarrow [c]$  there exists  $a, d$  such that*

$$COL(a) = COL(a + d) = COL(a + 2d) = \dots = COL(a + (k - 1)d).$$

**Theorem 1.3** *There are an infinite number of primes.*

**Proof:** We give a procedure that will, given a finite set of primes  $P = \{p_1, \dots, p_m\}$ , produce a prime  $p \notin P$ . Let  $p_{\max}$  be the max element of  $P$ .

Let  $v_p(x)$  be the largest  $r$  such that  $p^r$  divides  $x$ .

We define a coloring  $COL$  of  $\mathbb{N}$  as follows: Color a number  $n$  by the vector  $(v_{p_1}(n) \pmod 2, v_{p_2}(n) \pmod 2, \dots, v_{p_m}(n) \pmod 2)$ . The number of colors is  $2^m$  which is finite. We determine  $k$  later. By van der Warden's theorem there exists  $a, d$  such that

$$COL(a) = COL(a + d) = COL(a + 2d) = \dots = COL(a + kd).$$

We can assume  $a \geq 2$ .

In the subcases below whenever we are considering a prime  $p$  we will let  $a = Lp^{a'}$ ,  $d = Mp^{d'}$  where  $p$  does not divide  $L$  or  $M$ . We will use that  $p$  does not divide  $L$  or  $M$  implicitly. Note that  $a' = v_p(a)$  and  $d' = v_p(d)$ .

**Case 1:** There exists  $p \in P$  such that  $a' \geq d' + 2$  (we use the formulation  $a' - d' - 1 \geq 1$ ). We show this cannot occur.

$$v_p(a + id) = v_p(Lp^{a'} + iMp^{d'}) = v_p(p^{d'}(Lp^{a'-d'} + iM)) = d' + v_p(Lp^{a'-d'} + iM)$$

$$i = 1: v_p(a + d) = d' + v_p(Lp^{a'-d'} + M) = d'.$$

$$i = p: v_p(a + pd) = d' + v_p(Lp^{a'-d'} + pM) = d' + 1 + v_p(Lp^{a'-d'-1} + M) = d' + 1.$$

Since  $v_p(a + d) \not\equiv v_p(a + pd) \pmod{2}$ ,  $COL(a + d) \neq COL(a + pd)$ , a contradiction. Since we use  $i = p$ , we will take  $k \geq p_{\max}$ .

**Case 2:** There exists  $p \in P$  such that  $a' = d' + 1$ . We show this cannot occur.

$$v_p(a + id) = v_p(Lp^{a'} + iMp^{d'}) = v_p(p^{d'}(Lp^{a'-d'} + iM)) = d' + v_p(Lp + iM).$$

$$i = 1: v_p(a + id) = d' + v_p(Lp + M) = d'$$

$i = px$  where  $1 \leq x \leq p - 1$  is such that  $L + Mx \not\equiv 0 \pmod{p}$ :

$$v_p(a + pxd) = d' + v_p(Lp + Mpx) = d' + 1 + v_p(L + Mx) = d' + 1.$$

Since  $v_p(a + d) \not\equiv v_p(a + pxd) \pmod{2}$ ,  $COL(a + d) \neq COL(a + pd)$ , a contradiction. Since we use  $i = px$  and  $1 \leq x \leq p - 1$ , we will take  $k \geq p_{\max}^2$ .

**Case 3:** There exists  $p \in P$  such that  $a' = d' = b$ . We show this cannot occur.

$$v_p(a + id) = v_p(Lp^b + iMp^b) = v_p(p^b(L + iM)) = b + v_p(L + iM).$$

If  $i = 0$  then we get  $v_p(a + id) = b + v_p(L) = b$ .

We want  $v_p(L + iM) = 1$ . We obtain this by finding  $i$  such that

$$\begin{aligned} L + iM &\equiv p \pmod{p^2} \\ iM &\equiv p - L \pmod{p^2} \end{aligned}$$

Let  $M^{-1}$  be the inverse of  $M \pmod{p^2}$ . Let  $i$  be such that  $0 \leq i \leq p^2 - 1$  and  $i \equiv M^{-1}(p - L) \pmod{p^2}$ . With this value of  $i$  note that  $L + iM = p + Np^2 = p(1 + Np)$  for some  $N$ .

$$v_p(a + id) = b + v_p(L + iM) = b + v_p(p(1 + Np)) = b + 1.$$

Since  $v_p(a) \not\equiv v_p(a + id) \pmod{2}$ ,  $COL(a) \neq COL(a + id)$ , a contradiction. Since  $0 \leq i \leq p^2$ , we will take  $k \geq p_{\max}^2$ .

**Case 4:** For all  $p \in P$   $a' \leq d' - 1$ .

For all  $p \in P$ :

$$v_p(a + d) = v_p(Lp^{a'} + Mp^{d'}) = v_p(p^{a'}(L + p^{d'-a'}M)) = a' = v_p(a).$$

Hence

$$a = Q_1 \prod_{p \in S} p^{v_p(a)}$$

$$a + d = Q_2 \prod_{p \in S} p^{v_p(a+d)} = Q_2 \prod_{p \in S} p^{v_p(a)}$$

where no  $p \in P$  divides  $Q_1$  or  $Q_2$ .

Since  $a < a + d$ ,  $Q_1 < Q_2$ . Hence  $Q_2 \geq 2$ . Let  $p'$  be a prime factor of  $Q_2$ .  $p' \notin P$  so we are done.

Looking over all of the cases it suffices to take  $k = p_{\max}^2$ . ■

## 2 Compare to Other Proofs

How does this proof compare to others? Let  $P$  be a finite set of primes. Let  $B(P)$  be such that there is a prime  $p \notin P$ , with  $p \leq B(P)$ . We look at the bounds obtained from different proofs that the primes are infinite. Our bounds are functions of  $|P|$  and the max element of  $P$  which we denote  $p_{\max}$ .

1. From Bertrand's Postulate, which is a theorem stating that for all primes  $p$  there is a prime between  $p + 1$  and  $2p$ ,  $B(P) \leq 2p_{\max}$ . Note that this proof is somewhat sophisticated.

2. From Euclid's proof of the infinitude of the primes one obtains  $B(P) \leq p_{\max}^{|P|}$ .
3. From the proof above one obtains  $B(P) \leq W(p_{\max}^2, 2^{|P|})$ .

### 3 What Does it Mean to Prove $A$ from $B$ ?

When I told a colleague the statement *you can prove that the primes are infinite from VDW's theorem* he proposed the following.

1. State VDW theorem.
2. Assume that there are a finite number of primes  $p_1, \dots, p_n$ .
3. Form  $A = 1 + \prod_{i=1}^n p_i$ .
4. If  $A$  is prime then since  $A \notin \{p_1, \dots, p_n\}$  we have a contradiction. If  $A$  is not prime then it has a prime factor  $q \notin \{p_1, \dots, p_n\}$  that

This proof is clearly not what we mean when we say we can prove primes infinite from VDW's theorem. Can we formalize what it means to REALLY be a proof of  $A \rightarrow B$  that uses the premise  $A$ ?

Let  $PI$  mean Primes Infinite. Let  $\mathcal{S}$  be a logical system. That is, axioms and rules of inference. If  $\mathcal{S}$  does not suffice to prove the primes are infinite, but  $\mathcal{S}$  does suffice to prove  $VDW \rightarrow PI$  then that would be a way to formalize that  $VDW$  was really used. This approach is similar to the reverse math program where they show that, say, a proof needed to use König's lemma.

Alternatively one could look at length-of-proofs. Let  $L(T)$  be the length of the proof of  $T$  in  $\mathcal{S}$ . Let  $P_n$  be the statement that there are at least  $n$  primes. If  $L(VDW \rightarrow P_n) \ll L(P_n)$  then that would be a way to formalize that  $VDW$  was really used. This approach is similar to proofs that, say, to prove certain propositional statements parameterized by  $n$  requires  $c^n$  steps.