An Nonnegative Integer Solution to the Jones-Sato-Wada-Wiens Polynomial

Eric Zheng

March 20, 2021

1 Introduction

As seen in lecture, there is a polynomial P of degree 25 in 26 variables such that $P(\mathbb{N}^{26}) \cap \mathbb{N}$ is precisely the set of primes. This polynomial was constructed by Jones, Sato, Wada, and Wiens in [Jones76], and it is a consequence of the following theorem from their paper.

Theorem 1 (Jones et al., Theorem 2.12)**.** *For any integer $k \geq 1$, in order that $k+1$ be prime it is necessary and sufficient that there exist nonnegative integers a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z such that:*

(1) $q = wz + h + j$,

(2) $z = (gk + g + k)(h + j) + h$,

(3) $(2k)^3(2k + 2)(n + 1)^2 + 1 = f^2$,

(4) $e = p + q + z + 2n$,

(5) $e^3(e + 2)(a + 1)^2 + 1 = o^2$,

(6) $x^2 = (a^2 - 1)y^2 + 1$,

(7) $u^2 = 16(a^2 - 1)r^2y^4 + 1$,

(8) $(x + cu)^2 = \left[(a + u^2(u^2 - a))^2 - 1\right](n + 4dy)^2 + 1$,

(9) $m^2 = (a^2 - 1)l^2 + 1$,

(10) $l = k + i(a - 1)$,

(11) $n + l + v = y$,

(12) $m = p + l(a - n - 1) + b(2a(n + 1) - (n + 1)^2 - 1)$,

(13) $x = q + y(a - p - 1) + s(2a(p + 1) - (p + 1)^2 - 1)$,

(14) $pm = z + pl(a - p) + t(2ap - p^2 - 1)$.

Remark. Theorem 1 requires that $k \geq 1$, and correspondingly the prime is $k+1$. When constructing the polynomial, it is preferable to allow $k \geq 0$ instead, so we replace k with $k+1$; correspondingly, the prime becomes $k+2$. We will stick to the $k \geq 1$ convention in our analysis, so that the prime is $k+1$ rather than $k+2$.

The "trick" behind this is to encode the factorial function in Diophantine equations, and then to use Wilson's theorem to characterize the primes.

Despite this being a fairly old construction, I was unable to find anywhere online a correct assignment witnessing the prime 2 ($k = 1$). But with the help of Mathematica and some lemmata from [Jones76] and [Davis73], we can find a solution—it turns out that the numbers are quite large.

The rest of this paper is structured as follows: first, we briefly list some relevant lemmata about solutions to the Pell equation. Then, we give an explicit solution to Theorem 1, witnessing the prime 2. Most of the constraints can be verified by a computer, but in particular constraints 7 and 8 contain numbers far too large to be automatically verified, so we will give explicit arguments for them.

2 The Pell Equation

The Pell equation, for some $a \geq 1$, is

$$x^2 = (a^2 - 1)y^2 + 1.$$

The solutions are known to be of the form $(x, y) = (\chi_a(n), \psi_a(n))$, where χ and ψ are defined by the recurrences

$$\begin{array}{lll} \chi_a(0) = 1 & \chi_a(1) = a & \chi_a(n+2) = 2a \cdot \chi_a(n+1) - \chi_a(n) \\ \psi_a(0) = 0 & \psi_a(1) = 1 & \psi_a(n+2) = 2a \cdot \psi_a(n+1) - \psi_a(n). \end{array}$$

Moreover, all pairs (x, y) of this form are solutions. For our purposes, we will only need the following results, which are proven in [Davis73]:

Lemma 1 (Davis, Lemma 2.11)**.** $\psi_a(n)^2 \mid \psi_a(n \cdot \psi_a(n))$.

Lemma 2 (Davis, Lemma 2.15)**.** *If $a \equiv b \mod c$, then for all n,*

$$\chi_a(n) \equiv \chi_b(n) \mod c.$$

Since we will be expressing some values in our solution in terms of χ and ψ, it is nice to have closed form expressions for them. We can derive a closed form for $\chi_a(n)$ by applying some standard tricks: observe that

$$\begin{pmatrix} \chi_a(n+1) \\ \chi_a(n) \end{pmatrix} = \begin{pmatrix} 2a & -1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} a \\ 1 \end{pmatrix}.$$

The matrix has eigenvalues $\lambda_1 = a - \sqrt{a^2 - 1}$ and $\lambda_2 = a + \sqrt{a^2 - 1}$, and eigenvectors

$$v_1 = \begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix}, \qquad v_2 = \begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix}.$$

Now $(a, 1) = (v_1 + v_2)/2$, so applying linearity, we see that

$$\chi_a(n) = \frac{1}{2} \left(\lambda_1^n + \lambda_2^n \right).$$

We can apply the same process to determine $\psi_a(n)$; the only difference is that the initial value is $(1, 0) = (v_2 - v_1)/2\sqrt{a^2 - 1}$, so the solution is

$$\psi_a(n) = \frac{1}{2\sqrt{a^2 - 1}} \left(\lambda_2^n - \lambda_1^n \right).$$

3 An Explicit Solution

Claim 1. *A nonnegative integer solution to the constraints in Theorem 1, corresponding to the prime $k+1=2$, is:*

$$\begin{aligned}
a &= 7901690358098896161685556879749949186326380713409290912 \\
b &= 0 \\
c &= \frac{2(a+u^2(u^2-a))^2-x-1}{u} \\
d &= \frac{2(a+u^2(u^2-a))-n}{4y} \\
e &= 32 \\
f &= 17 \\
g &= 0 \\
h &= 2 \\
i &= 0 \\
j &= 5 \\
k &= 1 \\
l &= 1 \\
m &= a \\
n &= 2 \\
o &= 8340353015645794683299462704812268882126086134656108363777 \\
p &= 3 \\
q &= 16 \\
r &= \frac{\psi_a(4a\cdot\psi_a(4a))}{16a^2} \\
s &= 1 \\
t &= 0 \\
u &= \chi_a(4a\cdot\psi_a(4a)) \\
v &= 2a-3 \\
w &= 1 \\
x &= \chi_a(2) = 2a^2-1 \\
y &= \psi_a(2) = 2a \\
z &= 9.
\end{aligned}$$

For most of these values, it is straightforward to see that they are nonnegative integers, and most of the constraints in Theorem 1 can be automatically checked. A Wolfram Language/Mathematica program which does this is available at the author's website.[1]

[1] `https://www.ericzheng.org/files/misc/prime.wl`

However, some of these numbers, particularly c, d, r, and u, are large enough that directly computing them and substituting them into the constraint equations is not feasible, and it is not obvious that they are all nonnegative integers. This means that we must verify constraints (7) and (8) manually.

- First, we consider constraint (7), that

$$\begin{aligned} u^2 &= 16(a^2-1)r^2y^4 + 1 \\ &= (a^2-1)(16a^2r)^2 + 1. \end{aligned} \tag{1}$$

  This must hold because

$$\begin{aligned} u &= \chi_a(4a \cdot \psi_a(4a)) \\ 16a^2r &= \psi_a(4a \cdot \psi_a(4a)), \end{aligned}$$

  and so $(u, 16a^2r)$ must satisfy the Pell equation 1. So we only need to show that r is indeed an integer. Note that $16a^2 \mid 16a^4 = \psi_a(2)^4$. By applying Lemma 1 twice, we see that

$$\psi_a(2)^4 \mid \psi_a(2 \cdot \psi_a(2))^2 = \psi_a(4a)^2 \mid \psi_a(4a \cdot \psi_a(4a)),$$

  and therefore $16a^2 \mid \psi_a(4a \cdot \psi_a(4a))$.

- Next, we consider constraint (8), viz.

$$\begin{aligned} (x+cu)^2 &= \left[(a+u^2(u^2-a))^2 - 1\right](n+4dy)^2 + 1 \\ &= (\beta^2-1)(n+4dy)^2 + 1, \end{aligned} \tag{2}$$

  where we have substituted $\beta = a + u^2(u^2-a)$ for clarity. Again, we have

$$\begin{aligned} x + cu &= 2\beta^2 - 1 = \chi_\beta(2) \\ n + 4dy &= 2\beta = \psi_\beta(2), \end{aligned}$$

  and so direct substitution shows that equation 2 is satisfied. All that remains is to show that c and d are nonnegative integers. For c, observe that $a \equiv \beta \mod u$, and so by Lemma 2, $\chi_a(2) \equiv \chi_\beta(2) \mod u$. Additionally, since $\beta > a$, we definitely have $c \geq 0$.

  For d, notice that equation 1 implies that $u^2 \equiv 1 \mod 4y$. Therefore $\beta \equiv 1 \mod 4y$, and $2\beta \equiv 2 \mod 4y$. Recall that $n = 2$, and so $d = (2\beta - n)/4y$ is a nonnegative integer.

References

[Jones76] James P. Jones, Daihachiro Sato, Hidea Wada, and Douglas Wiens, Diophantine representation of the set of prime numbers, *The American Mathematical Monthly*, 83 (1976) 449-464.

[Davis73] Martin Davis, Hilbert's tenth problem is unsolvable, *The American Mathematical Monthly*, 80 (1973) 233-269.