# Exponential Diophantine Definition of the Set of Primes

**Theorem.** The set $\{< m, n, k > | \; m = \binom{n}{k}\}$ is exponential Diophantine.

Proof. Let $u = 2^n + 1 > 2^n \geq \binom{n}{k}$. Then the numbers $\binom{n}{k}$ are just the "digits" in the base u representation of $(u+1)^n$ :

$$(u+1)^n = \sum_{k=0}^{n} \binom{n}{k} u^k.$$

Therefore, $m = \binom{n}{k}$ if and only if the following system of exponential Diophantine equations has a solution:

$$\begin{aligned} u &= 2^n + 1 \\ (u+1)^n &= wu^{k+1} + mu^k + v \\ v + z + 1 &= u^k \\ m + t + 1 &= u. \end{aligned}$$

Note that the last pair of equations really express the inequalities $v < u^k$ and $m < u$, respectively. Since inequalities can always be reduced to equations in this manner (by increasing the number of unknowns), we can freely use inequalities in Diophantine and exponential Diophantine definitions. $\square$

**Lemma 1.** If $r > 2n$, then

$$\frac{1}{(1-\frac{n}{r})^n} < 1 + \frac{2n}{r} \cdot 2^n.$$

Proof.

$$\begin{aligned}
\frac{1}{1-\frac{n}{r}} &= 1 + \frac{n}{r} + \left(\frac{n}{r}\right)^2 + \cdots \\
&= 1 + \frac{n}{r}\left\{1 + \frac{n}{r} + \left(\frac{n}{r}\right)^2 + \cdots\right\} \\
&< 1 + \frac{n}{r}\left\{1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \cdots\right\} \\
&= 1 + \frac{2n}{r}
\end{aligned}$$

Hence

$$\begin{aligned}
\frac{1}{(1-\frac{n}{r})^n} &< \left(1 + \frac{2n}{r}\right)^n \\
&= \sum_{j=0}^{n} \binom{n}{j} \left(\frac{2n}{r}\right)^j \\
&\leq 1 + \frac{2n}{r} \sum_{j=1}^{n} \binom{n}{j} \\
&< 1 + \frac{2n}{r} \cdot 2^n \quad \square
\end{aligned}$$

Note: $$\sum_{j=0}^{n} \binom{n}{j} = (1+1)^n.$$

**Lemma 2.** If $r > (2n)^{n+1}$, then

$$n! < r^n / \binom{r}{n} < n! + 1.$$

Proof.

$$\binom{r}{n} = \frac{r(r-1)\cdots(r-n+1)}{n!}.$$

Hence

$$\begin{aligned} r^n / \binom{r}{n} &= \frac{r^n n!}{r(r-1)\cdots(r-n+1)} \\ &= n! \left\{ \frac{1}{(1-\frac{1}{r})\cdots(1-\frac{n-1}{r})} \right\}. \end{aligned}$$

But

$$\begin{aligned} n! &< n! \left\{ \frac{1}{(1-\frac{1}{r})\cdots(1-\frac{n-1}{r})} \right\} \\ &< n! \, \frac{1}{(1-\frac{n}{r})^n} \\ &< n! + \frac{2n}{r} \cdot 2^n n! \\ &\leq n! + \frac{2^{n+1} n^{n+1}}{r} \\ &< n! + 1. \ \square \end{aligned}$$

**Theorem.** The set $\{< m, n > |\ m = n!\}$ is exponential Diophantine.

Proof. We claim that the following equations provide the desired definition:

$$\begin{aligned} s &= 2n + 1 && (1)\\ t &= n + 1 && (2)\\ r &= s^t && (3)\\ u &= r^n && (4)\\ v &= \binom{r}{n} && (5)\\ mv + c &= u && (6)\\ u + d + 1 &= (m + 1)v && (7) \end{aligned}$$

(6) and (7) are equivalent to $mv \leq u < (m + 1)v$, and, together with (4) and (5), to

$$m \leq r^n / \binom{r}{n} < m + 1.$$

Finally since(1),(2), and (3), implies $r = (2n + 1)^{n+1} > (2n)^{n+1}$, Lemma 2 gives the result. □

**Wilson's Theorem.** $p$ is a prime if and only if $p > 1$ and $(p-1)! + 1$ is divisible by $p$.

**Theorem.** The set of prime numbers is exponential Diophantine.

Proof. By Wilson's Theorem, the following equations do the job:

$$\begin{aligned} p &= 2 + w \\ p &= 1 + t \\ q &= t! \\ q &= p(r+2) \end{aligned}$$

□

# The Number of Solutions of a Diophantine Equation

If $p(x_1, \ldots, x_m)$ is a polynomial with integer coefficients, we write $\#(p)$ for the number of solutions in natural numbers of the equation $p(x_1, \ldots, x_m) = 0$. Note that $0 \leq \#(p) \leq \aleph_0$. We write $T^+(p)$ for the polynomial

$$[(x_1 - a_1)^2 + \ldots + (x_m - a_m)^2] \cdot p(x_1, \ldots, x_m)$$

where $< a_1, \ldots, a_m >$ is the first $m$-tuple (in a suitable ordering) such that $p(a_1, \ldots, a_m) \neq 0$. Evidently $\#(T^+(p)) = \#(p) + 1$. We define

$$\begin{aligned} T^{\,0}(p) &= p \\ T^{\,i+1}(p) &= T^+(T^{\,i}(p)) \end{aligned}$$

so that $\#(T^{\,i}(p)) = \#(T(p)) + i$. We also define

$$T^{\,\infty}(p) = (2x_{m+1} + 1)p(x_1, \ldots, x_m)$$

so that

$$\#(T^{\,\infty}(p)) = \begin{cases} 0 & \text{if } \#(p) = 0 \\ \aleph_0 & \text{otherwise.} \end{cases}$$

**Theorem.** Let $\mathcal{C} = \{0, 1, 2, \ldots, \aleph_0\}$. Let $\mathcal{A} \subseteq \mathcal{C}$, but $\mathcal{A} \neq \emptyset, \mathcal{C}$. Then there is no algorithm to determine of a given polynomial Diophantine equation $p = 0$ whether $\#(p) \in \mathcal{A}$.

Proof. We consider several cases.

*Case* 1. $\mathcal{A} = \{0\}$. This is just Hilbert's 10th Problem. The other cases will be reduced to this one.

*Case* 2. $0, \aleph_0 \in \mathcal{A}$. Let $r \notin \mathcal{A}$. Then for any $p$,

$$\#(p) = 0 \Leftrightarrow \#(T^r(T^\infty(p))) \notin \mathcal{A}.$$

*Case* 3. $0 \in \mathcal{A}, \aleph_0 \notin \mathcal{A}$. Then for any $p$,

$$\#(p) = 0 \Leftrightarrow \#(T^\infty(p)) \in \mathcal{A}.$$

*Case* 4. $0 \notin \mathcal{A}$. Then $\mathcal{C} - \mathcal{A}$ will be in Case 2 or 3. $\square$

## Equations with Real Roots

The following is a corollary of a famous theorem of Alfred Tarski:

*There is an algorithm to determine whether a given polynomial with integer coefficients has a solution in real numbers.*

To get an unsolvability result involving real variables, we use the sine function. Specifically, by a *combined system of equations* we understand a simultaneous system of equations each of which is of one of the forms:

$$p(x_1, \ldots, x_m) = 0 \quad \text{or} \quad \sin(p(x_1, \ldots, x_m)) = 0$$

where, as usual, $p$ is a polynomial with integer coefficients.

**Theorem.** There is no algorithm to determine whether a given combined system of equations has a solution in real numbers.

Proof. We show that such an algorithm could be used for Hilbert's Tenth Problem. So, let $p(x_1, \ldots, x_m) = 0$ be a given Diophantine equation. We claim that this equation has a solution in natural numbers if and only if the following system has a solution in real numbers:

$$
\begin{aligned}
p(x_1^2, \ldots, x_m^2) &= 0 && (1)\\
\sin(3 + u^2) &= 0 && (2)\\
7u^2 + v^2 - 1 &= 0 && (3)\\
\sin((3 + u^2)x_1^2) &= 0 && (4)\\
&\ldots\ldots\ldots\ldots\\
\sin((3 + u^2)x_m^2) &= 0 && (5)
\end{aligned}
$$

To see this, first suppose that (1)-(5) has a solution in real numbers. By (2), $3 + u^2 = n\pi$ where $n \geq 1$ is a natural number. By (3), $7n\pi = 22 - v^2$. So

$$n\pi \leq 22/7 = 3.142857\ldots$$

Thus, $n = 1$ and $3+u^2 = \pi$. Then, by (4)-(5) $x_1^2, \ldots, x_m^2$ are natural numbers which, by (1), satisfy the given Diophantine equation.

Conversely, suppose that

$$p(r_1, \ldots, r_m) = 0$$

where $r_1, \ldots, r_m$ are natural numbers. We obtain a solution in real numbers to (1)-(5) by setting

$u = \sqrt{\pi - 3}$, $v = \sqrt{22 - 7\pi}$, $x_i = \sqrt{r_i}$, $1 \leq i \leq m$. $\square$

Of course, by summing the squares of (1)-(5), we could get a result about a single equation.