

Unprovable Ramsey-type statements reformulated to talk about primes

Andrey Bovykin*

Abstract

Let us say that two finite sets of natural numbers are primality-isomorphic if there is a difference-preserving primality-preserving and nonprimality-preserving bijection between them. Let Φ be the statement “every infinite set $B \subseteq \mathbb{N}$ has an infinite subset A such that for any $x < y < z$ in A , the interval $\{\frac{x+y}{2}, \dots, \frac{3x+y}{2}\}$ is primality-isomorphic to the interval $\{\frac{x+z}{2}, \dots, \frac{3x+z}{2}\}$ ”. We prove in RCA_0 , that the Hardy-Littlewood k -tuple Conjecture implies that Φ is equivalent to the Regressive Ramsey Theorem for pairs, a statement that axiomatises ACA_0 , and so in particular implies all theorems of Peano Arithmetic.

Let Ψ be the statement “for every infinite set $B \subseteq \mathbb{N}$ there is an infinite $A \subseteq B$ such that for any $k < m < n$ in A , $p_m \equiv p_n \pmod{p_k}$ ”, where p_n is the n th prime. We show, using $I\Sigma_1$ -provability of an effective version of Dirichlet’s theorem on primes in arithmetical progressions, that Ψ is again equivalent to the Regressive Ramsey Theorem for pairs and thus implies all theorems of Peano Arithmetic.

Finally, for every $n \geq 1$, let $P(n)$ be the statement “for all $m > n$, there is N such that for every polynomial $p(x_1, x_2, \dots, x_n)$ with integer coefficients, there is a set $H \subseteq \{0, 1, 2, \dots, N-1\}$ of size at least m such that $|H| > \min H$ and the values of the polynomial p are prime on all n -element subsets of H or composite on all n -element subsets of H ”. For every $n \geq 2$, the statement $P(n)$ is equivalent to the Paris-Harrington Principle in dimension n , and hence is $I\Sigma_{n-1}$ -unprovable. In particular the statement “for all n , $P(n)$ holds” is equivalent to the Paris-Harrington Principle and hence is not provable in Peano Arithmetic.

In this note we show how to use prime constellations, residues modulo a prime number and primality and non-primality of polynomials in place of colours as in Ramsey theory, to formulate some simple and attractive strong (unprovable) statements about prime numbers. In all examples in this note, our strong statements are mere reformulations of the Regressive Ramsey theorem, the Kanamori-McAloon Principle and the Paris-Harrington Principle.

The background material on Unprovability Theory is in [2]. We use standard names for arithmetical theories of this part of the spectrum of arithmetical strength. The theory $I\Delta_0 + \text{exp}$, also denoted $I\Delta_0(\text{exp})$ (and its variation EA as well as the conservative second-order version EFA) is the theory where usual concrete mathematics (that does not use genuine infinitary methods and does not talk about functions that grow faster than finite towers of exponents) takes place. See [1] for a discussion of this theory and its strength. A stronger theory $I\Sigma_1$, the one-quantifier induction arithmetic (and its variations, including primitive recursive arithmetic PRA and the conservative second-order extension RCA_0) is often identified with the intuitive concept of “finitary reasoning” or “all possible elementary methods in mathematics” but is actually somewhat stronger than the informal perception of “elementary methods”. The theory $I\Sigma_2$, the two-quantifier induction arithmetic, is an extension of $I\Sigma_1$ and is believed to be able to incorporate the rest of concrete mathematical proofs of first-order arithmetical theorems from the past, including all “non-elementary methods”, such as theorems of

*the author was supported by the John Templeton Foundation

complex analysis etc. The theory PA, first-order Peano Arithmetic (and its second-order conservative version ACA_0) is very strong and is often identified with “finite” or “separable” mathematics, the last outpost of the finite before truly infinitary methods kick in. All definitions and discussion of these theories can be found in S. Simpson’s book [11], which is the standard reference.

The classical number-theoretic theorems and conjectures we mention in this note can be found in most introductory number theory textbooks. I was occasionally using the textbook [10]. Let me formulate the three important unsolved problems in number theory that will often be mentioned below.

A finite sequence of zeros, ones and stars is called a constellation. We say that a constellation is realised in \mathbb{N} if there is an order-preserving, difference-preserving function that maps zeros into composite numbers, ones into prime numbers and stars into any numbers. (By difference-preserving we mean that two symbols of a constellation whose locations differ by n are mapped into two numbers whose difference is n .) We say that a constellation is allowable if it satisfies the following straightforward condition: for every prime number p , the set of places where 1 occurs in our constellation does not cover all residues modulo p . The Hardy-Littlewood k -tuple Conjecture says that every allowable constellation is realised infinitely-often (and even gives the asymptotic number of occurrences of each constellation below x). Only two easy cases of the Hardy-Littlewood Conjecture are known to hold: the case of an arbitrarily long string of zeros and the case of an arbitrary string of zeros and a single one.

The Buniakovsky Conjecture [4] says that for every irreducible polynomial $p(x)$ with integer coefficients, if $p(x)$ does not have local obstruction (i.e., there is no prime number that divides $p(x)$ for all x) then $p(x)$ takes infinitely-many prime values.

Hypothesis H is the ultimate generalisation of the Buniakovsky Conjecture to finite collections of polynomials: for any finite collection of irreducible polynomials $p_1(x), p_2(x), \dots, p_n(x)$, if there is no prime number that divides $\prod_{i=1}^m p_i(x)$ for all x , then on some infinite set of arguments x , the polynomials $p_i(x)$ are simultaneously prime.

This note was written on the occasion of the 70th birthday of Grigori Mints.

1 Primality-isomorphic intervals of natural numbers

We say that two intervals of natural numbers are primality-isomorphic if there is an order-preserving, primality-preserving and nonprimality-preserving bijection between them. For an interval $[m, n]$, we define *isotype*($[m, n]$) as the sequence of zeros and ones of length $n - m + 1$ such that for every $i < n - m + 1$, the i th entry is 0 if $i + m$ is composite and 1 if $i + m$ is prime.

Theorem 1. Let Φ be the statement “every infinite set B has an infinite subset A such that for any $x < y < z$ in A , the interval $\{\frac{x+y}{2}, \dots, \frac{3x+y}{2}\}$ is primality-isomorphic to the interval $\{\frac{x+z}{2}, \dots, \frac{3x+z}{2}\}$ ”. Then RCA_0 proves that, assuming the Hardy-Littlewood conjecture, Φ is equivalent to the Regressive Ramsey Theorem for pairs, thus implying all theorems of PA.

For every set X , $[X]^n$ denotes the set of all n -element subsets of X . We define a function f of n arguments $x_1 < x_2 < \dots < x_n$ to be regressive if $f(x_1, x_2, \dots, x_n) \leq x_1$ and 2^x -regressive if $f(x_1, x_2, \dots, x_n) \leq 2^{x_1}$. We say that a set H is f -min-homogeneous if for all $x_1 < x_2 < \dots < x_n$ and $x_1 < y_2 < \dots < y_n$ in H , $f(x_1, x_2, \dots, x_n) = f(x_1, y_2, \dots, y_n)$. RegRT^2 is the statement “for every regressive $f: [\mathbb{N}]^2 \rightarrow \mathbb{N}$, there exists an infinite f -min-homogeneous set”. $\text{RegRT}^2(2^x)$ is the statement “for every 2^x -regressive $f: [\mathbb{N}]^2 \rightarrow \mathbb{N}$, there exists an infinite f -min-homogeneous set”. It is known that RegRT^2 is equivalent to the infinite Ramsey Theorem for triples and two colours RT_2^3 (“for any infinite set $B \subseteq \mathbb{N}$ and any function $f: [B]^3 \rightarrow 2$, there exists an infinite set such that f is constant on its 3-element subsets”). It is also known that RT_2^3 axiomatises ACA_0 , and thus implies all theorems of Peano Arithmetic [11].

Let us first show that Φ follows from $\text{RegRT}^2(2^x)$. Consider any infinite set B and a colouring $iso: [B]^2 \rightarrow \mathbb{N}$ defined as follows: $iso(x, y) = isotype(\{\frac{x+y}{2}, \dots, \frac{3x+y}{2}\})$. Since there are fewer than 2^x possible isomorphism types, the function is 2^x -regressive. A min-homogeneous infinite subset of B is as needed.

We used a seemingly stronger version of $\text{RegRT}^2(2^x)$ by applying the principle to an arbitrary set B , not

to \mathbb{N} , which could theoretically turn out to be strictly stronger, for example false. Let us show that it is still equivalent to RT_2^3 . Consider any colouring $f: [B]^2 \rightarrow \mathbb{N}$ with $f(x, y) \leq 2^x$. Put

$$g(x, y, z) = \begin{cases} 0 & \text{if } f(x, y) = f(x, z) \\ 1 & \text{otherwise} \end{cases}$$

Using RT_2^3 , choose an infinite homogeneous set and notice that the colour is 0, so we are done.

Before we go into the proof of Theorem 1, we need the following lemma.

Lemma 2. Given numbers n and r and an allowable constellation C there is a number s such that there are at least n allowable constellations of the form

$$C \underbrace{*****}_r I$$

where each I is a string of zeros and ones of length s .

The lemma is provable in $I\Delta_0 + \text{exp}$.

Proof. (Proof of Lemma 2.) Let ℓ be the length of the sequence C . For every prime number $p_i \leq \ell + 2$, fix some residue a_i modulo p_i that occurs in C and define the sets

$$P_i = \{m \mid m \geq \ell + r \text{ and } m = k \cdot p_i + a_i \text{ for some } k \in \mathbb{N}\}.$$

By well-known properties of residues, the set $\bigcap_{p_i \leq \ell + 2} P_i$ is infinite (and recurring with period $\prod_{p_i \leq \ell + 2} p_i$). Set

$$b_1 = \min_{p_i \leq \ell + 2} P_i.$$

Clearly, for all primes $p_i \leq \ell + 2$, b_1 realises only existing residues modulo p_i and for every prime $p > \ell + 2$, b_1 does not complete the set of all residues modulo p (since we left two spare places when wrote $\ell + 2$).

Do the same process to define b_i for all $i \leq n$. Suppose the number b_i has been built. For every $p_i \leq b_{n-1} + 2$, fix a residue a_i occurring so far in C or as b_k for some $k = 1, 2, \dots, i - 1$ and define again

$$P_i = \{m \mid m > b_{n-1}, m = k \cdot p_i + a_i \text{ for some } k \in \omega\}.$$

Set $b_i = \min_{p_i \leq b_{i-1} + 2} P_i$ and define

$$C' = C \underbrace{*****}_r 000 \dots 0 \underline{1}_{b_1} 0 \dots 00 \underline{1}_{b_n},$$

where new ones stand in the places b_1, b_2, \dots, b_n and the rest are zeros. Notice that C' is an allowable constellation, and so is any constellation obtained from C' by substituting some of b_i 's ones by zeros. Therefore we have built 2^n -many allowable constellations that continue C . The number $s = b_n - r - \ell$ can be estimated, since at each stage there is a rough exponential bound $b_i \leq b_{i-1} + \prod_{p_i \leq b_{i-1} + 2} p_i$, so the construction can be conducted within $I\Delta_0 + \text{exp}$. \square

Now let us prove Theorem 1.

Proof. (Proof of Theorem 1). Consider an arbitrary regressive colouring $g: [\mathbb{N}]^2 \rightarrow \mathbb{N}$ and build a set $B_g \subseteq \mathbb{N}$ with its n th element denoted by b_n such that for any $n < m < k$ in \mathbb{N} , if $\text{iso}(b_n, b_m) = \text{iso}(b_n, b_k)$ then $g(n, m) = g(n, k)$, so the application of Φ to B_g will pick out the desired min-homogeneous set for g .

Let us define a sequence of points $\langle b_n \mid n = 0, 1, 2, \dots \rangle$ and a certain auxiliary tree T . Set b_0 to be arbitrary and fix an allowable interval constellation I_0 on $[0, b_0]$. Let the root of T be I_0 .

Define the point b_1 as follows. Apply the Hardy-Littlewood Conjecture to I_0 to find (using Lemma 2) the first realisation $[a, a + b_0]$ such that, defining $b_1 = 2a - b_0$, we have: there are at least two allowable constellations of the form

$$I_0 \underbrace{*****}_c I,$$

where I is of length $b_1 + 1$ and $c_0 = \frac{b_1 - 3b_0}{2}$.

Consider the set

$$[0, b_0] \underbrace{*****}_c \left[\frac{b_1 - b_0}{2}, \frac{3b_1 - b_0}{2} \right]$$

and fix two allowable constellations on this set: $I_0 ***** I_{00}$ and $I_0 ***** I_{01}$. These two constellations form the second level in T , and are the two immediate successors of the root I_0 .

Let us find a point b_2 such that

1. $b_2 > 17b_1$;
2. $iso(b_0, b_2) = I_0$, $iso(b_1, b_2) = I_{0,g(1,2)}$;
3. both I_{00} and I_{01} have three different (and different from each others') continuations, i.e. there are three constellations of the form

$$I_0 \underbrace{*****}_c I_{00} \underbrace{*****}_c I$$

and another three allowable constellations of the form

$$I_0 \underbrace{*****}_c I_{01} \underbrace{*****}_c I,$$

where I is of length $b_2 + 1$ and $c_1 = \frac{b_2 - 3b_1}{2}$.

The three continuations of $I_0 ***** I_{00}$ will be called I_{000} , I_{001} and I_{002} and the three continuations of $I_0 ***** I_{01}$ will be called I_{010} , I_{011} and I_{012} . It is important that we chose b_2 so that all these six constellations of length $b_2 + 1$ are different.

Now the general case. Suppose b_0, b_1, \dots, b_{n-1} have been defined, as well as the first $(n - 1)$ levels of the tree T .

Find a point b_n such that

1. $b_n > 17b_{n-1}$;
2. $iso(b_0, b_n) = I_0$;
 $iso(b_1, b_n) = I_{0,g(1,n)}$;
 $iso(b_2, b_n) = I_{0,g(1,n),g(2,n)}$;
 \vdots
 $iso(b_{n-1}, b_n) = I_{0,g(1,n),\dots,g(n-1,n)}$;
3. for every branch in T_{n-1} , i.e. for every constellation of the form

$$C = I_0 \underbrace{*****}_c I_{0k_1} \underbrace{*****}_c I_{0k_1 k_2} * \dots * I_{0k_1 k_2 \dots k_{n-1}},$$

where $k_i \in \{0, 1, \dots, i\}$, there are $(n + 1)$ different allowable continuations of the form

$$C \underbrace{*****}_c I,$$

where I is of length $b_n + 1$ and $c_{n-1} = \frac{b_n - 3b_{n-1}}{2}$.

Define B to be the set of all b_n for $n \in \mathbb{N}$. (Notice that it is well possible that $g(n, m) = g(n, k)$ but $iso(b_n, b_m) \neq iso(b_n, b_k)$ but it does not concern us since we are only interested in the inverse of this relation.)

Now, apply Φ to B and extract the set A as in Φ . Now notice that the set

$$\{m \in \mathbb{N} \mid b_m \in A\}$$

is min-homogeneous for g . □

There is another way to think about the proof of the strength of Φ , namely in terms of choosing an infinite branch through our tree T (which we eventually do when we extract A). So we could think not in terms of $\Phi \leftrightarrow \text{RegRT}^2$ but in terms of equivalence with full König's Lemma (which is equivalent to ACA_0) [7].

Let φ_2 be the statement "for all m , there is N such that for any set $a_1 < a_2 < \dots < a_N$, there is $H \subseteq \mathbb{N}$ such that whenever $i < j < k$ and are in H then the sets $iso(a_i, a_j)$ and $iso(a_i, a_k)$ are primality-isomorphic".

Corollary 3. $I\Sigma_1$ proves that the Hardy-Littlewood conjecture implies $\varphi_2 \rightarrow \text{KM}^2$. Thus φ_2 and the Hardy-Littlewood conjecture cannot be both provable in $I\Sigma_1$.

Proof. The proof is identical to the proof of Theorem 1 above. □

It is now possible to formulate some other related unprovable statements about polynomials and primes if instead of the Hardy-Littlewood k -tuple Conjecture we use the Bunyakovsky Conjecture or Hypothesis H. Since each of those unprovable statements uses exactly the same idea (realisation of constellations corresponding to colours) and a very similar proof, we shall stop here now.

Also, it is possible to generalise the statement φ_2 to the statement φ_n , equivalent to KM^n , using the function $iso(x_1, \frac{x_2+x_3+\dots+x_n}{n-1})$.

2 Basic congruences and Dirichlet's theorem

Let p_n be the n th prime. Consider the statement Ψ : "for every infinite set $B \subseteq \mathbb{N}$, there is an infinite subset $A \subseteq B$ such that for any $k < m < n$ in A , $p_m \equiv p_n \pmod{p_k}$ ".

Theorem 4. RCA_0 proves that Ψ is equivalent to RegRT^2 , and hence implies all of ACA_0 .

Proof. $\text{RegRT}^2 \rightarrow \Psi$ is easy. Set $f: [B]^2 \rightarrow \mathbb{N}$ to be defined as follows: $f(x, y)$ is the residue of p_y modulo p_x . Clearly f is x^2 -regressive (and even $x \ln x$ -regressive), so choose an infinite f -min-homogeneous set A and notice that this set is as needed in Ψ .

$\Psi \rightarrow \text{RegRT}^2$. Given a regressive colouring $g: [\mathbb{N} \setminus \{0\}]^2 \rightarrow \mathbb{N} \setminus \{0\}$, build a set $B_g \subseteq \mathbb{N}$ consisting of primes such that for any $m < n$ in \mathbb{N} ,

$$b_m \pmod{b_n} = g(m, n).$$

Set $b_1 = 2, b_2 = 3$. Clearly, $g(1, n) = 1$ for all $n > 1$, so for all prime numbers p , we have $p \pmod{b_1} = g(1, n)$ for all $n \in \mathbb{N}$. Suppose for $n \geq 2$ we have chosen prime numbers b_1, b_2, \dots, b_n . Find a number $a \in \{1, 2, \dots, b_1 b_2 \dots b_n - 1\}$ such that

$$a \pmod{b_1} = g(1, n+1) = 1$$

$$a \pmod{b_2} = g(2, n+1)$$

$$\vdots$$

$$a \pmod{b_n} = g(n, n+1).$$

This number exists because all b_i are prime. Notice also that since $g(i, j) \neq 0$, a is not divisible by any b_i . Now, every member of the arithmetic progression

$$b_1 b_2 \dots b_n \cdot k + a$$

satisfies the same set of congruences modulo b_i ($i = 1, 2, \dots, n$) as a , so, we can use Dirichlet's theorem and set b_{n+1} to the first prime member of this arithmetic progression for some $k \geq 1$.

$I\Sigma_1$ -provability of Dirichlet's theorem can be found in Cegielski [5]. See also discussion and some of the history of the question in Avigad [1]¹.

Therefore our proof of the equivalence $\Psi \leftrightarrow \text{RegRT}^2$ is clearly being conducted in RCA_0 .

Define $B_g = \{n \in \mathbb{N} \mid p_n \in B\}$. Apply Ψ to B_g to get a subset $A \subseteq B_g$ such that for $k < m < n$ in A , $p_m \equiv p_n \pmod{p_k}$. Notice that A is the g -min-homogeneous set we were looking for. \square

Corollary 5. The statement ψ_2 defined as “for all n there is N such that for every set B of size N , there is a subset $A \subseteq B$ of size n such that for all $m < k < \ell$ in A , $p_k \equiv p_\ell \pmod{p_m}$ ” is not provable in $I\Sigma_1$.

Proof. The proof repeats the proof of Theorem 4 above. \square

It is possible to transform ψ_2 into an equivalent statement in Π_2^0 form by substituting the quantifier “for every finite set B of size N ” by a bounded quantifier with an explicit upper bound $f(N)$ such that the set $\{b_1, b_2, \dots, b_N\}$ is stated to be chosen from $\{0, 1, \dots, f(N)\}$.

As with many strong Π_2^1 statements, both Φ and Ψ can be approximated by their “densities” in the sense of J. Paris. The resulting first-order statements are equivalent to 1-consistency of PA (and thus are much stronger than φ_2 or ψ_2) and talk in a certain iterative way about prime numbers. But those statements no longer look particularly interesting, so we omit them here. Another way to gain more strength than ψ_2 , but still end up with interesting assertions (while staying in the language of first-order arithmetic) is to imitate KM^n in the same way as in the proof of Theorem 4, by multiple applications of Dirichlet's theorem. This is quite straightforward and we also omit it.

3 Primality and non-primality of polynomials

Theorem 6. For every $n \geq 1$, let $P(n)$ be the statement “for all $m > n$, there is N such that for every polynomial $p(x_1, x_2, \dots, x_n)$ with integer coefficients, there is $H \subseteq \{0, 1, 2, \dots, N - 1\}$ of size at least m such that $|H| > \min H$ and p is prime on all n -element subsets of H or composite on all n -element subsets of H ”.

For every $n \geq 2$, the statement $P(n)$ is equivalent to PH_2^n , and hence is $I\Sigma_{n-1}$ -unprovable. In particular the statement “for all n , $P(n)$ holds” is equivalent to PH and thus is not provable in Peano Arithmetic.

Notice that since there are polynomials all of whose positive values are prime [8] and polynomials all of whose positive values are composite, it is important to mention both “primality” and “non-primality” cases here, to stay consistent.

We routinely think of each polynomial as a cut-off function from \mathbb{N} to \mathbb{N} , setting $p(x_1, x_2, \dots, x_n) = 0$ if the value turns out to be negative. Let us also mention what we mean by “primality on a set H ”. We mean that for all $x_1 < x_2 < \dots < x_n$ in H , the number $p(x_1, x_2, \dots, x_n)$ is prime. Similarly for “being composite on a set H ”.

Proof. It is clear that for every n , PH_2^n implies $P(n)$ and that PH₂ implies “for all n , $P(n)$ holds”. So let us now prove the opposite direction.

Consider an arbitrary m and find the number N as provided by the principle $P(n)$ for m . Consider an arbitrary colouring $f: [N]^n \rightarrow 2$. Let us build a polynomial $p_f(x_1, \dots, x_n)$ with integer coefficients such that for all $x_1 < x_2 < \dots < x_n < N$,

$$p_f(x_1, x_2, \dots, x_n) \text{ is prime} \iff f(x_1, x_2, \dots, x_n) = 1.$$

This is not difficult because we have finitely-many such functions f but an infinite supply of various polynomials we can use to imitate f by their primality or non-primality.

¹A related question concerns provability of the Prime Number Theorem. $I\Sigma_1$ -provability of the Prime Number Theorem, was done by Grigori Mints already in 1975, see [9]. (A $I\Delta_0(\text{exp})$ -provability proof can also be found in [6].)

First let us define for every $k_1 < k_2 < \dots < k_n$, an auxiliary polynomial

$$g_{k_1 k_2 \dots k_n}(x_1, x_2, \dots, x_n) = \prod_{i_1 < N, i_1 \neq k_1} (x_1 - i_1) \cdot \prod_{i_2 < N, i_2 \neq k_2} (x_2 - i_2) \cdot \dots \cdot \prod_{i_n < N, i_n \neq k_n} (x_n - i_n).$$

Clearly, for $x_1 = k_1, \dots, x_n = k_n$, $g_{k_1 k_2 \dots k_n}(x_1, x_2, \dots, x_n) \neq 0$, but for all other arguments $x_1, \dots, x_n < N$, $g_{k_1 k_2 \dots k_n}(x_1, x_2, \dots, x_n) = 0$.

Now consider C_N^n -many infinite sequences:

$$1 + i \cdot g_{k_1 k_2 \dots k_n}(k_1, k_2, \dots, k_n)$$

that is, one sequence for each n -element subset $k_1 < k_2 < \dots < k_n$ of $\{0, 1, 2, \dots, N - 1\}$.

Each of these sequences has infinitely-many composite values and, by Dirichlet's theorem, infinitely-many prime values, and we have a primitive recursive bound on when the first composite value and the first prime value is guaranteed.

For each $k_1 < k_2 < \dots < k_n < N$, find and fix the natural number $M_{k_1 k_2 \dots k_n}$ such that:

- if $f(k_1, k_2, \dots, k_n) = 0$ then $1 + M_{k_1 k_2 \dots k_n} \cdot g_{k_1 k_2 \dots k_n}(k_1, k_2, \dots, k_n)$ is composite;
- if $f(k_1, k_2, \dots, k_n) = 1$ then $1 + M_{k_1 k_2 \dots k_n} \cdot g_{k_1 k_2 \dots k_n}(k_1, k_2, \dots, k_n)$ is prime.

Now, set

$$p_f(x_1, x_2, \dots, x_n) = 1 + \sum_{k_1 < k_2 < \dots < k_n < N} M_{k_1 k_2 \dots k_n} \cdot g_{k_1 k_2 \dots k_n}(x_1, x_2, \dots, x_n).$$

Clearly, this polynomial is as needed.

Hence the set $H \subseteq \{0, 1, 2, \dots, N - 1\}$ of constant primality or non-primality for p_f is the homogeneous set for f needed in the Paris-Harrington Principle, so $P(n)$ implies PH_2^n . The proof of this implication has been carried out in $I\Sigma_1$ because the explicit bounds in Dirichlet's theorem are proved in $I\Sigma_1$. \square

At this moment we may want to formulate the following statement A (an easy consequence of the Infinite Ramsey Theorem): “for every polynomial p of several variables, there is an infinite set H on which primality or non-primality of p is constant”. It would be tempting to try a compactness argument to show that A implies “for all n , $P(n)$ holds” thus implying PH. However, it does not work (the infinite branch is not defined by a polynomial). There is more to say about this statement and several other interesting statements concerning prime values of polynomials. This is work in progress and will appear in due course in [3].

Although all unprovability proofs in this note are very simple, the main ideas (constellations of primes, residues modulo a prime and primality or non-primality as colours) appear as ingredients inside more serious arguments in the big project [3]. We extracted and isolated the unprovable statements Φ , φ_2 , Ψ and $\forall n P(n)$ of the current paper since they are simple, compact and might have some independent interest.

References

- [1] Avigad, J. (2003). Number theory and elementary arithmetic. *Philosophia Mathematica* (3), vol. 11, pp. 257 – 284.
- [2] Bovykin, A. (2008). Brief introduction to unprovability. *Logic Colloquium 2006*. Lecture Notes in Logic, pp. 38 – 64.
- [3] Bovykin, A. (2009). Unprovable statements about prime values of polynomials. Preprint. Work in progress.
- [4] Buniakovsky V. (1857). Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs. *Memoirs of St. Petersburg Academy of Sciences.*, **6**, pp. 305-329.

- [5] Cegielski, P. (1992). Le théorème de Dirichlet est finitiste. Technical Report 92.40. Laboratoire Informatique Théorique et Programmation. Institut Blaise Pascal, Paris.
- [6] Cornaros, C., Dimitracopoulos, C. (1994). The prime number theorem and fragments of PA, *Archive for mathematical logic*, 33, pp. 265 – 281.
- [7] Clote, P., McAloon, K. (1983). Two further combinatorial theorems equivalent to the 1-consistency of Peano Arithmetic. *Journal of Symbolic Logic*, 48, pp. 1090-1104.
- [8] Matiyasevich, Yu. (1992). Hilbert’s tenth problem. MIT Press.
- [9] Mints, G. (1976). What can be done in PRA. *Zapiski nauchnykh seminarov LOMI*, vol. 60, pp. 93 – 102.
- [10] Pollack, P. (2004). Not Always Buried Deep. Selections from analytic and combinatorial number theory. Book manuscript. Available online.
- [11] Simpson, S. (2009). Subsystems of Second-Order Arithmetic. Second Edition. Association for Symbolic Logic.

SCHOOL OF MATHEMATICS
UNIVERSITY OF BRISTOL
ENGLAND, BS8 1TW

`andrey.bovykin@bristol.ac.uk`