VDW's Theorem Implies Primes Infinite (Another Proof)

Exposition by William Gasarch

March 12, 2018

Levent Alpoge [1] proved, using van Der Waerden's theorem, that the primes are infinite.

Andrew Granville [2] gave another such proof. We present it and then:

1. Show that there is a proof using more Ramsey Theory and less number theory.
2. Ask if one can get the result using even less number theory (and we are okay with using more number theory).

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 and several places online.

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

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

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

We use the notation $W(k,c)$ throughout without commentary.

We second state a theorem due to Fermat.

Theorem 1.3 *There can never be four squares in arithmetic progression.*

We note that this theorem is rather difficult to prove.

Theorem 1.4 *There are an infinite number of primes.*

Proof: Assume, by way of contradiction, that $P = \{p_1, \ldots, p_m\}$ is the set of all primes. Let $v_p(x)$ be the largest r such that p^r divides x.

We define a coloring COL of $W(4, 2^m)$ as follows:

$$COL(n) = (v_{p_1}(n) \bmod 2, \ldots, v_{p_m}(n) \bmod 2).$$

The number of colors is 2^m. By Theorem 1.2 there exists a, d such that

$$COL(a) = COL(a+d) = COL(a+2d) = COL(a+3d).$$

Let the color be $(b_1, \ldots, b_m)$ where $b_i \in \{0, 1\}$. Then all the numbers in $\{a, a+d, a+2d, a+3d\}$ are of the form $p_1^{c_1} \cdots p_k^{c_k}$ where $c_i \equiv b_i \pmod 2$. Multiply all of the numbers by $\Pi = p_1^{1-b_1} \cdots p_k^{1-b_k}$. Now we have that all elements of

$$\{a\Pi, (a+d)\Pi, (a+2d)\Pi, (a+3d)\Pi\}$$

are squares. Hence

$$a\Pi, (a+d)\Pi, (a+2d)\Pi, (a+3d)\Pi$$

is an arithmetic sequence of squares of length four. This contradicts Theorem 1.3. ∎

2 Can We Please Have Less Number Theory and More Ramsey Theory?

The proof of Theorem 1.3 is difficult so we would rather use an easier theorem from number theory. We only used VDW's theorem with $k = 4$. Consider the following theorem.

Theorem 2.1 *There exists some k such that there can never be k squares in arithmetic progression.*

In the proof of Theorem 1.4 we can use $W(k, 2^m)$ instead of $W(4, 2^m)$ to get a proof that there are infinitely many primes from Theorem 2.1. Hence if there is a proof of Theorem 2.1 that is easier than the proof of Theorem 1.3 then we will have a proof that the primes are infinite that uses slightly more Ramsey Theory but less number theory. Of more importance is that this would be an easier proof (at least to us).

We now state an even weaker theorem from Number theory that would suffice.

Theorem 2.2 *There exists some k, L such that there can never be k Lth powers in arithmetic progression.*

We leave it to the reader to prove that from Theorem 2.2 and Theorem 1.2 one can show the number of primes is infinite. Hence we now seek an easy proof of Theorem 2.2.

3 Can We Please Have Even Less Number Theory and Even More Ramsey Theory?

The following extension of VDW's theorem is known:

Theorem 3.1 *For all k, for all c, there exists $W = W(k, c)$ such that for all c-colorings $COL : [W] \to [c]$ there exists a, d such that*

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

The following theorem is even weaker than Theorem 2.2

Theorem 3.2 *There exists some k, L such that there can never be k Lth powers in arithmetic progression with difference an Lth power.*

We prove that there an infinite number of primes using Theorem 3.1 and Theorem 3.2.

Theorem 3.3 *The number of primes is infinite.*

Proof: Assume, by way of contradiction, that $P = \{p_1, \ldots, p_m\}$ is the set of all primes. Let $v_p(x)$ be the largest r such that p^r divides x.

We define a coloring COL of $W(k, 2^m)$ as follows:

$$COL(n) = (v_{p_1}(n) \bmod L, \ldots, v_{p_m}(n) \bmod L).$$

The number of colors is L^m. By Theorem 1.2 there exists a, d such that

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

Let the color be $(b_1, \ldots, b_m)$ where $b_i \in \{0, \ldots, L-1\}$. Then all the numbers in $\{a, a+d, \ldots, a+(k-1)d, d\}$ are of the form $p_1^{c_1} \cdots p_k^{c_k}$ where $c_i \equiv b_i \pmod{L}$. Multiply all of the numbers by $\Pi = p_1^{L-b_1} \cdots p_k^{L-b_k}$. Now we have that all elements of

$$\{a\Pi, (a+d)\Pi, \ldots, (a+(k-1)d)\Pi, d\Pi\}$$

are Lth power. Also note that the arithmetic sequence

$$a\Pi, (a+d)\Pi, \ldots, (a+(k-1)d)\Pi$$

consists of Lth powers, and the difference is $d\Pi$, also an Lth power. This contradicts Theorem 3.2. ∎

So, is there an easy proof of Theorem 3.2? This depends on what you call easy. However, the following theorem has a proof that we believe is easier than that of Theorem 1.3.

Theorem 3.4 *There cannot be tw 4th powers whose differences is a 4th power.*

Proof: If $a, a+d$, and d are fourth powers then let $a = x^4$, $a+d = z^4$, $d = y^4$. We then have $x^4 + y^4 = z^4$ which contradicts Fermat's last theorem for $n = 4$. ∎

References

[1] L. Alpoge. Van der waerden and the primes. *The American Mathematical Monthly*, 122:784–785, 2015. http://www.jstore.org/stable/10.4169/amer.math.monthly.122.8.784.

[2] A. Granville. Squares in arithmetic progression and infinitly many primes. *The American Mathematical Monthly*, 124:951–954, 2017.